Bezpieczeństwo. Rodzina – naród – społeczeństwo
J. Zimny (red.), Wyższa Szkoła Ekonomiczna w Stalowej Woli, Katolicki Uniwersytet Lubelski, Stalowa Wola 2016, s. 269-292.
ISBN 978-83-63835-44-6

Bezpieczeństwo w cyberprzestrzeni jako wyzwanie dla współczesnych państw - zarys problemu
Security in cyberspace as a challenge for modern states - a general outline

Leszek Klich, Cezary Sochala

Streszczenie

Dynamiczny rozwój technologii cyfrowej sprawił, że komputeryzacja objęła niemal wszystkie sektory państwa. Ekspansja tej technologii wywarła ogromny wpływ także na społeczeństwo, które współcześnie przekształca się w społeczeństwo informacyjne. Również w Polsce, choć z opóźnieniami w stosunku do rozwiniętych państw europejskich - sukcesywnie wdrażany jest model gospodarki opartej na wiedzy. Powszechna informatyzacja, jako działalności natury technicznej, organizacyjnej i ekonomicznej, zapewnić może liczne korzyści. Oprócz pozytywnych aspektów cyfryzacji, należy dostrzec także pojawienie się wielu związanych z nią - nowych form zagrożeń. Wyniki badań wskazują, że niekorzystne procesy i zjawiska w cyberprzestrzeni dynamicznie ewoluują oraz multiplikują się, a ich liczebność oraz charakter uzasadniają ich uwzględnienie w ramach zagrożeń dla szeregu podmiotów, ze współczesnymi państwami - włącznie. Sytuacja taka sugeruje podejmowanie adekwatnych działań administracyjnych, a w konsekwencji determinujących je badań naukowych dotyczących bezpieczeństwa ww. podmiotów w aspekcie postępującej cyfryzacji państw i ich społeczeństw. W badaniach tych uwzględnić należy w szczególności procesy oraz zjawiska w cyberprzestrzeni, które wpływają na bezpieczeństwo państwa – jako instytucje odpowiedzialne za zapewnienie bezpieczeństwa społeczeństwom. Przedstawiono w niniejszej publikacji zarys ww. sytuacji problemowej tworzą rozdziały poświęcone: genezie i istocie społeczeństwa informacyjnego; informacji, jako dobra podlegającego ochronie – w aspekcie wymaganych zdolności systemów informatycznych i pozostałych systemów oraz usług służących przetwarzania informacji; problematyce współczesnych wyzwań dla bezpieczeństwa w cyberprzestrzeni, ze szczególnym uwzględnieniem wybranych problemów

jego programowania – w aspekcie zapewnienia bezpieczeństwa państwa oraz jego podmiotów, w tym społeczeństwa.

Summary

The dynamic development of digital technology has resulted in computerisation taking over all of the national sectors. The expansion of teleinformatics has also made a huge impact on society, which in our times is transforming into an IT society. This applies to Poland as well, but with delays in relation to developed European countries – the model of an economy based on knowledge is successively being implemented. The common informatisation can provide numerous benefits as an activity of a technical, organisational and economic nature. Apart from the positive aspects of digitalisation, we should also notice the many new forms of threats related to it. Research results indicate that unbeneficial processes and phenomena in cyberspace are evolving and multiplying dynamically, and their amount and character justify their consideration as part of threats for a series of subjects, including present countries. Such a situation suggests taking adequate administrative actions, and as a consequence, scientific research that determine those actions, which concerns the safety of the above-mentioned subjects in the aspects of the ongoing digitalisation of countries and societies. In these studies, processes and phenomena in cyberspace, which affect national safety, should be especially considered – as institutions responsible for providing societies with safety. The outline of the above-mentioned problematic situation has been presented in this publication, creating chapters dedicated to: the genesis and essence of the IT society; information as a good that is subject to protection – in the aspect of the required abilities of IT systems and the remaining systems as well as services used to process information; the problematics of present challenges for safety in cyberspace, with an especial consideration of chosen problems of its programing – in the aspect of providing safety to the country and its subjects, including society. The publication is complemented with motions.

Wstęp

Rozwój technologii informacyjnych wywarł dalekosiężne następstwa, które współcześnie oddziałują na szerokie spektrum podmiotów – od jednostek, po społeczeństwa państw oraz ich gospodarki. Na skutek masowego wykorzystania urządzeń elektronicznych do tworzenia, obróbki, transferu i dystrybucji informacji, dokonały się zmiany, które porównywane są do przemian ekonomicznych, technicznych kulturowych i społecznych w rewolucjach przemysłowych. Zmiany te, oprócz pozytywnych aspektów, niosą za sobą także określone zagrożenia – pierwotne i wtórne, które współcześnie dotyczyć mogą wszystkich podmiotów państw, a także szeregu domen ich działalności. Uwzględniając ich istotę, skalę oraz zasięg, dostrzec należy wyzwania dla bezpieczeństwa, które stanowią zagadnienia problemowe, zarówno dla teoretyków, jak i praktyków problematyki bezpieczeństwa.

Opisu naukowego wymaga zarówno część dotycząca genezy oraz istoty społeczeństwa informacyjnego, jak również informacji, jako współczesnego dobra – w aspekcie bezpieczeństwa podmiotów je wykorzystujących. Doskonalenia wymagać mogą niektóre rozwiązania prawne i organizacyjne państwa, którego niezmienną funkcją jest zapewnienie bezpieczeństwa swoich obywateli. Problematyce tej poświęcona została niniejsza publikacja. W jej pierwszej części przedstawiono genezę i istotę społeczeństwa informacyjnego. Drugą część zaś poświęcono informacji – jako dobru podlegającemu ochronie, w aspekcie wymaganych zdolności systemów informatycznych oraz pozostałych systemów i usług dotyczących przetwarzania informacji. W ostatniej części podjęto problematykę współczesnych wyzwań dla bezpieczeństwa w cyberprzestrzeni, ze szczególnym uwzględnieniem wybranych problemów jego programowania – w aspekcie zapewnienia bezpieczeństwa państwa oraz jego podmiotów – w tym społeczeństwa. Publikacje dopełniają wnioski.

Geneza i istota społeczeństwa informacyjnego

Masowa implementacja w latach 70. XX w. szeregu rozwiązań i urządzeń służących do przetwarzania informacji, a także rozwój usług z tym związanych, dał początek nowemu modelowi społeczeństwa. Ten nowy model wywodzi się z krajów postindustrialnych, gdzie

rozwój technologii informatycznej przybrał najszybsze tempo, a nauki informacyjne odegrały dużą rolę w rozwoju gospodarki. Należy wskazać, że w krajach tych, nowoczesne technologie dokonały transformacji modelu gospodarczego, wypierając pracę ręczną – maszynami, zaś produkcję jednostkową – produkcją masową[1].

Kolejnym i znaczącym krokiem, podobnym jak w przypadku rewolucji przemysłowej, był wzrost znaczenia informacji. Wysoko rozwinięte kraje zachodu, na skutek zdobywania, gromadzenia, przetwarzania i przekazywania informacji, stały się bazą dla powstania nowego modelu społeczeństwa, którego podstawowym zasobem jest wiedza, zaś jego cechami są: powszechność narzędzi informatycznych oraz coraz nowsze sposoby przekazywania informacji. Takie podejście wymusiło ewolucję organizacji państwa oraz jego gospodarki, a ciężar konkurencji został przeniesiony w sferę nauki. Informacja, jako zasób produkcyjny, prowadzi do nasilenia się integracji badań naukowych oraz procesów produkcyjnych. Kluczowym elementem tego modelu jest infrastruktura naukowa, która prowadzi do rozwoju produktów, umożliwiając swobodny przepływ zarówno wiedzy, jak i technologii pomiędzy krajami[2]. Nieodłącznym elementem tych procesów informacyjnych jest człowiek, jako użytkownik, a niejednokrotnie – także jako element systemu. Obecnie zaobserwować można stały postęp technologiczny w dziedzinie przetwarzania informacji, dokonujący się za pomocą stale rosnącej techniki komputerowej.

