prof. nadzw. dr hab. Izabela OLEKSIEWICZ
Politechnika Rzeszowska
Wydział Zarządzania

# CYBERTERRORYZM JAKO REALNE ZAGROŻENIE DLA POLSKI

# CYBERTERRORISM AS A REAL THREAT TO POLAND

**Streszczenie:** Pojawienie się zagrożeń globalnych spowodowało zmianę podejścia do problematyki bezpieczeństwa. Do czasów pojawienia się nowej epoki problemy bezpieczeństwa i ich rozwiązywanie można podzielić na dwie kategorie. Średni poziom bezpieczeństwa narodu zapewniany był przez ogólny rozwój państwa, a także poprzez administracyjną i wojskową działalność państwa. Indywidualny poziom bezpieczeństwa zależy od osobistego postępowania człowieka w życiu codziennym. Działalność cyberterrorystów w sieci jest bardzo poważnym problemem, gdyż ich poczynania są ukryte. Z uwagi na łatwość maskowania tożsamości można mówić o relatywnej anonimowości atakujących, którzy bez obaw, że zostaną wykryci, przeprowadzają za pomocą sieci wrogie działania. Wynika stąd kolejny problem – skala potencjalnych strat, zarówno pod względem finansowym, jak i bezpieczeństwa, jest trudna do oszacowania (e-Terroryzm.pl, 2013, s. 8). Zagrożenia stwarzają najczęściej państwa lub podmioty niepaństwowe o stwierdzonych wrogich zamiarach wobec innych państw bądź organizacji, dysponujące środkami ich realizacji. Zagrożenia w sferze teleinformatycznej, są coraz częściej trudne do identyfikacji dążąc do dezorganizacji kluczowych systemów informacyjnych instytucji rządowych, elementów infrastruktury krytycznej w tym baz danych. Czynnikami sprzyjającymi powstawaniu tego typu zagrożeń są niskie koszty przygotowania operacji oraz ogromna skala zniszczeń. Cechą charakterystyczną tych działań jest globalny ich zasięg. Założeniem niniejszej publikacji jest ukazanie, że przyczyną powstania polityki antycyberterrorystycznej jest brak istnienia odpowiednich mechanizmów i regulacji w tym zakresie, w związku z czym mamy do czynienia z procesem instytucjonalizacji. Należy więc stwierdzić, że polityka antycyberterrorystyczna Polski jest nie tylko odpowiedzią, ale i naczelnym wyzwaniem dla poprawnego funkcjonowania systemu bezpieczeństwa narodowego RP.

**Słowa kluczowe:** cyberterroryzm, polityka, bezpieczeństwo RP.

**Summary:** The emergence of global threats caused a change in the approach to security issues. Until the advent of a new era of security problems, their solution can be divided into two categories. The average level of security of the nation was ensured by the general development of the state and by the administrative and military activities of the state. The individual level of security depends on personal behavior in daily life. Cyberterrorists' activity in the network is a very serious problem as their actions are hidden. Due to the ease of identity fraud, it is possible to talk about the relative anonymity of attackers who, without the fear of being detected, carry out hostile actions. That brings about another problem – the scale of potential losses, both financial and security, is difficult to estimate. The threats are most often caused by states or non-state actors with hostile intentions towards other states or organizations that have the means to implement them. Threats in the tele-information sector are increasingly difficult to identify,

seeking to disorganize key government information systems and critical infrastructure components including databases. The factors favoring the emergence of such risks are low costs of preparing an operation and the enormous scale of the destruction. The characteristic feature of those activities is their global reach. The purpose of this publication is to show that the cause of counter-cyberterrorism policy is the lack of appropriate mechanisms and regulations in this regard, and that is why we are dealing with the process of institutionalization. Therefore, it should be stated that the counter-cyberterrorism policy of Poland is not only an answer but also a major challenge for the proper functioning of the national security system in Poland.

**Keywords:** cyberterrorism, policy, security of the Republic of Poland

## Istota polityki antycyberterrorystycznej

Cyberterroryzm stał się modnym pojęciem, jednak niewiele osób wie, czym on tak naprawdę jest. Wielu uważa, że jest to jedynie teoretyczne pojęcie, działanie, które prawdopodobnie nigdy nie będzie miało miejsca w rzeczywistości. Ale nikt nie wie, co przyniesie przyszłość.

