dr Magdalena El Ghamari[a)]*

[a)]*Collegium Civitas, Centrum Badań nad Ryzykami Społecznymi i Gospodarczymi CC, Pracownia Bezpieczeństwa Kulturowego / Collegium Civitas, Centre for Social and Economic Risk Research, Cultural Security Workshop*
**Autor korespondencyjny/Corresponding author: elghamari@op.pl*

Ochrona cyberprzestrzeni – wyzwanie naszych czasów?

Cyberspace Protection – the Challenge of Our Time?

Защита киберпространства – вызов нашего времени?

ABSTRAKT

Cel: Głównym celem niniejszych rozważań jest identyfikacja ochrony cyberprzestrzeni w świetle Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2014 roku, polskiej legislacji w zakresie ochrony przed cyberprzestępczością, polityki ochrony cyberprzestrzeni oraz postawy Unii Europejskiej wobec cyberterroryzmu.
Wprowadzenie: Pojęcia takie jak bezpieczeństwo Polski, cyberterroryzm, kontrola operacyjna, służby mundurowe czy służby specjalne nie schodzą z medialnych czołówek. Nie jest to jednak efekt potrzeby chwili, medialności, aktualnej sytuacji międzynarodowej czy zmian organizacyjnych, a niestety efekt wieloletnich zaniedbań w tym ważnym aspekcie, jakim jest symulowanie, prognozowanie i reagowanie na potencjalne zagrożenia bezpieczeństwa. Wraz z postępem cywilizacyjnym ostatniej dekady, nastąpiły zmiany technologiczne, społeczne, polityczne, czy kulturowe. Jednym z ważniejszych elementów powyższych zmian jest rozwój dotyczący globalnych procesów wymiany, a także przekazywania i przetwarzania informacji. Daje to korzyści dla wielu państw, jednocześnie powoduje uzależnienie od technologii informatycznych. Wspomniane zmiany niosą ze sobą jednak pewnego rodzaju zagrożenia dla państw, określane mianem cyberterroryzmu. Mówi się o tzw. wojnie informacyjnej, która oznacza wszelkie działania mające na celu uzyskanie przewagi informacyjnej poprzez wpływanie na informacje, procesy informacyjne, systemy informatyczne oraz sieci komputerowe przeciwnika przy jednoczesnym zapewnieniu ochrony własnym zasobom informacyjnym. Została ona zdefiniowana już wcześniej, jednak w erze Internetu zyskała na znaczeniu.
Projekt i metody: Do określenia istoty ochrony cyberprzestrzeni przedstawiono rozważania dotyczące metodologicznych podstaw badanego obszaru, w dziedzinie bezpieczeństwa cyberprzestrzeni Polski, NATO oraz Unii Europejskiej. Wykorzystano metodę monograficzną, analizę materiałów źródłowych oraz weryfikację danych zastanych.
Wyniki: Na podstawie przeprowadzonych badań ustalono, że wszelkie działania, decyzje podejmowane na mocy Konwencji Rady Europy o cyberprzestępczości są zgodne z innymi aktami prawa, lecz również mają na względzie poszanowanie praw człowieka, zgodnie z którymi ma on prawo do wolności, w tym możliwość głoszenia swoich opinii, czy wyrażania własnych poglądów. Współpraca państw na arenie międzynarodowej w obszarze cyberprzestrzeni ma za zadanie ujednolicanie aktów prawnych, wszelkiego typu regulacji, w celu łatwiejszego i skoordynowanego działania w zakresie cyberbezpieczeństwa. Normy prawne państw, które są ze sobą skoordynowane, ułatwiają namierzanie, ściganie i karanie cyberprzestępców.
Wnioski: Wnioski przedstawione w artykule pozwalają określić działania mające na celu identyfikację ryzyk wynikających z zagrożeń w cyberprzestrzeni i jego ustawodawstwa.
Słowa kluczowe: cyberprzestrzeń, bezpieczeństwo, współpraca, wojna informacyjna, służby mundurowe, wymiana informacji, cyberterroryzm, cyberataki
Typ artykułu: z praktyki dla praktyki

Przyjęty: 04.12.2017; Zrecenzowany: 05.01.2018; Zatwierdzony: 10.04.2018;
Proszę cytować: BiTP Vol. 49 Issue 1, 2018, pp. 24–33, doi: 10.12845/bitp.49.1.2018.2;

ABSTRACT

Aim: The main purpose of these considerations is to identify the cyberspace protection issues in the light of the National Security Strategy of the Republic of Poland of 2014, Polish legislation in the field of cybercrime protection, the cyberspace protection policy and the attitude of the European Union to cyber-terrorism.
Introduction: Concepts such as the security of Poland, cyberterrorism, operational control, uniformed services or special services have remained the front-page story. However, this is not the outcome of the current need, media coverage, current international circumstances or organizational changes, but rather the effect of many years of neglecting this important aspect of simulation, forecasting and reacting to potential security threats. Along with the civilization development in the last decade, technological, social, political or cultural changes have occurred. One of the most important elements of the above changes is the development concerning global processes of information exchange, as well as information transfer and processing. While providing

benefits to many countries, it causes dependence on IT technologies. The reference changes entail a kind of threat to the states, which isreferred to as cyber-terrorism. One can speak of the so-called information war, which means all actions aimed at gaining an informational advantage by influencing information itself, information processes, IT systems and computer networks of the opponent, while ensuring the protection of one's own information resources. This term was coined earlier, but it grew in importance in the Internet age.
Project and methods: To determine the essence of cyberspace protection, considerations were made regarding the methodological foundations of the studied area, in the field of security of the Polish,European Union and NATO`s cyberspace. A monographic method was employed, together with the analysis of source materials and verification of existing data.
Results: On the basis of the conducted research, it was found that all the actions and decisions taken under the Council of Europe Convention on Cybercrime are consistent with other legal acts, as well as respect human rights, including the right of freedom and the opportunity to express one's opinions and views. International cooperation between in the area of cyberspace is aimed at harmonising legal acts and all kinds of regulations, in order to facilitate and coordinate actions in the field of cyber security. The legal standards of different countries, when they are coordinated with one another, make it easier to track, prosecute and punish cybercriminals.
Conclusions: The conclusions presented in this paper enable us to define the actions needed to identify the actual risks resulting from cyberspace threats, along with related legislation.
Keywords: cyberspace, security, cooperation, information war, uniformed services, information exchange, cyber-terrorism, cyber attacks
Type of article: best practice in action

Received: 04.12.2017; Reviewed: 05.01.2018; Accepted: 10.04.2018;
Please cite as: BiTP Vol. 49 Issue 1, 2018, pp. 24–33, doi: 10.12845/bitp.49.1.2018.2;