Trudno jest jednoznacznie określić, co napędza ten proces. Wielu badaczy uważa, że motorem zmian jest gospodarka – ze względu na jej szerokie oddziaływanie, które obejmuje wszystkie aspekty życia. W konsekwencji, fundamentalne znaczenie zyskuje współcześnie jakość posiadanych informacji[3].

Naukowcy podjęli próby zdefiniowania tego fenomenu, w wyniku czego powstały takie określenia jak: *społeczeństwo informacyjne* czy *społeczeństwo oparte na wiedzy*. Niezależnie od różnic terminologicznych podkreślić należy, że obie definicje dotyczą tego samego zjawiska. Koncepcja społeczeństwa informacyjnego ma charakter interdyscyplinarny, będąc częścią wiedzy z dziedziny socjologii, ekonomii oraz dziedzin technicznych, choć

[1] M. Leszczyńska, *Współczesny model rozwoju społecznego z perspektywy rewolucji informacyjnej*, Katedra Teorii Ekonomii i Stosunków Międzynarodowych, Uniwersytet Rzeszowski, s. 125.
[2] M. Majta, *Rola informacji w kształtowaniu nowych społeczeństw*, EBIB, Wrocław 2005, s. 4.
[3] Red M. Witkowska, K. Cholawo – Sosnowska, *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*, s. 13

czasem w literaturze spotkać można sprowadzenie tego pojęcia jedynie do wymiaru technologicznego[4].

Termin *społeczeństwo informacyjne* użyty został po raz pierwszy w 1963 r. - przez japońskiego socjologa Tadao Umesao. Jednak dopiero inny japoński naukowiec – futurolog Keinichi Koyama, autor rozprawy *Introduction to Information Theory*, podjął się jego uszczegółowienia. Kolejnym naukowcem, który badał to zjawisko - był Yoneji Masuda, rozpowszechniając w roku 1990 na Oxfordzie znamienne słowa: *Cywilizację, którą zbudujemy, zbliżając się do końca XX wieku, nie będzie cywilizacją materialną, symbolizowaną przez ogromne konstrukcje, ale będzie faktycznie cywilizacją niewidoczną. Precyzyjnie powinno się ją nazwać cywilizacją informacyjną. Homo sapiens, który pod koniec ostatniej epoki lodowcowej stanął przed początkiem pierwszej – materialnej cywilizacji, stoi dziś po dziesięciu tysiącach lat na progu drugiej – cywilizacji informacyjnej*[5].

Definicję społeczeństwa informacyjnego zawarto także m.in. w tzw. raporcie Bangemanna[6]. W świetle ustaleń tego dokumentu [...] społeczeństwo informacyjne charakteryzuje się przygotowaniem i zdolnością do użytkowania systemów informatycznych i wykorzystuje usługi telekomunikacyjne do przekazywania i zdalnego przetwarzania informacji.

Niezależnie od przyjętej definicji, społeczeństwo oparte na wiedzy charakteryzuje się wysokim stopniem wykorzystania informacji i wiedzy w życiu codziennym, zaś podstawowym warunkiem dla jego rozwoju jest powszechny, nieograniczony i jednocześnie akceptowalny ekonomicznie dostęp do informacji. Innymi warunkami są: kompatybilność technologiczna oraz bezpieczeństwo medium przekazu, które powinno zapewnić niezakłóconą możliwość przetwarzania danych. Wynika z tego, że kierunek przekształceń

---

[4] M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji,* Katedra Informatyki Akademii Ekonomicznej w Krakowie, s. 3.

[5] Y. Masuda, *The Information Society as Post-Industrial Society*, cyt. Za: P. Sienkiewicz, *Masowe komunikowanie w społeczeństwie informacyjnym*, [w:] *Mass media w systemie komunikacji społecznej w Polsce*, red. A. Kudłaszczyk, A. Małkiewicz, R. Karpiński, s. 56.

[6] Na spotkaniu Rady Europejskiej w grudniu 1993 roku w Brukseli postanowiono zwrócić się do grupy wybitnych osobistości z prośbą o przygotowanie raportu na zebranie mające się odbyć w dniach 24 - 25 czerwca 1994 roku w Corfu w sprawie konkretnych posunięć do rozważenia przez Wspólnotę i kraje członkowskie w kwestii infrastruktur w zakresie informacji. Na podstawie tego raportu Rada uchwalić miała program wykonawczy definiujący dokładne procedury działania i konieczne środki. Raport Bangemanna. Zalecenia dla Rady Europejskiej. http://cyberbadacz.republika.pl/raport_bangemanna.html

współczesnych społeczeństw jest silnie zdeterminowany technologicznie[7]. Nie mniej ważnym kryterium decydującym o rozwoju społeczeństwa informacyjnego jest umiejętność użycia technologii przez uczestników procesu. Dopiero spełnienie tych zależności czyni społeczeństwo – informacyjnym.

Równolegle z nową technologią, ewoluowało społeczeństwo, które wykorzystując technologię informacyjną, stawało sie coraz bardziej świadome możliwości oraz szans, jakie niesie współczesna technika informacyjna.

Należy przy tym odróżnić dwa funkcjonujące równolegle i bardzo podobnie brzmiące pojęcia: *społeczeństwo informacyjne* oraz *społeczeństwo informatyczne*, które często są zestawiane jako równorzędne bądź też używane zamiennie, choć w rzeczywistości mają one odrębne znaczenia. Wyjaśnienie związków i różnic pojęciowych stanowi w tym przypadku kluczowy element opisu relacji między postępem technologicznym a informacyjnym. W podziale tym należy wyodrębnić rewolucję informacyjną – wraz z bezpieczeństwem informacyjnym oraz rewolucję informatyczną – z bezpieczeństwem informatycznym.

Pojęcie rewolucji informacyjnej oraz bezpieczeństwa informacyjnego ma szerszy zakres znaczeniowy, ponieważ oprócz opisów technologii, obejmuje równocześnie stały wzrost wartości informacji, niezależnie od jej formy. Jest to szczególnie istotne dla funkcjonowania społeczeństwa oraz wytwarzania dóbr i dochodu narodowego[8].

Z kolei pojęcie *społeczeństwo informatyczne* dotyczy bezpośrednio fizycznej części technologii teleinformatycznych, choć sama technologia, bez umiejętności jej wykorzystania, nie czyni społeczeństwa informacyjnym. Istota społeczeństwa informacyjnego nie polega więc na rodzaju wykorzystanej techniki, lecz na skutkach jej użycia. Sensem informacji jest zaś nadawanie oraz odbiór, analiza, gromadzenie czy przekazywanie.

Elementarną właściwością społeczeństwa informacyjnego jest przetwarzanie informacji, zatem społeczeństwo informacyjne oraz informacja stanowią komplementarną jedność.

---

[7] E. Inglot-Brzęk, *Brak dostępu do Internetu jako wskaźnik wykluczenia społecznego*, Katedra Nauk Społecznych Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie, s. 374.

[8] Red. M. Madej, M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 18.