Powszechne wykorzystywanie technologii informatycznych jest niewątpliwie szczególnym atrybutem współczesności. Komputer i Internet to narzędzia, bez których nie potrafi dziś normalnie funkcjonować ani administracja, ani gospodarka, ani pojedynczy obywatel. Dzięki informatyzacji zwiększył się dostęp do informacji, pojawiła się łatwość przetwarzania każdej informacji, zwiększyły się możliwości komunikacyjne, a cały świat staje się powoli jedną globalną wioską. Zmiany cywilizacyjne, jakie nastąpiły w ostatnich latach, są ogromne i nieodwracalne, zaś skutki jakie niosą za sobą nie do końca jeszcze przewidywalne.

Zdefiniowanie cyberterroryzmu jako połączenie cyberprzestrzeni i terroryzmu oznacza, że taka aktywność wiąże się nie tylko z wrogim użyciem IT i działaniem w sferze wirtualnej, ale także cechuje się wszystkimi elementami konstytuującymi aktywność terrorystyczną (Denning, 2017). Pojęcie to odnosi się do bezprawnych ataków i zagrożeń wobec komputerów, sieci i informacji przechowywanych w nich celem, którym jest zastraszenie lub zmuszenie rządu albo jego ludzi po to, aby osiągnąć pewne korzyści polityczne lub społeczne. Ponadto, aby móc zakwalifikować atak jako cyberterroryzm, powinien on być dokonany w wyniku przemocy wobec osób lub mienia, lub przynajmniej powodować znaczne szkody po to, aby wywołać strach. Przykładami takich ataków mogłyby być te, które prowadzą do śmierci lub obrażeń ciała, powodują eksplozje lub straty gospodarcze. Jak twierdzi D. Denning, poważne ataki na infrastrukturę krytyczną mogą być również uznane za akty cyberterroryzmu, w zależności od ich wpływu. Natomiast ataki, które zakłócają nieistotne usługi lub są przede wszystkim kosztowne do nich nie należą (Denning, 2000).

Tak więc należy stwierdzić, że pojęcie „cyberterroryzmu" używane jest w kontekście politycznie umotywowanego ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach dale-

ko idących politycznych i społecznych celów w szerokim rozumieniu tego słowa (Riedel, Piasecka, 2011, s. 18).

Przytoczone powyżej definicje dowodzą, że cyberterroryzm[1] pojmowany jest na świecie w dwojaki sposób. Według jednej koncepcji od terroryzmu klasycznego odróżnia go jedynie użycie technologii informatycznych w celu przeprowadzenia zamachu, druga natomiast kładzie nacisk na systemy komputerowe jako cel ataków, a nie narzędzie do ich przeprowadzenia. Wydaje się, iż prawdziwa definicja powstaje dopiero po połączeniu obu tych działań (Suchorzewska, 2010, s. 17).

Mianem „cyberprzestępczości" określa się takie formy posługiwania się sieciami telekomunikacyjnymi, siecią komputerową, Internetem, których celem jest naruszenie jakiegokolwiek dobra chronionego prawem (Białoskórski, 2011, s. 63; Gniadek, 2009, s. 222; Kosiński, Waszczuk, 2015, s. 333). Cyberprzestępczość od klasycznej przestępczości odróżnia przede wszystkim działanie w środowisku związanym z technologią komputerową i wykorzystanie sieci komputerowych do popełniania przestępstwa (Siwicki, 2013, s. 20). Jej wyróżnikiem nie jest natomiast ochrona jakiegoś jednego wspólnego dobra (Siwicki, 2013, s. 21). Dzisiaj niemal każda nielegalna działalność ma swoje odbicie w Internecie. Globalny charakter Internetu umożliwił niezwykle szybką komunikację i przeniesienie większości form aktywności człowieka do sieci, także i tych negatywnie odbieranych. Coraz powszechniej mówi się o cyberprzestrzeni jako nowej przestrzeni społecznej, w której odbijają się te same problemy co w świecie rzeczywistym. Cyberprzestępczość jest zatem nowoczesną odmianą przestępczości, wykorzystującą możliwości technik cyfrowych i środowiska sieci komputerowych.