АННОТАЦИЯ

Цель: Основной целью этих размышлений является определение защиты киберпространства в свете Стратегии Национальной Безопасности Республики Польша от 2014 года, польского законодательства в области защиты от киберпреступности, политики защиты киберпространства и отношения Европейского Союза к кибертерроризму.
Введение: Такие понятия, как безопасность Польши, кибертерроризм, оперативный контроль, силовые структуры или специальные службы, очень часто присутствуют в заголовках СМИ. Однако, это не является следствием необходимости, заинтересованности СМИ, текущей международной ситуации или организационных изменений, а, к сожалению, последствием многолетнего пренебрежения такими важными аспектами, как моделирование, прогнозирование и реагирование на потенциальные угрозы безопасности. Наряду с развитием цивилизации на протяжении последнего десятилетия произошли технологические, социальные, политические и культурные изменения. Одним из наиболее важных составляющих вышеуказанных изменений является развитие, связанное с глобальными процессами обмена, передачи и обработки информации. Оно благотворно для многих государств, но в то же время вызывает зависимость от информационных технологий. Однако, вышеперечисленные изменения несут определённую угрозу для стран, именуемую кибертерроризмом. Речь идёт о так называемой информационной войне, которая представляет собой разного рода действия, направленные на получение информационного превосходства с помощью влияния на информацию, информационные процессы, ИТ-системы и компьютерные сети противника при обеспечении защиты собственных информационных ресурсов. Определение информационной войны существовало давно, но в эпоху Интернета оно приобрело большее значение.
Проект и методы: С целью определения сути значения защиты киберпространства были представлены идеи, касающиеся методологических основ изучаемой области в сфере безопасности киберпространства в Польше и НАТО. Был использован монографический метод, метод анализа исходных материалов и проверки имеющихся данных.
Результаты: На основе проведенных исследований было установлено, что все действия и решения, принятые исходя из Конвенции Совета Европы о киберпреступности согласованы с другими правовыми актами и учитывают права человека, согласно которым он имеет право на свободу, в том числе возможность высказывания своего мнения или выражения своих собственных взглядов. Сотрудничество стран на международной арене в области киберпространства направлено на гармонизацию законодательных актов, разного рода правил, с целью упрощения и координации действий в области кибербезопасности. Согласование правовых норм разных стран облегчает отслеживание, уголовное преследование и наказание киберпреступников.
Выводы: Выводы, представленные в статье, позволяют определить действия, направленные на выявление рисков, связанных с угрозами в киберпространстве, и соответствующее законодательство.
Ключевые слова: киберпространство, безопасность, сотрудничество, информационная война, силовые структуры, обмен информацией, кибертерроризм, кибератаки
Вид статьи: с практики для практики

Принята: 04.12.2017; Рецензирована: 05.01.2018; Одобрена: 10.04.2018;
Просим ссылаться на статью следующим образом: BiTP Vol. 49 Issue 1, 2018, pp. 24–33, doi: 10.12845/bitp.49.1.2018.2;

Wprowadzenie

Już dekadę temu J. Pilżys wykazał istnienie 109 definicji terroryzmu, w których pojawiają się takie określenia, jak: „przemoc, siła (83%); polityczny (65%); strach, podkreślenie terroru (51%); groźba (47%); (psychologiczne) skutki i (przewidywane) reakcje (41,5%); rozróżnienie ofiara – cel (37,5%); celowa, planowana, systematyczna, zorganizowana akcja (32%); metody walki,

strategia, taktyka (30,5%); nienormalność, konflikt z przyjętymi regułami, brak humanitarnych ograniczeń (30%); wymuszanie, zniewolenie, powodowanie uległości (28%); aspekt rozgłosu, reklamy (21,8%)" [1].

Wspomniane definicje nie obrazują w pełni omawianego zjawiska. Dzięki analizie można dostrzec w nich wspólne elementy, którymi są:

1) stosowanie przemocy i siły,
2) skutki i reakcje psychologiczne przeprowadzonych działań,
3) wywoływanie strachu,
4) groźbę jako element zastraszania,
5) polityczny aspekt czynu [2].

Pojęcie „cyberterroryzm" nadal stwarza wiele problemów i wątpliwości. Za jego twórcę uważa się B. Collina, który w latach 80. połączył w jeden wyraz słowa „terroryzm" i „cyberprzestrzeń". Według niego cyderterroryzm jest to „świadome wykorzystanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia terrorystycznej akcji" [3]. Postrzeganie tego zjawiska można podzielić na trzy grupy: „pojęcia prezentowane w mediach; definicje obowiązujące w gronie specjalistów; definicje stworzone na użytek innych dziedzin działalności człowieka w dziedzinie informatyki" [4]. Według D. Denning cyberterroryzm jest to „(...) groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołują powszechne poczucie strachu" [5]. Z kolei J. Lewis pojęcie to określa jako „(...) wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe, itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań" [6].

Podczas definiowania pojęć związanych z atakami terrorystycznymi dotyczącymi systemów informatycznych należy również zwrócić uwagę na pojęcie cyberprzestępczości, która stanowi coraz większe zagrożenie współczesnego świata – świata na wysokim poziomie zinformatyzowania oraz usieciowienia.

Cyberprzestępczość wiąże się z cechą transgraniczności, poprzez możliwość przekraczania wszelkich barier (na przykład państw).Cyberprzestrzeń w kontekście niniejszych rozważań oznacza przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.

„Bezpieczeństwo sieci i systemów informatycznych", inaczej „cyberbezpieczeństwo" lub „bezpieczeństwo teleinformatyczne" oznacza odporność systemów i sieci teleinformatycznych, przy określonym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych bądź przetwarzanych w nich danych lub oferowanych w nich usług.

Bezpieczeństwo cyberprzestrzeni we współczesnych uwarunkowaniach i przy stale postępującym zagrożeniu cyberprzestrzeni jest niezwykle istotnym wyzwaniem, a także powinnością. W związku z powyższym istnieje potrzeba jego rozwijania i angażowania w ten rozwój państw oraz międzynarodowych, krajowych, regionalnych organizacji. Niezwykle ważna jest skoordynowana współpraca, która ma za zadanie zapewnić państwu skuteczną ochronę, poprzez stosowanie nowych technologii i technik niwelujących zagrożenie, dostosowanych do zmian, jakie zachodzą w cyberatakach.

Głównymi wątkami niniejszego artykułu, w kontekście najnowszych dyskusji w metodologii badań naukowych, jest identyfikacja ochrony cyberprzestrzeni w świetle Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2017 roku oraz charakterystyka podejścia badawczego, które pozwalałoby w adekwatny sposób prowadzić badania w zakresie bezpieczeństwa cyberprzestrzeni wybranych aktów normatywnych, jako jednego z elementów szeroko rozumianego bezpieczeństwa.