Informacja jako zasób szczególnie chroniony

W uwarunkowaniach społeczeństwa informacyjnego – informacja i wynikająca z niej wiedza – wraz z technologią, stanowią podstawowy czynnik wytwórczy[9].

Słowo *informacja* pochodzi od łacińskiego słowa *informatio* (wyobrażenie, wyjaśnienie, zawiadomienie), stanowiąc teorię przekazywania wiadomości. Według Małego Słownika Języka Polskiego, *informacja* to powiadamianie o czymś, oznajmianie, wiadomość lub pouczenie[10]. Z kolei *informacja naukowa* oznacza zorganizowaną działalność, która jest związaną z gromadzeniem, przetwarzaniem i udostępnianiem wiadomości z różnych dziedzin, szczególnie nauki i techniki[11]. Informację stanowić może liczba, słowo, obraz, dźwięk, itp. Może ona zostać wykorzystana przez ludzi lub urządzenia do zgodnego z zamiarem wykonywania określonego zadania, sterowania procesem czy budowania wiedzy. Stąd ważnym aspektem jest jej prawidłowe i nieprzekłamane przesyłanie.

Informacja jest podstawowym elementem procesu decyzyjnego we wszystkich dziedzinach życia, zaś podstawą jej powstawania są dane, które muszą być dla odbiorcy zrozumiałe oraz wnosić element nowości. Należy jednocześnie podkreślić, że wytwarzanie informacji jest powszechną cechą społeczeństwa informacyjnego, zaś każda jednostka społeczna może generować informacje, stając się tym samym jej źródłem (emiterem). Odbiór natomiast może mieć charakter jednostkowy lub też masowy, w zależności od typu medium przekazu oraz przeznaczenia[12].

Współczesne technologie pozwalają na przechowywanie niemal dowolnej ilości informacji, ograniczonej jedynie pojemnością nośników, która wciąż się zwiększa, osiągając teoretycznie nieograniczone pojemności. Terabajty informacji gromadzone są już nie tylko na powszechnie dostępnych stronach internetowych, lecz także w publicznych oraz zamkniętych bazach danych. Ogromny postęp, jaki dokonał się w XX w., jest procesem powodującym nieustanny rozwój technik przechowywania informacji przy uwzględnieniu czynników

[9] Krajowa Rada Radiofonii i Telewizji, *Społeczeństwo informacyjne w Polsce – Wstęp do formułowania założeń polityki Państwa*, Warszawa 1996, http://kbn.icm.edu.pl/pub/info/dep/spo.html (stan na 28.03.2016).
[10] Red. E. Sobol, *Mały Słownik Języka Polskiego*, PWN, Warszawa 1993, s. 265.
[11] Zob. *Encyklopedia PWN*, http://encyklopedia.pwn.pl/haslo.php?id=4008527 (stan na 9-02-2011).
[12] M. Gajewicz, *Społeczeństwo informacyjne – problemy (zagadnienia)*: http://www.id.uw.edu.pl/~mgajlewicz/SpoleczenstwoInformacyjne, s. 4.

ekonomicznych, co jeszcze bardziej przyspiesza procesy digitalizacji wszelkich dziedzin życia.

Specyfiką informacji, jako dobra konsumpcyjnego, jest jej zróżnicowana wartość dla poszczególnych odbiorców. Zjawisko to dotyczy także innych dóbr i usług „nieinformacyjnych", lecz w przypadku informacji, to odbiorca ostatecznie decyduje o jej przydatności. W przypadku zjawiska „konsumpcji informacji", którego specyfika polega na interpretacji odbieranych sygnałów, jako procesu semiotycznego trwającego w czasie, dostrzec należy prawidłowość, gdzie konsumpcja nie zależy wyłącznie od cech informacji, lecz także od zdolności semiotycznych odbiorcy[13].

Wartość informacji można analizować wielopłaszczyznowo. Informacja, podobnie jak w epoce przemysłowej - kapitał, jest dziś ważnym czynnikiem wpływającym na rozwój[14]. Jak podkreśla A. Targowski, że *informacja jest sercem nauki i techniki, czyli agentem przemian*[15]. Stanowi ona współcześnie podstawę egzystencji nie tylko społeczeństwa, ale także gospodarki opartej o przepływ wiedzy[16].

Coraz bardziej efektywne oprogramowanie zapewnia możliwość bieżącej subskrypcji wielu źródeł danych w dowolnej ilości i z całego świata. Presja czasu, z jaką mamy obecnie do czynienia, implikuje konieczność stałej synchronizacji danych w wielu sektorach państwa, stanowiących jego kluczowe elementy dla gospodarki. Bankowość, giełda, waluty, energetyka czy transport to obszary, które wymagają dokładnej informacji oraz jak najkrótszego czasu jej przekazywania (gdzie liczą się setne części sekundy, zaś procesy i zjawiska trwające minuty - stanowią przeszłość). Szybsze zdobycie najświeższej, sprawdzonej i niezakłóconej informacji decyduje o bardziej skutecznym zarządzaniu firmą, pozwalając na wyprzedzenie konkurencji, ponieważ *ubóstwo informacji jest niezwykle powszechną przyczyną błędnych ocen i wnioskowania*[17].

Informacja wykorzystywana jest na wiele sposobów, z których wymienić można edukację, jako proces upowszechniania wiedzy naukowej oraz uświadamiania uczestnikom cyberprzestrzeni stałej konieczności podnoszenia własnych kwalifikacji. Informacja to

---

[13] J. Oleński, *Ekonomika informacji*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2001, s. 313.
[14] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Adam Marszałek, Toruń 2005, s. 5.
[15] A. Targowski, *Informatyka – klucz do dobrobytu*, PIW, Warszawa 1971, s. 40.
[16] L. H. Haber, *Społeczeństwo informacyjne – wizja czy rzeczywistość*?, II ogólnopolska konferencja naukowa, Kraków, 30 maja 2003, s. 171.
[17] Tamże.

również komunikacja czasu rzeczywistego. Komunikowanie się było od zawsze nieodłącznym elementem interakcji międzyludzkiej.

Należy zauważyć, że komunikowanie się oznacza przepływ informacji – niezależnie od treści komunikatu, a skuteczne komunikowanie się polega na takim przekazaniu informacji, aby osoba odbierająca przekaz zrozumiała jego treść. Nie chodzi tutaj o komunikację bezpośrednią, a raczej - zjawisko przepływu informacji w ramach poszczególnych grup społecznych, zbiorowości etc. (np. skupionych w forach dyskusyjnych, portalach społecznościowych czy internetowych komunikatorach czasu rzeczywistego). Zjawisko stało się faktem i wciąż zyskuje co do zasięgu i znaczenia - za sprawą młodego pokolenia, będącego swego rodzaju „motorem zmian", których starsze pokolenie może nie rozumieć, a nawet może się go obawiać.

Dzięki nowym technologiom stało się możliwe przełamywanie barier kulturowych w obrębie jednej harmonijnej całości – globalnego społeczeństwa informacyjnego. W przypadku osób stale lub czasowo wyłączonych z możliwości swobodnego funkcjonowania w społeczeństwie, powszechny dostęp do informacji pełnić może rolę socjalizacyjną oraz aktywizacyjną, czego przykładem jest coraz powszechniejsza telepraca. Funkcje te w niektórych przypadkach są jedyną możliwością powrotu jednostki do społeczeństwa, w szczególności dla osób niepełnosprawnych bądź też przewlekle chorych.