Pojęcie cyberprzestępczości pojawia się coraz częściej w literaturze przedmiotu, choć należy zaznaczyć, że nie doczekało się ono jeszcze swojego normatywnego ustalenia. Cyberprzestępczość określana jest jako podkategoria przestępczości komputerowej, obejmująca wszelkie rodzaje przestępstw, do popełnienia których użyto Internetu lub innych sieci komputerowych. Przy czym komputery i sieci komputerowe mogą służyć do popełniania przestępstw na kilka sposobów: jako narzędzie przestępstwa, jako cel przestępstwa lub służyć do realizacji innych zadań dodatkowych (np. przechowywania danych uzyskanych w wyniku przestępstwa) (Littlejohn, Tittel, 2004, s. 25). Mieszczą się tu zatem wszelkie ataki kierowane przeciwko połączonym systemom komputerowym i mające na celu uniemożliwienie im prawidłowego działania, bądź danym przechowywanym w formie elektronicznej na pojedynczym komputerze, bądź też kilku połączonych wspólną siecią. Cechą najbardziej charakterystyczną cyberprzestępczości jest to, że poszczególne czyny mogą być dokonywane za pomocą komputera podłączonego do Internetu lub wewnętrznych sieci intranetowych (Skowera, 2006, s. 142; Depa, Pomykała, 2014, s. 8).

[1] W USA działań hakerskich nie traktuje się jako cyberterroryzmu, chyba, że dokonywane są one przez organizacje terrorystyczne. Próby uzyskania nieuprawnionego dostępu do sieci wojskowych czy rządowych, które mają na celu kradzież danych (tajnych informacji) klasyfikować powinniśmy raczej jako szpiegostwo niźli sam akt cyberterroryzmu. Taka sama sytuacja dotyczy włamań do systemów bankowych, których celem jest opróżnienie kont. Tę działalność powinno klasyfikować się jako klasyczną działalność kryminalną, a nie jako cyberterroryzm. Patrz szerzej: e-Terroryzm.pl, nr 5/2012 (5), s. 8.

Polityka antycyberterrorystyczna jest więc reakcją powstałą na zaistniałe zagrożenie. Należy też stwierdzić, że polityka antycyberterrorystyczna nie jest tylko odpowiedzią. Przyczyną powstania polityki antycyberterrorystycznej jest również brak istnienia odpowiednich mechanizmów i regulacji w tym zakresie, w związku z czym mamy do czynienia z procesem instytucjonalizacji.

## Uwarunkowania polityki antycyberterrorystycznej

Czynnikiem, który wywiera większy wpływ na środowisko bezpieczeństwa, większy niż podziały w społeczności międzynarodowej są procesy globalizacyjne. Globalizacja wydaje się już tak zaawansowana, że sieć różnorodnych powiązań między państwami i społeczeństwami na świecie ma zbyt dużą gęstość, aby ulec dezintegracji czy znacznej redukcji. Nieuniknioną konsekwencją globalizacji jest erozja suwerenności państw, która dotyka każdego z państw, choć w zróżnicowanym stopniu. Wynika to z „odterytorialnienia" procesów społecznych oraz pogłębienia się rozmaitych współzależności w skali globalnej lub międzynarodowej w każdej dziedzinie życia społecznego. Proces ten dokonuje się stopniowo, jest jednak równie trwały jak sama globalizacja, wpływając w ten sposób na porządek i środowisko międzynarodowe.

Procesy globalizacji, zwłaszcza oddziałujące na sferę społeczno-ekonomiczną, tworzą nowe zagrożenia bezpieczeństwa. Ma również znaczenie fakt, że część zjawisk kryzysogennych toczy się poza jej terytorium. Wprost oddziałują one na wewnętrzną sytuację państw europejskich oraz społeczność europejską. W opinii znacznych części społeczeństw utrzymanie gwarancji zatrudnienia i adekwatnej liczby miejsc pracy, odpowiedniego poziomu bezpieczeństwa socjalnego czy tożsamości kulturowej powinno stać się priorytetowym zadaniem państwa.

Aby znaleźć odpowiedź na pytanie, czym w zasadzie jest cyberwojna, należałoby jednak na wstępie zrozumieć, dlaczego sieci teleinformatyczne są w coraz większym stopniu wykorzystywane przez rządy? Przede wszystkim wynika to ze specyfiki sygnału elektronicznego, a co za tym idzie z samej cyberprzestrzeni. W cyberprzestrzeni nie istnieją bowiem tradycyjnie rozumiane granice, choć infrastruktura teleinformatyczna znajduje się na obszarze określonych państw. Ma ona charakter niematerialny, choć działa na podstawie rzeczywiście istniejącej infrastruktury, generującej pole elektromagnetyczne. Wykorzystując tę cechę, można uzyskać wymierne korzyści materialne[2].

Z niematerialnością cyberprzestrzeni wiążą się jeszcze inne cechy. Przede wszystkim, sieć jest globalna[3]. Co za tym idzie, nie obowiązują tu ograniczenia o charakterze fizycznym. Stosunkowo łatwo ukryć w niej również prawdziwą tożsamość sprawców

[2] Teoretycznie, jedna osoba mogłaby potencjalnie wyrządzić szkody, które w rzeczywistości mogłyby być efektem działań zorganizowanej grupy terrorystycznej lub jednostek wojskowych.