Trudność tkwi przede wszystkim w tym, że nauki o bezpieczeństwie obejmują zróżnicowane aspekty, które w bardziej tradycyjnym ujęciu odpowiadają konglomeratowi różnych dyscyplin, ale jednocześnie oczekuje się – m.in. ze względu na rekomendacje na podstawie badań – że wynik będzie miał charakter spójny i jednolity. Tego rodzaju problem obserwuje się nie tylko w badaniach nad bezpieczeństwem, lecz – z uwagi na rosnącą złożoność podejść do przedmiotu badania – również w przypadku wielu dyscyplin w obrębie szeroko rozumianych badań społecznych. Odzwierciedleniem tej tendencji jest szereg studiów nad „interdyscyplinarnością", „mutli-dyscyplinarnością" czy „trans-dyscyplinarnością" w badaniach nad bezpieczeństwem [7].

W niniejszym artykule autorka zawęża rozważania dotyczące metodologicznych podstaw badanego obszaru do badań w dziedzinie bezpieczeństwa cyberprzestrzeni Polski oraz Unii Europejskiej i NATO. Umożliwiają one szerokie postrzeganie problematyki obrony oraz ochrony cyberprzestrzeni, a stosowane w nich metody i techniki badawcze mają zastosowanie w pozostałych naukach społecznych.

Głównym celem niniejszych rozważań jest identyfikacja ochrony w świetle Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, polskiej legislacji w zakresie ochrony cyberbezpieczeństwa polityki ochrony cyberprzestrzeni oraz postawy Unii Europejskiej wobec cyberterroryzmu.

Ochrona cyberprzestrzeni powinna być realizowana przez sprecyzowane działania poszczególnych krajów oraz organizacji zajmujących się ową tematyką. Ważne jest również bezpieczeństwo w obszarze zarządzania kryzysowego na szczeblu państwa. Wśród metod i sposobów walki z zagrożeniami cyberprzestrzeni wyróżnia się metody fizyczne, specjalne, techniczne, a także organizacyjno-administracyjne. Metody użyte w sposób poprawny są skuteczne i służą do ochrony informacji oraz systemów teleinformatycznych. Mogą one efektywnie bronić cyberprzestrzeń przed zagrożeniami, na które jest ona narażona. Skuteczne działanie powyższych metod jest zauważalne pod warunkiem ich kompleksowego stosowania.

 ISSN 1895-8443

W badaniach związanych z cyberbezpieczeństwem „przestrzeń online" staje się ważnym aspektem badań w obszarze nauk społecznych. Coraz częstsze ataki w sieci ukazują, że ryzyko potencjalnych zagrożeń ukierunkowanych na bezpieczeństwo stało się faktem, przez co właśnie skuteczna ochrona i świadomość zagrożenia jest wyzwaniem stojącym zarówno przed Polską, jak i jej obywatelami. Pieczę nad bezpieczeństwem cybernetycznym sprawuje administracja państwa przy pomocy podmiotów, które zostały specjalnie powołane do tego zadania.

Zapewnienie bezpieczeństwa cyberprzestrzeni stało się dla międzynarodowych organizacji, kooperacji w skali całego globu i poszczególnych regionów zadaniem priorytetowym. Doskonałym przykładem są działania, jakie podejmuje administracja Unii Europejskiej czy Paktu Północnoatlantyckiego wraz z państwami członkowskimi powyższych organizacji.

NATO odgrywa istotną rolę w niwelowaniu cyberterroryzmu. W 2002 roku na szczycie w Pradze zostały podjęte pierwsze decyzje NATO, które dotyczyły właśnie kwestii cyberobrony. Wówczas przyjęty został program cyberobrony, *The Cyber Defense Program*, a także program dotyczący reakcji na pojawiające się komputerowe incydenty *The Computer Incident Response Capability*. Sześć lat później w styczniu 2008 roku w Brukseli NATO podjęło decyzję o przyjęciu strategii Obrony Cyberprzestrzeni, *The policy on cyber defense* [8]. Swoją działalność na rzecz obrony cyberprzestrzeni NATO kształtowało także w roku 2010, kiedy to na szczycie w Lizbonie, została przyjęta Koncepcja Strategiczna NATO. Zwalczanie cyberterroryzmu stało się celem priorytetowym dla działań politycznych oraz militarnych państw członkowskich. W punkcie 12 Koncepcji zapisano, że „Cyberataki stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej: mogą one sięgnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności. Źródłem takich ataków mogą być obce siły wojskowe i służby wywiadowcze, zorganizowane grupy przestępcze, terrorystyczne i/lub grupy ekstremistyczne" [9]. Koncepcja wyodrębniła odpowiednie struktury, którym zostało powierzone zadanie obrony przed cyberatakami w zawartym „Sojuszu". W Programie zostały wyznaczone trzy cele:

1) **wspieranie poszczególnych sojuszników** – państwa uczestniczące w sojuszu mogą otrzymać pomoc, jednak muszą one spełniać wyznaczone warunki, procedury;
2) **badania i szkolenia** – dopracowano warunki i zasady, według których prowadzona jest obrona w sieci przed atakami cyberterrorystycznymi. Wyciągnięto wnioski i zauważono potrzebę utworzenia jednolitych zasad i działań dla wszystkich państw Sojuszu. Zgłoszono chęć szkolenia i edukowania na temat obrony przy pomocy Centrum Kompetencyjnym w Tallinie;
3) **współpraca z partnerami w postaci koordynacji działań i doradztwa** – podkreślono, iż niezwykle ważna jest skoordynowana współpraca państw Sojuszu. Istotną rolę odrywa także podejmowanie wspólnych działań z sektorem prywatnym i akademickim.

Według zasad Sojuszu niezbędne jest również organizowanie ćwiczeń z zakresu cyberataków. Tego rodzaju działania są szansą sprawdzenia swoich możliwości nie tylko dla państw członkowskich Sojuszu, ale również państw partnerskich, służb wojskowych i specjalnych. Działania te mają usprawniać reagowanie na pojawiające się zagrożenia, zwalczanie ich, a także nawiązywanie międzynarodowej współpracy i wymianę informacji na różnych szczeblach. Przeciwdziałanie cyberterroryzmowi stało się jednym z priorytetów dla wspólnych działań politycznych i militarnych sojuszników. W punkcie 12 zapisano: Ataki w cyberprzestrzeni stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne – biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej. Mogą one osiągnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności. Źródłem takich ataków mogą być obce siły wojskowe i służby wywiadowcze, zorganizowane grupy przestępcze, terrorystyczne i/lub grupy ekstremistyczne". Zgodnie z Koncepcją wdrażaniem postanowień obrony przed cyberatakami w Sojuszu zajmują się właściwe, wymienione w dokumencie struktury NATO.