Dla wielu państw, pewne cechy i funkcje społeczeństwa informacyjnego stały się strategicznie ważną ścieżką rozwoju cywilizacyjnego, stąd można wymienić podstawowe uwarunkowania gwarantujące jego rozwój – a wśród nich przede wszystkim liberalizację rynków, na których realizowane są usługi. Dotyczy to zarówno powszechnego i równego dostępu dla operatorów i usługodawców, oferujących dostęp do sieci, lecz także innych sfer gospodarki. Takie stanowisko gwarantuje swobodę wyboru przez obywateli. Wiele państw dąży do zapewnienia takiego stanu w możliwie wielu sektorach funkcjonowania społeczeństwa.

Cyberprzestrzeń jako nowa przestrzeń ekspozycji na zagrożenia

Rozwój technologiczny zapoczątkował proces uniezależniania się człowieka od nieprzewidywalnych zjawisk natury, poprzez ograniczenie wpływu niektórych negatywnych

zjawisk środowiskowych na życie człowieka. Pozytywnym skutkiem tego procesu stało się dodatkowo poszukiwanie wtórnych, w stosunku do pierwotnych – potrzeb.

Jednocześnie proces ten kreował lub powodował kreację nieznanych dotąd zagrożeń. Obecnie ta swoista spirala rozwoju jest zjawiskiem, bez którego trudno sobie wyobrazić funkcjonowanie człowieka w oderwaniu zarówno od infrastruktury teleinformatycznej, ale także od dobrodziejstw, które niesie za sobą technologia[18]. Pojawienie się zjawiska dyfuzji innowacji,[19] spowodowało zapoczątkowanie istnienia szeregu zagrożeń, z których jako część wspólną, wymienić można zależność odtechnologiczną.

W takim ujęciu dostrzec należy stały wzrost liczby możliwych obszarów negatywnego oddziaływania w cyberprzestrzeni i jednocześnie zwiększenie ilości punktów potencjalnego ataku. W konsekwencji nawet krótkotrwałe przerwy w funkcjonowaniu infrastruktury, spowodowane np. zakłóceniami w pracy systemów informatycznych, mogą wywołać konsekwencje społeczne i gospodarcze, a scenariusze uwzględniające długotrwałe przerwy – nie był dotąd zazwyczaj nawet rozważane.

Oprócz licznych pozytywnych skutków dla społeczeństwa, w tym rozwoju gospodarczego kraju, powszechny i nieograniczony dostęp do cyberprzestrzeni niesie także nieznane dotąd zagrożenia. Szybko dostrzeżono, iż cyberprzestrzeń stała się miejscem dokonywanie przestępstw za pomocą technologii komputerowej. Silne osieciowienie wielu obszarów życia spowodowało przeniesienie tam także wielu innych negatywnych działań. Coraz bardziej powszechne stają się anonimowe cyberataki na informacje, prowadzące zarówno do zakłóceń ich przetwarzania, jak i do bardziej destrukcyjnych skutków, na które społeczeństwo, a co gorsze – państwa, nie są obecnie przygotowane technicznie, prawnie i organizacyjnie: efekty tego typu działań cyberprzestępców są coraz bardziej dostrzegalne, ponieważ tradycyjne miejsce przestępstw w wielu obszarach przeniosło się na zupełnie inny teren, przez co zaobserwowanie procesów i skutków cyberataków stało się o wiele trudniejsze, a ich analiza i metody obrony – zarezerwowane dla wąskiego grona specjalistów.

---

[18] Pod red. J. Świątkowskiej, *Bezpieczeństwo infrastruktury krytycznej. Wymiar teleinformatyczny*, Instytut Kościuszki, Kraków 2014, s. 9.

[19] Dyfuzja innowacji polega między innymi na dzieleniu się informacją a także przekazywaniu referencji opinii między grupami społecznymi, zaś istotną cechą jest fakt, że komunikacja ta dotyczy produktów czy idei, które jednostka postrzega jako nowe. M. Muras, W. Zabłocki, *Zastosowanie teorii dyfuzji innowacji na przykładzie wprowadzenia na rynek Airbusa A380*, Prace Naukowe Politechniki Warszawskiej, Politechnika Warszawska, nr 89/2013, s. 137.

Bezpieczeństwo państwa jest obecnie ściśle powiązane ze stanem jego bezpieczeństwa teleinformatycznego, przez co kategoria ta jest zawsze obecna w polityce bezpieczeństwa państwa, łącząc procedury i narzędzia ochrony danych, informacji i systemów[20]. Zdaniem K. Liedela, bezpieczeństwo narodowe w każdej płaszczyźnie jest coraz bardziej uzależnione od swobodnego przepływu informacji i od zachowania systemów bazujących na przesyłanych informacjach. Prognoza rozwoju sieci teleinformatycznych oraz systemów wskazuje zaś, że obszary zastosowania technologii transmisji i przetwarzania danych będą się stale zwiększać. Obszar militarny, gospodarka, energetyka, media, systemy finansowe i transportowe są szczególnie uzależnione od systemów informatycznych[21].

Trendy rozwoju zagrożeń cybernetycznych wskazują wyraźnie na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne kraju, co przy rosnącym uzależnieniu od technologii teleinformatycznej może poważnie zakłócić funkcjonowanie społeczeństw oraz państw[22].

W szczególnych przypadkach, przejęcie kontroli przez podmioty zewnętrzne nad danymi, informacjami lub systemami infrastruktury krytycznej może spowodować paraliż państwa[23], zaś funkcjonowanie społeczeństw i gospodarek jest w ogromnym stopniu uzależnione od ciągłego zapewnienia dostępu do: wody, elektryczności, gazu, ropy naftowej, transportu, łączności, żywności, czy usług bankowych[24].

Dostrzec należy także dynamiczny rozwój oprogramowania dedykowanego cyberprzestępstwom. W przeszłości dokonujący ataków musieli odznaczać się dużą wiedzą dotyczącą łamania zabezpieczeń systemów do przeprowadzenia ataku. Sytuacja ta jednak uległa zmianie i obecnie niemal każdy może dokonać ataku w cyberprzestrzeni poprzez pozyskanie niezbędnych narzędzi oraz ich użycie bez posiadania ww. wiedzy. Istnieje bowiem bardzo wiele narzędzi służących do zautomatyzowanego generowania i rozpowszechniania złośliwego oprogramowania. Ich skuteczność wynika już nie tylko

---

[20] A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, Roczniki Kollegium Analiz Ekonomicznych nr 29/2013, Wydział Humanistyczny Uniwersytet Pedagogiczny w Krakowie, http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z29_30.pdf, s. 452.

[21] Zob. K. Liedel, *Bezpieczeństwo informacyjne jako element bezpieczeństwa narodowego*, http://www.liedel.pl/?p=13 (stan na 05-11-2014).

[22] Tamże, s. 19.

[23] Mirosław Maj, *Debata na temat strategii obrony cyberprzestrzeni*, Dziennik Gazeta Prawna, nr 5 (3395).

[24] Zob. http://www.computerworld.pl/news/383495/Wojny.w.cyberprzestrzeni.html (stan na 17-03-2016).

z powszechnej dostępności, ale także z dużej wydajności – w szczególności w sferze szybkości rozprzestrzeniania się infekcji[25].