[3] Mogą się w niej ścierać podmioty odległe od siebie o tysiące kilometrów. Przestrzeń teleinformatyczna ułatwiła ten proceder zarówno podmiotom państwowym, jak i pozapaństwowym. Obecnie, z drugiego końca globu, przy relatywnie niskim ryzyku poniesienia konsekwencji możliwe jest niemal błyskawiczne uzyskanie istotnych danych, w tym np. dokumentów i technologii o fundamentalnym znaczeniu dla bezpieczeństwa państwa.

incydentów teleinformatycznych. Brak tu nie tylko wywiadu strategicznego, ale także, w wielu przypadkach, możliwości zidentyfikowania osoby odpowiedzialnej za dany atak komputerowy. Jest to wbrew pozorom problem o fundamentalnym znaczeniu. Wskazanie podmiotu odpowiedzialnego za włamanie jest bowiem kwestią zasadniczą w przypadku przygotowania odpowiedniej reakcji politycznej, prawnej czy wojskowej (Oleksiewicz, 2015, s. 35-36).

Kolejną istotną cechą cyberprzestrzeni są relatywnie niskie koszty działania w niej. Rozwój konwencjonalnego potencjału wojskowego wiąże się z reguły z bardzo wysokimi nakładami finansowymi, obejmującymi nie tylko szkolenie personelu, lecz także modernizację i utrzymanie sprzętu. Tymczasem narzędzia, które mogą zostać wykorzystane do ataku w środowisku teleinformatycznym, w tej perspektywie, są prawie darmowe[4]. Wykorzystaniu cyberprzestrzeni sprzyja również fakt, że jak udowodniła operacja przeprowadzona przez grupę Harkat–ul- Ansar środki tego typu mogą czasami zastępować lub uzupełniać konwencjonalne działania zbrojne (Oleksiewicz, 2015, s. 37-38).

Cyberprzestrzeń oraz szybkość przeprowadzania ataków sprawiają, że prowadzenie działań obronnych jest utrudnione. Jednocześnie jak wskazano wyżej, akcje ofensywne są relatywnie tanie i łatwe do przeprowadzenia. Ta cecha cyberprzestrzeni jest tym wyraźniejsza, im większe jest uzależnienie społeczeństw od jej wykorzystania. Można tu bowiem zauważyć pewien paradoks. Z jednej strony, wykorzystanie technologii ICT we wszystkich sferach życia ludzkiego wiąże się z doniosłymi korzyściami, np. natury organizacyjnej, komunikacyjnej czy finansowej. Równocześnie sprawia to, iż zaawansowany technologicznie podmiot jest zdecydowanie bardziej wrażliwy na ataki teleinformatyczne. Ponadto, jak zauważył Fred Schreier (Oleksiewicz, 2016, s. 530 i n.), przestrzeń teleinformatyczna przez wielu jest postrzegana jako część wspólnego dziedzictwa ludzkości. Jego zdaniem istotną cechą przestrzeni teleinformatycznej jest faworyzowanie działań ofensywnych nad defensywnymi.

Ostatnia grupa powodów, dzięki którym cyberprzestrzeń cieszy się rosnącym zainteresowaniem państw, wiąże się z szeroko pojętą sferą informacyjną. Przestrzeń teleinformatyczna posiada bowiem ogromny potencjał z perspektywy działalności propagandowej lub psychologicznej. Nowe technologie informacyjne i komunikacyjne mogą być skutecznie wykorzystane np. do manipulowania opinią publiczną czy dezinformacji.

Aktorów sceny cyberterrorystycznej znakomicie obrazuje schemat przedstawiony przez Thomasa R. Mockatis'a, który wymienia kryminalne organizacje pełniące rolę ubezpieczającą działania cyberterrorystyczne oraz państwa posługujące się terrorem i go wspomagające, wśród których ogromną rolę pełnią cyberterrorystyczne grupy (Mockatis, 2008, s. 29). Osoby, które mogą dokonać aktów cyberterrorystycznych stanowią grupę działaczy różnych organizacji typową dla XXI wieku. W opinii specjalistów spośród nich można wyróżnić fanatyków religijnych, ortodoksyjnych działaczy New Age, separatystów i rewolucjonistów etniczno–narodowościowych oraz innego rodzaju