W lutym 2012 roku powstało NATO Computer Incident Response Capability w skrócie – NCIRC. Projekt ten kosztował 58 mln euro i z założenia obejmuje wszystkie sieci komputerowe państw NATO programem wspólnej, scentralizowanej ochrony przed włamaniami i atakami. Pierwotnie NCIRC miało osiągnąć pełną gotowość do działania do końca 2012 roku.

Działania w tym obszarze prowadzi także Unia Europejska; jako zjednoczenie państw współpracujących ze sobą w różnym zakresie, zajmuje się również kwestią cyberataków.

W celu identyfikacji i symulowania potencjalnych zagrożeń cyberbezpieczeństwa powstał dokument Strategia bezpieczeństwa cyberprzestrzeni Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, który został opublikowany 7 lutego 2013 roku. Dokument ten przedstawia całościowe spojrzenie na wspólne dla wszystkich krajów członkowskich Unii Europejskiej kwestie bezpieczeństwa w sieci. Strategia zawiera wizję Unii Europejskiej dotyczącą efektywnego zapobiegania powstającym zakłóceniom i atakom, a także reakcji na tego rodzaju ataki. Ma na celu zapewnienie i promowanie wolności, demokracji oraz pomocy w utrzymaniu bezpiecznego rozwoju gospodarki cyfrowej. Działania Strategii są nakierowane na zapewnienie bezpieczeństwa systemów informacyjnych i niwelowanie cyberprzestępczości. Poprzez realizację strategii ma nastąpić wzmocnienie polityki międzynarodowej Unii Europejskiej w zakresie cyberbezpieczeństwa.

Bezpieczeństwo cyberprzestrzeni według unijnej strategii składa się z 5 priorytetów, do których zaliczają się:

- „osiągnięcie odporności w dziedzinie bezpieczeństwa cyberprzestrzeni;
- radykalne ograniczenie cyberprzestępczości;
- opracowanie polityki obrony cyberprzestrzeni i rozbudowa zdolności w dziedzinie bezpieczeństwa cyberprzestrzeni

o w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (w skrócie: WPBiO);
– rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cyberprzestrzeni;
– ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE" [10].

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej

Strategia została podpisana 5 listopada 2014 roku przez Prezydenta Rzeczypospolitej Polskiej Bronisława Komorowskiego, zastępując tym samym Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2007 roku. Strategie z 2007 i 2014 roku różnią się przede wszystkim rodzajem zagrożeń, jakie mogą występować. Nowo podpisany dokument podkreśla rolę Rosji, która poprzez podejmowane działania militarne, stała się źródłem zagrożeń. Obejmuje zagadnienia dotyczące narodowego bezpieczeństwa i ujmuje je w sposób całościowy. Pokazuje, jak skutecznie i efektywnie wykorzystywać zasoby państwa, zarówno w sferze ochronnej, społecznej, jak i obronnej, przy pomocy integracji dostępnych zasobów w systemie bezpieczeństwa narodowego. Ukazana została zależność polskiego bezpieczeństwa od realizacji narodowych interesów. Wg tego dokumentu: „Bezpieczeństwo Europy determinowane będzie przez cztery główne czynniki: NATO, Unię Europejską, strategiczną obecność USA na kontynencie europejskim oraz relacje z Rosją" [11].

Na podstawie strategii oceniono ryzyko występowania na obszarze Polski konfliktów o lokalnym oraz regionalnym charakterze, a także podkreślono, że Polska jest zależna od wpływów politycznych, które mogą wywoływać zagrożenia wojenne i kryzysowe. Przedstawiono strategiczne cele Polski w zakresie bezpieczeństwa kraju. „Wskazano na potrzebę zrównoważonego umiędzynarodawiania i samodzielności w zakresie bezpieczeństwa naszego państwa, w tym zwiększenie strategicznej odporności kraju na różnego rodzaju zagrożenia. Określono w niej trzy priorytety polityki bezpieczeństwa:

– zapewnienie gotowości i demonstracja determinacji do działania w sferze bezpieczeństwa i obrony oraz wzmocnienie narodowych zdolności obronnych, ze szczególnym traktowaniem tych obszarów bezpieczeństwa narodowego, w których sojusznicze (wspólne) działania mogą być utrudnione;
– wspieranie procesów służących wzmocnieniu zdolności NATO do kolektywnej obrony, rozwój Wspólnej Polityki Bezpieczeństwa i Obrony UE, umacnianie strategicznego partnerstwa (w tym z USA) oraz strategicznych relacji z partnerami w regionie;
– wspieranie i selektywny udział w działaniach społeczności międzynarodowej, realizowanych na podstawie prawa międzynarodowego, mających na celu zapobieganie powstawaniu nowych źródeł zagrożeń, a także reagowanie na zaistniałe kryzysy oraz przeciwdziałanie ich rozprzestrzenianiu się [11]".

W trzech priorytetach ujęto działania, jakie Polska podejmuje w celu niwelowania zagrożenia bezpieczeństwa. Priorytet I Strategiczne wysiłki Polski skoncentrowane na bezpieczeństwie obywateli oraz terytorium kraju. Priorytet II określa wspieranie przez Polskę konsolidacji NATO, pogłębianie współpracy w ramach uczestnictwa w UE. Ważną rolę ogrywa Priorytet III „Jego realizacja wymaga m.in. wzmocnienia ONZ, kontynuacji starań o dokonanie przeglądu norm prawa międzynarodowego oraz wzmacniania skuteczności regulacji w obszarze kontroli zbrojeń i rozbrojenia, w tym środków budowy zaufania i bezpieczeństwa. W wymiarze regionalnym istnieje potrzeba odbudowy znaczenia OBWE. Zgodnie z przyjętymi priorytetami, Polska organizuje i prowadzi strategiczne działania obronne, ochronne oraz w sferze bezpieczeństwa społecznego i gospodarczego.

Działania w sferze militarnej ukierunkowane są na utrzymywanie i demonstrowanie wszechstronnej gotowości państwa do skutecznego reagowania na militarne zagrożenia dla niepodległości i integralności terytorialnej Polski.

Celem działań ochronnych jest zapewnienie warunków do utrzymywania ładu konstytucyjnego, wewnętrznej stabilności państwa, bezpieczeństwa powszechnego i porządku publicznego, zarówno wspólnych, jak i indywidualnych zasobów materialnych i niematerialnych, a także funkcjonowania infrastruktury krytycznej.