Współcześnie wzrasta znaczenie walki informacyjnej. Zarówno w otoczeniu zewnętrznym jak i wewnętrznym, zajmuje ona znaczącą pozycję, stanowiąc zagrożenie dla wszystkich sfer działalności państwa oraz jednostki[26]. W aspekcie bezpieczeństwa, istotne znaczenie przypisywać należy zagrożeniom hybrydowym, czy też jak należałoby obecnie stwierdzić – wojnie hybrydowej[27]. Strategia ta łączy poszczególne elementy działań konwencjonalnych, nieregularnych, cybernetycznych, a w zależności od definicji – również innych elementów działań o charakterze destrukcyjnym[28]. Tego typu wojna, prowadzona często bez wypowiedzenia, może stanowić niezwykle agresywną formę działań wojennych, zaś w rzeczywistości, jak pokazuje praktyka, pozwala na całkowite lub częściowe – uniknięcie odpowiedzialności za jej podjęcie[29].

W przypadku ataków międzynarodowych, jedną z metod ochrony cyberprzestrzeni państwa jest odstraszanie. Metoda ta, rozwijana także przez NATO, jako jedna z metod ochrony zasobów cyfrowych, może stanowić skuteczną metodę zwiększenia bezpieczeństwa - poprzez deklarację o wspólnej reakcji sojuszu na potencjalny atak. Niestety – wielu sojusznikom brakuje odpowiednich zdolności ofensywnych. Zatem potencjalni agresorzy wciąż mogą decydować się na uderzenie cybernetyczne, którego ewentualne niepowodzenie nie będzie miało dla nich poważnych konsekwencji. Deklaracja Walijska[30] wprowadziła w życie zapis o możliwości uruchomienia artykułu 5, związanego z odwetem, jednak nie sprecyzowano jasno określenia „dotkliwości" skutków cyberataku. Wyraźnie zaznaczono jednak, że decyzja o zbiorowej odpowiedzi będzie podejmowana przez Radę Atlantycką w zależności od danego przypadku, co w praktyce oznacza porównywalne skutki do efektów uderzeń konwencjonalnych. Tego typu sformułowanie może sugerować, że NATO zareaguje

---

[25] Autor ma na myśli zarówno modyfikację i tworzenie kolejnych generacji oprogramowania złośliwego – w tym stosowanie mechanizmów polimorfizmu oraz technik szyfrowania.
[26] Tamże, s. 447.
[27] Zob. http://www.defence24.pl/125802,nato-nie-ma-strategii-dzialania-na-wojne-hybrydowa (stan na 21-03-2016).
[28] *Hybrid war – does it even exist?*, http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm (stan na 21-03-2016).
[29] L. Skoneczny, *Wojna hybrydowa – Wyzwanie przyszłości? – wybrane zagadnienia*, http://tnij.org/hybridwarfareskoneczny (stan na 21-03-2016), s. 50.
[30] Wobec szybko rosnących zagrożeń w cyberprzestrzeni, na szczycie w Walii, NATO przyjęło deklarację o możliwości przywołania art. 5 w przypadku najpoważniejszych cyberataków.

na straty ludzkie oraz zniszczenia fizyczne. Niejasność polityki odstraszania wydaje się być w pewnym sensie logicznym rozwiązaniem w celu utrzymania potencjalnego agresora w niepewności co do tego, czy zaatakowani odpowiedzą na cyberatak[31]. Aspekt psychologiczny dobrze dostrzegalny jest jako ważny element walki z terroryzmem, ponieważ jak potwierdza K. Seger, psychologia odgrywa istotną rolę w ramach trzech komponentów walki z tym zjawiskiem[32].

Uzyskanie przewagi w cyberprzestrzeni musi jednakże opierać się na stałym zwiększaniu ochrony własnych systemów informacyjnych, monitorowaniu systemów informacyjnych potencjalnych przeciwników oraz wyszukiwaniu słabych punktów przeciwnika, w tym także przygotowania technik wtargnięcia do systemów wroga na wypadek zarządzenia akcji odwetowej. Niezwykle ważne wydaje się być przygotowanie możliwych scenariuszy odpowiedzi za pomocą informacyjnych oraz konwencjonalnych środków rażenia oraz rozwijanie metod szacowania poniesionych lub zadanych strat informacyjnych[33].

Celowym rozwiązaniem byłoby utworzenie międzynarodowej organizacji ds. bezpieczeństwa cybernetycznego, która pełniłaby rolę niezależnej globalnej platformy umożliwiającej międzynarodową współpracę oraz zawieranie traktatów o niestosowaniu cyberbroni. Tego typu organizacja mogłaby również być odpowiedzialna za prowadzenie dochodzeń w sprawie incydentów oraz zwalczanie cyberterroryzmu[34].

Obecnie żadne ze współczesnych państw nie dysponuje kompleksowymi planami obronnymi, które w sposób całościowy uwzględniają obronę przed cyberatakami, cyberterroryzmem oraz cyberwojną. Historycznie rzecz ujmując, na polu walki najpierw pojawiały się nowe metody ataków, zaś dopiero potem tworzono metody obrony przed nimi.

---

[31] A. Kacprzyk, *Politka NATO w cyberprzestrzeni: obrona i odstraszanie*, Biuletyn Polskiego Instytutu Spraw Międzynarodowych, Nr 68(1305) 2015, s. 1.

[32] Psychologia wnosi ogromny wkład w każdy z czterech elementów polityki antyterrorystycznej: od neutralizacji podłoża terroryzmu, przez ograniczanie możliwości działania terrorystów, wpływanie na ich intencje, aż po obronę bezpośrednią i minimalizowanie skutków działań terrorystycznych, Por. B. Bolechów, *Terroryzm*, Warszawa 2010, s. 336-337.

[33] A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, Roczniki Kolegium Analiz Ekonomicznych, nr 29/2013, s. 453.

[34] *Walka z cyberterroryzmem*, http://inwestycje.pl/it_ebiznes/Walka-z-cyberterroryzmem-;159775;0.html (stan na 25.01.2013).

Na temat programowania bezpieczeństwa cybernetycznego z zakresu zarządzania Internetem toczy się obecnie międzynarodowa dyskusja, w której jej uczestnicy starają się określić rolę oraz odpowiedzialność poszczególnych aktorów. Cyberzagadnienia muszą być wkomponowane w pracę ministerstw spraw zagranicznych, co niesie za sobą konieczność zmian organizacyjnych. Pomimo istnienia tematów związanych z ochroną praw człowieka czy zagadnień związanych z prowadzeniem konfliktów i kwestii ekonomicznych prowadzonych przez różne departamenty, problemy w cyberprzestrzeni łączy specyfika środowiska cyfrowego. Stąd tak ważne jest skoordynowanie horyzontalnych działań opartych o skuteczne metody komunikacji oraz ustalenie wspólnych celów[35].

Zagrożenia w cyberprzestrzeni jako problemy bezpieczeństwa

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej uwzględnia fakt, że we współczesnym środowisku bezpieczeństwa zacierają się granice pomiędzy wymiarem wewnętrznym i zewnętrznym, militarnym i pozamilitarnym, zaś globalizacja oraz wzrastająca współzależność często skutkują nieprzewidywalnością zjawisk, których zasięg nie jest już ograniczony barierami geograficznymi, systemami politycznymi i gospodarczymi[36].

Różnorodność cyberprzestępstw jest bardzo duża. Niektóre negatywne działania przestępców zostały przeniesione z codziennego życia wprost do cyberprzestrzeni, inne zaś związane są ściśle ze specyfiką Internetu. Szereg z nich zostało stypizowanych w Kodeksie Karnym[37], który wyznacza granice swobodnego poruszania się w cyberprzestrzeni. Jednak specyfika współczesnej technologii powoduje, że prawodawstwo nie nadąża z wprowadzaniem niezbędnych unormowań prawnych[38]. W polskim prawodawstwie oraz w dokumentach doktrynalnych występują istotne braki definicyjne oraz systemowe. Brakuje także naukowych opracowań w kwestiach technicznych, które zmniejszałoby podatność systemów na zagrożenia. Nie została również, jak dotąd - jasno określona odpowiedzialność za ochronę cyberprzestrzeni oraz sankcje za brak niedopełnienia obowiązków w tym zakresie. Nie istnieje także żaden spójny krajowy system, który realizowałby zadania w zakresie takiej ochrony.