Istotą działań społecznych w sferze bezpieczeństwa jest stworzenie bezpiecznych warunków do godnego życia obywateli. Do kluczowych działań należą: ochrona dziedzictwa narodowego, w tym zapewnienie jego bezpiecznego rozwoju, zwłaszcza w sferze ekonomicznej, społecznej i intelektualnej oraz niematerialne wsparcie systemu bezpieczeństwa narodowego" [11].

Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2009–2011

Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej został utworzony w celu wykreowania odpowiednich działań, które zagwarantują bezpieczeństwo Polski w cyberprzestrzeni.

Program zawiera trzy podstawowe założenia: działania w sferze technicznej, edukacyjnej oraz organizacyjno-prawnej. Odbiorcami programu są obywatele polscy mieszkający i korzystający z sieci poza granicami kraju oraz wszyscy użytkownicy sieci na terytorium państwa. Zaproponowane rozwiązanie przewiduje wypracowanie i skuteczne wdrożenie regulacji prawnych, określających miejsce i rolę instytucji prawnych w obszarze cyberprzestrzeni, ale również definiujących rolę zwykłych użytkowników sieci. Do istotnych założeń programu zalicza się wypracowanie systemu, który miałby ułatwić i zabezpieczyć proces wymiany informacji pomiędzy prywatnym sektorem i publicznym.

W obszarze technicznym programu podejmowano badania naukowe dotyczące rozwoju ochrony cyberprzestrzeni kraju. Przez ośrodki badawcze prowadzące badania nad

 ISSN 1895-8443

rozwojem technologicznym wypracowane zostały narzędzia, pozwalające analizować zagrożenie, skutecznie je zwalczać i zapewniać dalsze bezpieczeństwo. Znaczący wkład wnieśli również przedsiębiorcy, mogący indywidualnie badać, opracowywać i wdrażać środki ochrony i metody walki z cyberatakami, jednocześnie dzieląc się zdobytą wiedzą z sektorem publicznym.

Na znaczeniu zyskał również obszar edukacji, w ramach którego miały się odbywać szkolenia z zakresu wykrywania zagrożenia oraz prawidłowej obsługi Internetu. Szkolenia te prowadzone były w szkołach i miały docierać do zwykłych użytkowników sieci, aby uświadamiać im, że istnieją zagrożenia, które mogą prowadzić do negatywnych skutków. Edukacja dotyczy także urzędników oraz funkcjonariuszy i instytucji, na których spoczywa zapewnienie cyberbezpieczeństwa.

Zmiany wprowadzone w kwestii funkcjonalno-organizacyjnej, pozwalały na delegowanie zadań i podział odpowiedzialności za bezpieczeństwo w cyberprzestrzeni. Podział ról usprawnia funkcjonowanie mechanizmu obronnego i umożliwia szybsze reagowanie na pojawiające się zagrożenie.

Wart podkreślenia jest fakt, iż Polska podejmuje działania nie tylko obronne, ale również ofensywne. W efekcie kraj staje się przeciwnikiem równorzędnym w obszarze cyberprzestrzeni [16].

Legislacja polska w zakresie cyberprzestępczości

W Polsce ciągle brakuje prawnych regulacji, które w skumulowany i kompleksowy sposób normowałyby kwestię cyberterroryzmu oraz ochrony cyberprzestrzeni. Odpowiedzialność za bezpieczeństwo w cyberprzestrzeni jest rozproszona pomiędzy Ministerstwo Obrony Narodowej, Rządowe Centrum Bezpieczeństwa, Ministerstwo Cyfryzacji oraz Radę Ministrów, Agencję Bezpieczeństwa Wewnętrznego, Komendę Główną Policji, Ministerstwo Sprawiedliwości, Urząd Komunikacji Elektronicznej, a także przez CERT Polska znajdujący się w strukturze Naukowej i Akademickiej Sieci Komputerowej (NASK). Funkcjonują także zespoły publiczne oraz prywatne ds. reagowania na incydenty komputerowe CERT, które swoim zakresem obejmują wojskową administrację, policję, a także administrację rządową. Istnieją również zespoły utworzone z inicjatywy operatorów telekomunikacyjnych . Istotnym problemem, z którym borykają się wymienione podmioty, jest niedoprecyzowanie granic, po których przekroczeniu mają one podejmować reakcję i wdrażać działania zapobiegawcze. Niezbędnym warunkiem do prawidłowego funkcjonowania polskiego systemu jest szereg szkoleń, ćwiczeń, które będą dopracowane i tworzone na podstawie warunków i norm. Nie powinny one odzwierciedlać ćwiczeń prowadzonych w innych krajach, które mogą być niedostosowane do sytuacji i rodzaju cyberataków pojawiających się w sieci. Problem stanowi także brak szacowania możliwego do wystąpienia ryzyka. Usprawniłoby ono funkcjonowanie systemu obrony i pozwoliło określić potrzeby, jakie niesie ze sobą wypracowanie systemu barier obronnych dla cyberprzestrzeni.

Dotychczasowe działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej [12]. Przykładem mogą być polskie samorządy, potencjalnie zagrożone cyberatakami ze względu na fakt, iż dysponują ogromnymi bazami danych oraz dokonują niejednokrotnie dużych operacji finansowych.

Prezydent Rzeczypospolitej Polskiej Bronisław Komorowski 27 września 2011 roku podpisał nowelizację ustawy o stanie wojennym. Kluczowym celem ustawy było wprowadzenie i usystematyzowanie w polskim porządku prawnym definicji cyberprzestrzeni. Oznacza ona „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami" [13].

Powyższe działania legislacyjne umożliwiły utworzenie podstaw prawnych do rozpoczęcia praktycznych prac planistycznych oraz organizacyjnych, realizowanych przez organy władzy i administracji w kwestii określania w programach i planach operacyjnych dotyczących przygotowań obronnych założeń odnośnie nowych zagrożeń związanych z cyberprzestrzenią. Wprowadzenie pojęcia cyberprzestrzeni do polskiego systemu było impulsem do dalszych zmian legislacyjnych poruszających wątek cyberprzestępczości i bezpieczeństwa w sieci.

W celu podniesienia poziomu bezpieczeństwa w cyberprzestrzeni RP, w 2013 r. rząd przyjął Politykę Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Wyodrębniono w niej następujące cele szczegółowe:

1) „Zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej Państwa.
2) Zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni.
3) Zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne.
4) Określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni.
5) Stworzenie i realizacja spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych.
6) Stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni.
7) Zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni" [14].

Realizacja założeń programu z 2013 roku odbywała się poprzez podejmowanie działań, do których zaliczyć można przede wszystkim szacowanie ryzyka. Odgrywało ono kluczową rolę w zapewnieniu odpowiedniego poziomu bezpieczeństwa cyberprzestrzeni. Bezpieczeństwo portali administracji

rządowej było kolejnym zadaniem, które pozwalało realizować założone cele. Jednostki administracji rządowej zostały zobowiązane do wdrożenia organizacyjnych i technicznych zabezpieczeń swoich stron internetowych, które miały chronić je przed wyciekami danych. Trzecim rodzajem zadań były założenia działań legislacyjnych, polegające na analizie, wnikliwym przeglądzie dotychczasowych norm prawnych dotyczących bezpieczeństwa w cyberprzestrzeni, skierowane na tworzenie nowych norm prawnych, które uzupełniałyby istniejące już w tamtym okresie akty. Kolejna grupa działań to założenia dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa, które – zdaniem ekspertów – miały usprawniać funkcjonowanie systemu dbającego o bezpieczeństwo. W ramach tej polityki przewidziano szkolenia skierowane nie tylko do podmiotów tworzących system bezpieczeństwa i ochrony cyberprzestrzeni, lecz do całego społeczeństwa. Często użytkownicy Internetu nie zdają sobie sprawy, że stali się ofiarami owych ataków, dlatego też istnieje potrzeba zwiększania ich świadomości, a tym samym czujności. Wyżej wspomniana strategia zakładała zwiększenie zaufania obywateli oraz przedsiębiorców do e-usług, poprzez zapewnienie im większego bezpieczeństwa w sieci podczas wykonywania szeregu przelewów finansowych, przetwarzania i przechowywania informacji.

Istotnym aspektem było stwierdzenie, że polityka ta jest realizowana z uwzględnieniem praw człowieka, według których każdemu obywatelowi przysługuje prawo do wolności i prywatności. Od 2011 roku w Polsce następują liczne zmiany mające na uwadze poprawę bezpieczeństwa, ochronę swoich obywateli, baz danych. Stale doskonalone są regulacje prawne, które dostosowywane są do wymogów stawianych na poziomie międzynarodowych, aby skoordynować działania i usprawniać funkcjonowanie systemu ochrony cyberbezpieczeństwa. W roku 2015 powstała Doktryna Cyberbezpieczeństwa, która „wskazuje strategiczne kierunki działań dla zapewnienia bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni. Jednocześnie powinna być traktowana jako jednolita podstawa koncepcyjna, zapewniająca spójne i kompleksowe podejście do zagadnień cyberochrony i cyberobrony – jako wspólny mianownik dla działań realizowanych przez podmioty administracji publicznej, służby bezpieczeństwa i porządku publicznego, siły zbrojne, sektor prywatny oraz obywateli. Dzięki temu doktryna cyberbezpieczeństwa może stanowić punkt wyjścia do dalszych prac na rzecz wzmocnienia bezpieczeństwa Polski" [15]. W dokumencie opisano zadania powierzane poszczególnym podmiotom i przypisano im odpowiedzialność. Doktryna określa szereg zadań i kierunków działań, jakie powinno realizować państwo jako całość oraz poszczególne jego komórki.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej była dokumentem, którego treści odpowiadały wymaganiom wskazanym programem rządowym oraz z obowiązującymi w Unii Europejskiej, czy też różnego rodzaju strategiami związanymi z bezpieczeństwem narodowym. Jej kontynuację stanowi dokument, jakim jest obecnie obowiązująca: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Na jej podstawie powstała ustawa o krajowym systemie cyberbezpieczeństwa, która stanowi kolejny kluczowy element w budowie ram prawnych i instytucjonalnych, mających zapewnić efektywność funkcjonowania państwa polskiego w obszarze ochrony cyberprzestrzeni. Po przygotowaniu dokumentu strategicznego – Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017–2022[1] oraz planistycznego – Planu Działań na rzecz wdrażania Krajowych Ram Cyberbezpieczeństwa RP na lata 2017–2022, Ministerstwo Cyfryzacji, jako organ właściwy ds. bezpieczeństwa cyberprzestrzeni, przedstawił projekt aktu normatywnego Ma on stanowić kompleksową regulację z harmonizowanego i skonsolidowanego krajowego systemu cyberbezpieczeństwa oraz transponować do prawa polskiego postanowienia unijnej Dyrektywy NIS (Dyrektywa Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii).

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022

Bezpieczeństwo informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a także podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów teleinformatycznych, użytkowników cyberprzestrzeni, organów władzy publicznej, a także wyspecjalizowanych podmiotów zajmujących się bezpieczeństwem teleinformatycznym w sferze operacyjnej. Jest to tym istotniejsze, iż Polska jest ściśle powiązana z innymi państwami poprzez współpracę międzynarodową w ramach takich organizacji jak UE, NATO, ONZ czy OBWE.

W szczególności Strategia wskazuje:

- cele w zakresie bezpieczeństwa teleinformatycznego,
- główne podmioty zaangażowane we wdrażanie strategii w zakresie bezpieczeństwa teleinformatycznego,
- ramy zarządzania służące realizacji celów krajowej strategii w zakresie bezpieczeństwa teleinformatycznego,
- potrzebę zapobiegania i reagowania w odniesieniu do incydentów oraz przywracania stanu normalnego zakłóconego incydentem, w tym zasady współpracy pomiędzy sektorami publicznym i prywatnym,
- podejście do oceny ryzyka,
- kierunki podejścia do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa,

[1] Wymaganiami z zakresu cyberbezpieczeństwa zostaną objęci również dostawcy usług cyfrowych (chodzi o internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe). Ze względu na transgraniczny charakter tych usług i międzynarodową specyfikę podmiotów – obowiązki dla dostawców usług cyfrowych zostaną objęte łagodniejszym reżimem regulacyjnym. Ustawa odwołuje się tutaj do rozporządzenia wykonawczego Komisji Europejskiej 2018/151.

 ISSN 1895-8443

– działania odnoszące się do planów badawczo-rozwojowych w zakresie bezpieczeństwa teleinformatycznego,
– podejście do współpracy międzynarodowej w zakresie cyberbezpieczeństwa.