---

[35] Tamże.
[36] Zob. *Strategia Bezpieczeństwa Narodowego 2014*, http://www.bbn.gov.pl/ftp/SBN%20RP.pdf, s. 17.
[37] Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (Dz. U. z 1997 nr 88 poz. 553, z późn. zm.).
[38] J. Janowski, *Elektroniczny obrót prawny*, Wolters Kluwer, 2008, s. 28.

Utrzymanie bezpieczeństwa cybernetycznego państwa wymaga sprawnego i kreatywnego działania właściwych organów oraz jego struktur – także w dziedzinie szybkiego prawodawstwa. Tymczasem trudno oprzeć się wrażeniu, że ukształtowane relacje organów państwowych mają charakter głownie kontrolny oraz blokujący[39]. Natomiast państwo powinno tworzyć spójne i przejrzyste prawodawstwo, które musi być dostosowane do nowych wyzwań, w tym - wyprzedzając fakty, nowe procesy oraz zjawiska i zapewniając prawo dla nowych obszarów funkcjonowania jego podmiotów.

Skuteczna ochrona cyberprzestrzeni przez organy państwowe wymaga stałego monitorowania dokonujących się procesów, zaś w razie potrzeby – zastosowania skutecznej, szybkiej i stanowczej reakcji ze strony wyznaczonych podmiotów. W przypadku najbardziej niebezpiecznych zachowań, niezbędna jawi się także ścisła międzynarodowa współpraca dla utworzenia wspólnych standardów odpowiedzi na agresję. Istotną rolę w programowaniu bezpieczeństwa cyberprzestrzeni współczesnego świata odgrywa ponadto współpraca organów państwowych z sektorem prywatnym.

W przypadku istotnej części społeczeństwa pozbawienie dostępu do informacji, może powodować niekorzystne zjawisko polaryzacji, jako negatywnego podziału społecznego. Nosi ono nazwę cyfrowego podziału (ang. *digital divide*)[40]. Przyczyn tego zjawiska można upatrywać zarówno w braku dostępu do zasobów informacyjnych, jak i niedostosowaniu się części społeczeństwa do korzystania z nowoczesnych technologii[41]. Problem ten stanowi jedno z największych wyzwań dla współczesnego państwa, a powody jego występowania mogą wynikać z przyczyn politycznych, technicznych lub też edukacyjnych. Efektem tego zjawiska jest występowanie różnego rodzaju upośledzeń społecznych, prowadzących do wykluczenia ekonomicznego w sferze zatrudnienia i udziału w rynku pracy, ograniczenia w życiu politycznym i społecznym, prowadząc do stopniowej utraty łączności ze społeczeństwem[42]. W szerszym kontekście cyfrowy podział jest zjawiskiem, które może

---

[39] D. Littejohn Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Helion, Gliwice 2004, s. 52.

[40] Kancelaria Senatu, *Wykluczenie cyfrowe w Polsce*, Biuro Analiz i Dokumentacji, Grudzień 2015, s. 3.

[41] U. Eco stwierdził, iż społeczeństwo w erze powszechnego dostępu do informacji podzieli się na trzy klasy: proletariuszy nie mających dostępu do komputerów i książek, uzależnionych od przekazu audiowizualnego (np. telewizji), drobnomieszczaństwa - które umie korzystać z komputera biernie oraz nomenklaturę, która wie, jak wykorzystać komputer do wykonywania analiz oraz potrafiąca odróżniać informacje wartościowe, od nic nie wnoszących (Eco 2002, s. 539-540).

[42] E. Inglot-Brzęk, *Brak dostępu do Internetu jako wskaźnik wykluczenia społecznego*, Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie, s. 375.

pociągać za sobą skutki ekonomiczne, objawiające się brakiem poczucia bezpieczeństwa, poczucia niższości czy zagubienia, poprzez ograniczony dostęp do usług publicznych, edukacji czy kultury[43].

W konsekwencji dostrzec należy konieczność adekwatnego do zwiększających się potrzeb - rozwoju infrastruktury teleinformatycznej, który umożliwiłby powszechny dostęp do Internetu - każdemu obywatelowi. Należy przy tym miejscu zaznaczyć, że powszechny dostęp oznacza dostępność technologii na jak największym obszarze, co wiąże się ze stale zwiększanymi nakładami na rozwój technologii i badania, ale również zapewniać ma akceptowalną cenę dostępu do technologii. Ponieważ jesteśmy społeczeństwem niezamożnym, aspekt ekonomiczny może stanowić barierę dla istotnej części społeczeństwa. Jak wynika z raportu Ministerstwa Administracji i Cyfryzacji *Społeczeństwo informacyjne w liczbach 2013*, w którym zebrano informacje o dostępie do sieci na terenie Polski oraz kompetencjach cyfrowych Polaków, w kraju wciąż istnieje duży odsetek gospodarstw domowych (w roku 2012 około 30%), które nie mają dostępu do Internetu. Przyczyny tego stanu są różne: w przypadku aż 60% przyczynę taką stanowiło przekonanie o braku potrzeby posiadania ww. dostępu, w dalszej części – koszty związane z dostępem (7%), niewiedza użytkowników na temat technologii (11%) oraz brak wiedzy na temat możliwości, jakie niesie za sobą posiadanie łącza z dostępem do sieci Internet[44].

Należy także zwrócić uwagę na problem niedostatecznego poziomu wykorzystania szans płynących z uczestnictwa w globalnej ewolucji informacyjnej. Uwzględniając obszar jakościowy, objawiający się w coraz mniejszym stopniu brakiem niezbędnej infrastruktury do zapewnienia dostępu do Internetu, należy zwrócić uwagę na poważny problem społeczny, polegający na braku dostrzegania szans posiadania dostępu do niego przez część społeczeństwa lub też braku umiejętności w wykorzystywaniu potencjału tego medium. W przypadku 59% gospodarstw, przyczyną tego stanu było przeświadczenie o zbędności korzystania z sieci, co wskazywać mogłoby na niską świadomość potencjalnych użytkowników. Niekorzystnym zjawiskiem okazuje się też sposób wykorzystywania Internetu, który ogranicza się tylko do wysyłania i odbierania poczty elektronicznej (53%) czy

[43] E. Kina, *Rozwój zrównoważony w społeczeństwie informacyjnym – szanse i zagrożenia*, [w:] Red. R. Grądzki, M. Mateun, *Rozwój zrównoważony – zarządzanie innowacjami ekologicznymi*, Politechnika Łódzka, Łódź 2009, s. 11.
[44] *Społeczeństwo informacyjne w liczbach 2013*, : https://mac.gov.pl/wp-content/uploads/2013/09/Spoleczenstwo-informacyjne-w-liczbach-2013.pdf, s. 15.

wyszukiwania informacji na temat towarów i usług (50%). Wśród osób w wielu 12-15 lat, głównym celem korzystania z sieci były fora dyskusyjne, komunikatory oraz sieci społecznościowe (odsetek ten wyniósł aż 85%). W przypadku osób w wieku 16-74 lata, odsetek osób korzystających z administracji publicznej w sieci wyniósł jedynie 27%. Głównym celem wykorzystania Internetu było wyszukiwanie informacji na stronach, nie zaś załatwianie spraw. Administracja elektroniczna w swoim założeniu ma zapewniać oszczędność czasu i bieżące śledzenie zmian w przepisach i aktach prawnych. Słaby wynik wykorzystania tych narzędzi może wynikać z braku dostępnych usług w wielu obszarach e-administracji oraz niewystarczające umiejętności użytkowników[45].