W Polsce wyróżnia się następujące podmioty, które odgrywają znaczącą rolę w systemie ochrony cyberprzestrzeni:

1) **Ministerstwo Cyfryzacji**, któremu przypisano rolę kluczową, jeśli chodzi o procesy związane z cyberprzestrzenią. Koordynuje system ochrony cyberprzestrzeni RP.
2) **Agencję Bezpieczeństwa Wewnętrznego**, która ma za zadanie rozpoznawać, zwalczać zagrażające bezpieczeństwu wewnętrznemu Polski incydenty oraz im zapobiegać,
3) **Ministerstwo Spraw Wewnętrznych i Administracji**, monitorujące i kontrolujące działania policji w zakresie zwalczania cyberprzestępczości,
4) **Policję,** która ma za zadanie zwalczać cyberprzestępczość,
5) **Ministerstwo Obrony Narodowej**, które odpowiada za strefę wojskową dotyczącą ochrony cyberprzestrzeni RP. W strukturze MON istnieje Narodowe Centrum Kryptologii,
6) **Urząd Komunikacji Elektronicznej,** regulujący rynek telekomunikacyjny oraz pocztowy pod względem bezpieczeństwa cyberprzestrzeni,
7) **Rządowe Centrum Bezpieczeństwa,** które zarządza kryzysowo i chroni infrastrukturę krytyczną,
8) **Ministerstwo Sprawiedliwości,** które ustanawia prawo w kwestii cyberprzestępczości oraz sprawuje pieczę nad jego wykonywaniem,
9) **Ministerstwo Finansów**, regulujące kwestie finansowe, które państwo ponosi wskutek działań na rzecz cyberbezpieczeństwa,
10) **Biuro Bezpieczeństwa Narodowego**, które jest doradczym organem głowy państwa,
11) **Naukową i Akademicką Sieć Komputerową**, która jest instytutem badawczym.

Unia Europejska wobec cyberterroryzmu

23 listopada 2001 roku w Budapeszcie została podpisana Konwencja Rady Europy o cyberprzestępczości. Konwencja powstała w związku z potrzebą prowadzenia polityki kryminalnej w sposób spójny oraz w celu zapewnienia bezpieczeństwa społecznego i ochrony przed cyberprzestępczością. Miała ona pomóc osiągnąć powszechnie panującą jedność pomiędzy krajami członkowskimi Rady Europy, wzajemną integrację oraz ustanowienia wspólnych przepisów prawnych. Miała też uściślić współpracę europejską, międzynarodową oraz krajową, aby wspólnie walczyć z cyberprzestępczością.

Wynikiem podjętych prac zmierzających do zidentyfikowania kluczowych obszarów wymagających wspólnych działań na poziomie międzynarodowym, w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości, było przyjęcie w 2009 r. *Programu sztokholmskiego* będącego najnowszym programem pięcioletnim (na lata 2010–2014), w którym przez wyznaczanie obszarów priorytetowych sprecyzowano postanowienia Traktatu z Lizbony dotyczące tego zagadnienia [17]. Należy podkreślić, że dokument ten – poprzez zawarte w nim odwołania do ochrony cyberprzestrzeni oraz wytyczne w dziedzinie wolności, bezpieczeństwa i sprawiedliwości – to olbrzymi krok na drodze zwiększania bezpieczeństwa wewnętrznego UE. Nie tylko zalicza on cyberprzestępczość do sześciu głównych priorytetów dla całej UE, lecz także wzywa do: propagowania prawodawstwa, które zapewnia bardzo wysoki poziom bezpieczeństwa sieci i umożliwia szybsze reagowanie w przypadku ataków cybernetycznych; przyspieszenia procesu ratyfikacyjnego Konwencji o cyberprzestępczości; udzielenia pełnego poparcia krajowym podmiotom powiadamiania o zagrożeniach, odpowiedzialnym za walkę z cyberprzestępczości; współpracy z państwami spoza Unii; wzmocnienia (usprawnienia) partnerstwa publiczno-prywatnego oraz poprawy współpracy sądowej w sprawach dotyczących cyberprzestępczości.

Istotnym z punktu widzenia bezpieczeństwa dokumentem jest komunikat Komisji Europejskiej z 28 marca 2012 r. wprowadzający definicję „cyberprzestępczości" rozumianej jako „wysokodochodowa, niskiego ryzyka forma przestępczej działalności, która coraz bardziej staje się powszechna i szkodliwa". Jednak wyjaśnienie terminu cyberprzestępczości pojawiło się już wcześniej w *Europejskiej agendzie cyfrowej*, dokumencie Komisji Europejskiej, w którym określono ją jako „nową formę przestępczości obejmującą między innymi wykorzystywanie dzieci, kradzież tożsamości i ataki cyberprzestrzeni".

Analizując przedstawione powyżej pojęcia cyberprzestępczości i bezpieczeństwa, można zauważyć nie tylko niejednolity stopień szczegółowości tych definicji, ale również różny ich zakres przedmiotowy. Dodatkowo należy także przywołać charakterystykę cyberprzestępczości przedstawioną w obszernym materiale Parlamentu Europejskiego, która została opracowana na podstawie doświadczeń państw członkowskich UE. Parlament Europejski, dokonując analizy zebranych materiałów oraz korzystając z dorobku całej Unii w zakresie cyberprzestępczości, wskazał na nią jako na jedną z największych obaw i zagrożeń dla zinformatyzowanego współczesnego świata. Charakteryzuje się ona: niejednoznaczną naturą podmiotów w cyberprzestrzeni, szeroką skalą, dużym zróżnicowaniem i trudnością w przeciwdziałaniu i zwalczaniu, stosowaniu w dużej mierze podobnych technik ataków oraz z pewnością zaawansowaniem i wysokim poziomem dochodowości.

Rozpatrując działania Unii Europejskiej w zakresie ochrony cyberprzestrzeni, przede wszystkim należy zwrócić uwagę na dwutorowość podejmowanych prac, w czym również upatruje się słabości wszelkich inicjatyw. Podział prac UE został dokonany ze względu na kryterium przedmiotu: zwalczanie cyberataków (włączając w to cyberprzestępczość i cyberterroryzm) oraz utrzymanie ochrony (infrastruktury krytycznej[2],

[2] Critical Infrastructure Security – CIS.

bezpieczeństwa sieci i informacji[3] i krytycznej infrastruktury informatycznej[4]).

Dokument porusza problematykę bezpieczeństwa sieci teleinformatycznych, na których ciąży duże ryzyko cyberataków oraz informowania o pojawiających się w sieci przestępstwach. Konwencja ma za zadanie identyfikować działania, które mogłyby zagrażać integralności, poufności, jak i dostępności danych przechowywanych w sieci. Jest również środkiem do skutecznego zwalczania owych przestępstw, dzięki skutecznemu wykrywaniu, a także ściganiu sprawców. Ściganie to jest możliwe dzięki współpracy nie tylko na obszarze kraju, lecz także poza jego granicami.

W dokumencie tym zostały rozróżnione zadania podlegające terytorium kraju i zadania dla szczebla międzynarodowego. Dokument nazywa i definiuje cyberprzestępstwa, oraz systematyzuje je, tworząc kategorie m.in., "przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów; przestępstwa komputerowe; przestępstwa ze względu na charakter zawartych informacji oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych [18]".

Podsumowanie

Wszelkie działania i decyzje podejmowane na mocy Konwencji Rady Europy o cyberprzestępczości są transparentne z innymi aktami prawa. Uwzględniają poszanowanie praw człowieka, zgodnie z którymi każdy ma możliwość głoszenia swoich opinii i poglądów oraz prawo do wolności.

Duża odpowiedzialność spoczywa na władzach kraju, ponieważ to one kreują, wdrażają i kontrolują regulacje prawne ułatwiające walkę z cyberprzestępczością. Niezwykle ważne jest, aby tworzone regulacje nie naruszały prywatności obywateli, przysługującej im zgodnie z prawem. Stąd też należy podejmować szereg działań umożliwiających bezpieczne użytkowanie Internetu przez osoby prywatne, jednocześnie dążąc do zabezpieczyenia systemów rządowych, w których przechowywane są niezliczone ilości informacji, także ściśle tajne.

Współpraca państw na arenie międzynarodowej w obszarze cyberprzestrzeni ma za zadanie ujednolicanie aktów prawnych i wszelkiego typu regulacji, w celu łatwiejszego i skoordynowanego działania w zakresie cyberbezpieczeństwa. Normy prawne państw, które są ze sobą skoordynowane, ułatwiają namierzanie, ściganie i karanie cyberprzestępców. Wspólne działanie krajów w ramach Unii Europejskiej daje możliwość prowadzenia szkoleń na większą skalę, o wyższym stopniu zaawansowania, co jest bardziej korzystne dla uczestniczących w nich państw uczestniczących niż szkolenia „w pojedynkę". Umożliwiają one wymianę doświadczeń, umiejętności w zakresie wytworzonych już zabezpieczeń.

Podczas formułowania norm, regulacji prawnych dotyczących ochrony cyberprzestrzeni (czy to na poziomie kraju, czy w skali międzynarodowej) istotne jest uwzględnienie szybkiego reagowania na pojawiające się zagrożenia. Ustawodawstwo państw członkowskich na podstawie norm określanych przez Unię Europejską, powinno być bardzo kompatybilne. Ewentualne rozbieżności w kwestiach prawnych poszczególnych państw należy niwelować. Działania te, mające na celu spełnienie kryteriów, jakie stawia przed państwami członkowskimi UE, mają na celu współtworzenie zintegrowanego systemu, zapewniającego bezpieczeństwo w cyberprzestrzeni.

Wszystkie wyżej wymienione aspekty i działania wspólnie tworzą całość, która prowadzi do osiągnięcia jednego celu – cyberbezpieczeństwa. Działania państw powinny być ukierunkowane na bezpieczeństwo kraju oraz jego obywateli tak, by każdy mógł z pełna swobodą i bez żadnych obaw korzystać z wynalazków powstałych wraz z rozwojem technologii teleinformatycznych.

Literatura

[1] Pilżys J., *Transnarodowe zagrożenia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, w: *Terroryzm globalne wyzwanie*, K. Kowalczyk, W. Wróblewski (red.), Toruń 2008, s. 189.

[2] Szubrycht T., *Cyberbezpieczeństwo*, „Zeszyty naukowe marynarki wojennej" 2005, (160)1.

[3] White K.C., *Cyber-Terrorism: Modem Mayhem*, Carlisle 1998, s. 10.

[4] Szubrycht T., *Zagrożenia cyberbezpieczeństwa*, „Zeszyty naukowe marynarki wojennej" R. 61, (2005)1, s. 25.

[5] Denning D., *Cyberterrorism*, 2000, http://www.cs.georgetown.edu~denning/infosec/cybert [dostęp: 02.01.2017].

[6] Lewis J.A, *Assessing the risk of cyber terrorism, cyber war and other cyberthreats*, Center for Strategic and International Studies 2002, http:// www.csis.org/tech/0211lewis.pdf [dostęp: 02.01.2017].

[7] Fielding N.G., *Triangulation and Mixed Methods Designs Data Integration With New Research Technologies*, "Journal of Mixed Methods research", 2012, 124–136.

[8] Górka M. (red.), *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, w: *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa 2014.

[9] *Active Engagement, Modern Defence*, North Atlantic Treaty Organization, 19.11.2010 [dostęp: 22.01.2017].

[10] Unijny plan bezpieczeństwa cyberprzestrzeni na rzecz ochrony otwartego Internetu oraz wolności i możliwości w Internecie, Bruksela 2013, http://europa.eu/rapid/press-release_IP-13-94_pl.htm [dostęp: 22.01.2017].

[11] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, https://www.bbn.gov.pl/ftp/dok/01/sbn_rp_2014.pdf [dostęp 13.02.2017].

[12] NIK: Informacja o wynikach kontroli Informacja o wynikach kontroli: Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, 2015.

[13] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, (Dz.U. 2011 Nr 222, poz. 1323).

[3] Network and Information Security – NIS.

[4] Critical Information Infrastructure Protection – CIIP.

[14] Polityka Ochrony Cyberprzestrzeni Polskiej, http://www.cert.gov.pl/cerCyberprzestrzeni-Rzeczypospolitej-Polskiej.html, Warszawa 2013, [dostęp: 13.02.2017].
[15] Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, https://www.bbn.gov.pl/ftp/dok/01/sbn_rp_2014.pdf [dostęp: 24.01.2017].
[16] Polska Izba Informatyki i Telekomunikacji, http://www.piit.org.pl/-/piit-opinia-ws-rzadowego-programu-ochrony-cyberprzestrzeni-rp-2011-2016, [dostęp: 20.02.2017].
[17] Informacje instytucji, organów i jednostek organizacyjnych Unii Europejskiej, Rada Europejska Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli, (Dz. Urz. UE C 115 z 4 maja 2010).
[18] Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, (Dz.U. 2014 poz. 1514).

DR MAGDALENA EL GHAMARI – kierownik Pracowni Bezpieczeństwa Kulturowego Collegium Civitas, fundator i prezes Fundacji El-Karama. Członek Stowarzyszenia Euro-Atlantyckiego, European Security Assosiation, Stowarzyszenia Kombatantów Misji Pokojowych ONZ, Polskiego Towarzystwa Studiów Międzynarodowych, Towarzystwa Polsko-Albańskiego i International Institute for Private-, Commercial, and Competition Law w Tiranie. Członek zespołu redakcyjnego magazynu „E-terroryzm", Securitologia oraz Security Review. Absolwentka studiów doktoranckich w Katedrze Działań Połączonych Akademii Obrony Narodowej. Wykładowca akademicki oraz szkoleniowiec z obszaru: MENA, fundamentalizm islamski, zagrożenia bezpieczeństwa międzynarodowego, terroryzm, migracje, komunikacje międzykulturowa, Bałkany, operacje NATO, militaria.