W kontekście istniejących zagrożeń, niezmiernie ważna jest także szeroko rozumiana edukacja społeczeństwa z zakresu bezpieczeństwa,[46] ponieważ dobra komunikacja pomiędzy państwem a obywatelem wywiera istotny wpływ na racjonalne korzystanie z praw obywatelskich[47]. Powszechny dostęp do informacji jest dla społeczeństwa zjawiskiem niezwykle pozytywnym, dając wolność, dzięki czemu, jednostka lub zbiorowość może decydować o własnym losie[48].

Dużym wyzwaniem i zarazem formą najbardziej zbliżoną do tradycyjnych działań dyplomatycznych jest wzmacnianie ochrony praw człowieka i obywatela. Działania w tym obszarze są jednym z podstawowych zadań w państwie demokratycznym, stąd ważne jest takie prowadzenie polityki, by prawa obowiązujące w świecie realnym (prawo do wolności słowa, wymiany poglądów czy prawo do prywatności), przestrzegane były także w cyberprzestrzeni[49].

Należy jednak podkreślić, że programowanie bezpieczeństwa cyberprzestrzeni nieuchronnie wiązać się musi z potrzebą ograniczenia niektórych praw wolności jednostki, co w społeczeństwie może budzić uzasadniony niepokój. Prawodawca, walcząc z negatywnymi zjawiskami w cyberprzestrzeni, zmuszony jest ingerować w sferę wolności i praw człowieka. Stąd pragnienie bezpieczeństwa oraz zagwarantowanie wolności są wartościami, które może

---

[45] Tamże.
[46] Zob. http://oapuw.pl/relacja-z-seminarium-pt-cyberbezpieczenstwo-polski-15-10-2013 (stan na 10-02-2016).
[47] K. Jakubowicz, *Społeczeństwo obywatelskie, niezależna sfera publiczna i społeczeństwo informacyjne: niemożliwe połączenie*, [w:] *Rewolucja informacyjna i społeczeństwo. Niektóre trendy, zjawiska i kontrowersje*, red. L. W. Zacher, s. 198.
[48] J. Kisielnicki, *Cyberterroryzm jako element zagrożenia współczesnej cywilizacji*, WSIZiA, Warszawa 209, s. 23.
[49] Tamże.

być trudno pogodzić. Z drugiej strony, poczucie zagrożeniem w kontekście najnowszych wydarzeń związanych z terroryzmem lub innymi zagrożeniami sprawia, że użytkownicy cyberprzestrzeni tracą pierwotny impet dążenia do bezgranicznej wolności na rzecz zwiększenia bezpieczeństwa[50].

Szereg państw, w tym Polska - może skorzystać z doświadczenia innych państw, tworząc ochotniczą cyberarmię na wzór istniejących struktur w Estonii i Łotwie, gdzie formacje te zostały powołane po atakach z 2007 roku. Cyberarmie tych państw składają się z cywilnych informatyków, na co dzień pracujących w branży IT, zaś pozazawodowo stale rozwijających własne umiejętności w dziedzinie cyberbezpieczeństwa. W czasie cyberwojny, podlegają oni dowództwu wojskowemu, a ich zadaniem jest najczęściej ochrona przed atakami na infrastrukturę krytyczną państwa i instytucje takie jak banki czy urzędy. Tego typu formacja organizuje także akcje uświadamiające i szkolenia użytkowników, zaś przypadku realnych cyberataków, współpracuje także z wojskowymi zespołami cyberbezpieczeństwa[51].

Postępująca informatyzacja kraju sprawia, że konieczne jest tworzenie skutecznych rozwiązań profilaktycznych, technicznych i organizacyjno-prawnych, pozwalających chronić jego obywateli. Odpowiedzialność za wzmacnianie bezpieczeństwa cyberprzestrzeni nie może więc spoczywać wyłącznie na władzach, lecz część zobowiązań z tego zakresu powinna zostać przeniesiona na barki społeczeństwa, sektora prywatnego oraz organizacji pozarządowych[52].

W lutym 2016 roku Ministerstwo Cyfryzacji opublikowało międzyresortowy dokument *Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, który zawiera propozycje podziału kompetencji głównych podmiotów, założenia budowy systemu ochrony cyberprzestrzeni RP oraz projekt proponowanej struktury krajowego systemu cyberbezpieczeństwa. Ministerstwo zakłada trzypoziomowy podział struktury cyberbezpieczeństwa na poziomie strategicznym, operacyjnym oraz technicznym. Efektem tego zapowiadana jest wielopoziomowa struktura reagowania na incydenty, z jasno

[50]W. Lis, *Bezpieczeństwo w cyberprzestrzeni w ujęciu prawnokarnym – wybrane zagadnienia*, Rocznik Bibliologiczno – Prasoznawczy, tom 6/17, Kielce 2014, s. 254-255.
[51]Zob.http://finanse.wp.pl/kat,1033701,title,Ekspert-Polska-powinna-powolac-ochotnicza-cyberarmie,wid,16718979,wiadomosc.html?ticaid=116aae (stan na: 12-02-2016).
[52] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski*, BBN, s. 136.

określonymi kompetencjami, strukturą adekwatną do występujących zagrożeń oraz czytelnymi procedurami reagowania[53]. Założenia te dają dużą nadzieję na modyfikację dotychczasowego stanu bezpieczeństwa, wynikającego zarówno z braku jednolitego ustawodawstwa regulującego instytucjonalno-prawny system ochrony cyberprzestrzeni, rozproszonego charakteru ochrony, braku jednoznacznych procedur reagowania na zagrożenia, niedostatecznie występujących ćwiczeń z zakresu ochrony cyberprzestrzeni, całkowitego braku funkcjonowania szacowania ryzyk, braku wspólnej wizji systemowej oraz kluczowego ośrodka decyzyjnego – co zostało szczegółowo opisane w wynikach kontroli NIK[54].

Podsumowanie

Zagrożenia społeczeństwa informacyjnego pojawiają się w różnych kategoriach, które często wzajemnie na siebie oddziałują. Oddziaływanie to może mieć istotny wpływ na bezpieczeństwo społeczeństwa zarówno w sferze informacyjnej, jak i technicznej – w tym także poprzez mechatroniczne mechanizmy wykonawcze. Wynika to między innymi z wykorzystania cyberprzestrzeni do przesyłania parametrów sterujących dla sterowników stosowanych w wielu obszarach życia, przez co efekty procesów wykonawczych mogą modyfikować rzeczywistość – a tym samym oddziaływać na procesy myślowe oraz zmieniać zachowania społeczne.

Kluczową kwestią w zapewnieniu bezpieczeństwa cybernetycznego jest przede wszystkim zrozumienie wpływu bezpieczeństwa tego obszaru na całokształt funkcjonowania państwa – także w relacjach międzynarodowych. Istotne jest przy tym zrozumienie wpływu cyberprzestrzeni także na relacje międzynarodowe, diagnoza najważniejszych problemów, zmapowanie najistotniejszych aktorów oraz odszyfrowanie ról, jakie ci uczestnicy odgrywają.

Niezbędna jest budowa zintegrowanego Systemu Bezpieczeństwa Narodowego także w sferze kultury bezpieczeństwa wszystkich podmiotów tworzących podsystemy związane z bezpieczeństwem informacyjnym. Możliwości doskonalenia efektywności Systemu

[53] *Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Ministerstwo Cyfryzacji, luty 2016.
[54] *Informacja o wynikach kontroli Realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, NIK, 2015.

Bezpieczeństwa Narodowego należy także upatrywać w wykorzystaniu potencjału społeczeństwa – przede wszystkim w licznie funkcjonujących w Polsce organizacjach wchodzących w skład tzw. „trzeciego sektora"[55], w tym zwłaszcza coraz częściej tworzonych w jego ramach organizacji proobronnych[56]. Zastosowanie inżynierii społecznej dla dobra społeczeństwa[57], które obejmowałaby wpajanie oraz wzmacnianie pozytywnych idei w procesie wychowania, jak i działalność na rzecz zapewnienia bezpieczeństwa narodowego, przynieść może znaczące efekty – zwłaszcza w przypadku obrony narodowej.

Polska musi stać się także aktywnym aktorem na arenie międzynarodowej w obszarze działań dotyczących cyberprzestrzeni, a największy priorytet muszą otrzymać kwestie związane z cyberbezpieczeństwem. Obecnie, na wielu forach międzynarodowych, jesteśmy zbyt bierni lub często – nieobecni[58].

Bibliografia

1. Leszczyńska M., *Współczesny model rozwoju społecznego z perspektywy rewolucji informacyjnej*, Katedra Teorii Ekonomii i Stosunków Międzynarodowych, Uniwersytet Rzeszowski.
2. Majta M., *Rola informacji w kształtowaniu nowych społeczeństw*, EBIB, Wrocław 2005.
3. Red. Witkowska M., Cholawo – Sosnowska K., *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*.
4. Grabowski M., Zając A., *Dane, informacja, wiedza – próba definicji,* Katedra Informatyki Akademii Ekonomicznej w Krakowie.
5. Masuda Y., *The Information Society as Post-Industrial Society*, cyt. Za: P. Sienkiewicz, *Masowe komunikowanie w społeczeństwie informacyjnym*, [w:] *Mass media w systemie komunikacji społecznej w Polsce*, red. A. Kudłaszczyk, A. Małkiewicz, R. Karpiński.
6. Inglot-Brzęk E., *Brak dostępu do Internetu jako wskaźnik wykluczenia społecznego*, Katedra Nauk Społecznych Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie.

[55] Jak w teorii podziału nowoczesnego państwa określa się ogół organizacji pozarządowych (w odróżnieniu od dwóch pozostałych jego głównych sektorów: państwowego oraz rynkowy).

[56] W odniesieniu do oddolnych, niesformalizowanych oraz spontanicznych inicjatyw obywatelskich używane bywa także określenie „czwarty sektor".

[57] Jak podkreśla A. Podgórecki, inżynieria społeczna stosowana powinna być wyłącznie do realizacji celów ocenianych jako społecznie wartościowe. Zob. A. Podgórecki, *Logika praktycznego działania*, [w:] Socjotechnika, t. 2, A. Podgórecki (red.) Książka i Wiedza, Warszawa 1968, s. 47.

[58] Tamże.

7. Red. Madej M., Terlikowski M., *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009.
8. Sobol E., *Mały Słownik Języka Polskiego*, PWN, Warszawa 1993.
9. Oleński J., *Ekonomika informacji*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2001.
10. Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski*, BBN.
11. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Adam Marszałek, Toruń 2005.
12. Targowski A., *Informatyka – klucz do dobrobytu*, PIW, Warszawa 1971.
13. Haber L. H., *Społeczeństwo informacyjne – wizja czy rzeczywistość*?, II ogólnopolska konferencja naukowa, Kraków, 30 maja 2003.
14. Pod red. Świątkowska J., *Bezpieczeństwo infrastruktury krytycznej. Wymiar teleinformatyczny*, Instytut Kościuszki, Kraków 2014.
15. Maj M., *Debata na temat strategii obrony cyberprzestrzeni*, Dziennik Gazeta Prawna, nr 5.
16. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (Dz. U. z 1997 nr 88 poz. 553, z późn. zm.).
17. Janowski J., *Elektroniczny obrót prawny*, Wolters Kluwer 2008.
18. Kina E., *Rozwój zrównoważony w społeczeństwie informacyjnym – szanse i zagrożenia*, [w:] Red. R. Grądzki, M. Mateun, *Rozwój zrównoważony – zarządzanie innowacjami ekologicznymi*, Politechnika Łódzka, Łódź 2009.
19. Littejohn Shinder D., Tittel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Helion, Gliwice 2004.
20. Jakubowicz K., *Społeczeństwo obywatelskie, niezależna sfera publiczna i społeczeństwo informacyjne: niemożliwe połączenie*, [w:] *Rewolucja informacyjna i społeczeństwo. Niektóre trendy, zjawiska i kontrowersje*, red. L. W. Zacher.
21. Kisielnicki, *Cyberterroryzm jako element zagrożenia współczesnej cywilizacji*, WSIZiA, Warszawa 2009.
22. Lis W., *Bezpieczeństwo w cyberprzestrzeni w ujęciu prawnokarnym – wybrane zagadnienia,* Rocznik Bibliologiczno – Prasoznawczy, tom 6/17, Kielce 2014.
23. Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, Roczniki Kolegium Analiz Ekonomicznych, nr 29/2013.
24. Littejohn Shinder D., Tittel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice.
25. *Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Ministerstwo Cyfryzacji, luty 2016.
26. *Informacja o wynikach kontroli Realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, NIK.
27. Podgórecki A., *Socjotechnika*, t. 2, Książka i Wiedza, Warszawa 1968.

Netografia

1. *Encyklopedia PWN*, http://encyklopedia.pwn.pl
2. Gajewicz M., *Społeczeństwo informacyjne – problemy (zagadnienia)*, http://www.id.uw.edu.pl/~mgajlewicz/SpoleczenstwoInformacyjne.
3. Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, Roczniki Kollegium Analiz Ekonomicznych nr 29/2013, Wydział Humanistyczny Uniwersytet Pedagogiczny w Krakowie, http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z29_30.pdf.
4. Liedel K., *Bezpieczeństwo informacyjne jako element bezpieczeństwa narodowego*, http://www.liedel.pl/?p=13.
5. Krajowa Rada Radiofonii i Telewizji, *Społeczeństwo informacyjne w Polsce – Wstęp do formułowania założeń polityki Państwa*, Warszawa 1996, http://kbn.icm.edu.pl/pub/info/dep/spo.html.
6. Zob. *Strategia Bezpieczeństwa Narodowego 2014*, http://www.bbn.gov.pl/ftp/SBN%20RP.pdf.
7. *Społeczeństwo informacyjne w liczbach 2013*, https://mac.gov.pl/wp-content/uploads/2013/09/Spoleczenstwo-informacyjne-w-liczbach-2013.pdf.
8. *Hybrid war – does it even exist?*, http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm.
9. Skoneczny L., *Wojna hybrydowa – Wyzwanie przyszości? – wybrane zagadnienia*, http://tnij.org/hybridwarfareskoneczny.
10. http://finanse.wp.pl/kat,1033701,title,Ekspert-Polska-powinna-powolac-ochotnicza-cyberarmie,wid,16718979,wiadomosc.html?ticaid=116aae.
11. *Walka z cyberterroryzmem*, http://inwestycje.pl/it_ebiznes/Walka-z-cyberterroryzmem-;159775;0.html.

Spis treści