[4] Państwa stosunkowo łatwo mogą wejść w posiadanie szkodliwego oprogramowania (wirusów, trojanów, robaków), jak również sprzętu potrzebnego do przeprowadzenia nawet zaawansowanych operacji. Coraz częściej, agencje rządowe same opracowują najbardziej rozbudowane narzędzia, co nie wiąże się jednak z poważnymi kosztami z punktu widzenia budżetu (casus wirusa Stuxnet).

ekstremistów (e-Terroryzm.pl, 2013, s. 11). Wśród fanów regijnych (szczególnie islamskich) w wielu przypadkach zauważa się, że metody cyberterrorystyczne nie są przez nich stosowane. Przywódcy często nie znają się lub nie rozumieją nowoczesnych technologii, a ponadto brak im przygotowanej technologicznie i zaangażowanej ideowo kadry.

Inaczej jest w przypadku ortodoksyjnych działaczy New Age, wśród których można wyróżnić organizacje działające na rzecz praw zwierząt lub antyglobalistów. Posiadają oni w swych szeregach członków organizacji bardzo dobrze przygotowanych do roli cyberterrorystów, jednak ze względu na poglądy nie stosują cyberterroryzmu przeciw życiu ludzkiemu i wręcz wykluczają ofiary w ludziach. Bardzo groźną grupą (o różnym przygotowaniu specjalistycznym) są separatyści i rewolucjoniści etniczno–narodowościowi, którzy nie posiadają żadnych obiekcji w stosunku do obiektów ataku. W miarę postępu cywilizacyjnego na świecie mogą pojawić się również innego typu ekstremiści.

Nową, bardzo niebezpieczną zmianę w cyberterroryzmie (która przyspieszyć może nadejście tego groźnego zjawiska) wyznacza pojawienie się tzw. „najemników". Jest to ostatnio coraz częściej pojawiająca się tendencja wykorzystywania znawców zaawansowanych technologii w przestępczych działaniach komputerowych (Verton, 2004, s. 194).

Organizacje terrorystyczne, które posługują się nowymi technikami można, zdaniem A. Rathmella (Białoskórski, 2011, s. 60) podzielić na trzy kategorie:

– kategoria I, która obejmuje nowe techniki używane przez terrorystów do prowadzenia tradycyjnej działalności. Internet wykorzystuje się tutaj do zbierania informacji, komunikacji, zdobywania środków finansowych i komunikacyjnych;
– kategoria II, w której wykorzystywane są stare techniki do nowej działalności. Używana jest tutaj siła fizyczna, która ma na celu zniszczenie systemu informacyjnego;
– kategoria III, w której używa się nowe techniki do nowych działań – jest to atak w cyberprzestrzeni na system informacyjny[5] (Verton, 2004, s. 220).

Zauważyć można również, że coraz częściej organizacje ekstremistyczne (głównie islamskie) w celu wsparcia swych działań i przeprowadzania ofensywnych ataków budują sieci hackerskie. Obecnie można wyróżnić trzy poziomy zagrożenia związanego z cyberterroryzmem (Maj, 2017; e-Terroryzm.pl, 2013, s. 10-12). Pierwszym z nich jest tzw. *simple–unstructured*. Polega na dokonaniu przez cyberterrorystów prostych włamań do indywidualnych systemów informacyjnych poprzez wykorzystanie narzędzi internetowych skonstruowanych przez inną osobę.

Drugim poziomem zagrożenia jest tzw. *advanced–structured*. Na tym poziomie cyberterroryści dokonują bardziej skomplikowanych ataków przeciw złożonym sieciom komputerowym i systemom. Posiadają możliwość tworzenia lub modyfikacji własnych narzędzi, które służą do atakowania w cyberprzestrzeni, mają zdolność analizy celów,

[5] Problem ten przeanalizował również NCS (National Communications System), który w 2000 roku stwierdził, że „globalna zależność od połączonych ze sobą komputerów i słabości tego systemu sprzyja wzrostowi zagrożenia cyberterroryzmem. Ponadto kierunek ewolucji grup terrorystycznych czyni je szczególnie dostosowanymi do wykorzystania Internetu w realizacji swych celów. Wiele grup terrorystycznych przeszło ewolucję od struktur silnie hierarchicznych z określonymi przywódcami na czele do stowarzyszeń o dość luźnych powiązanych między częściowo niezależnymi komórkami, bez wyraźnej hierarchii – jak Hamas i organizacja bin Ladena. Szerzej: D. Verton, *Black ice…*, s. 220.

które będą przedmiotem ataku, a także dowodzenia, kontroli i uczenia się nowych metod atakowania.

Ostatnim, najpoważniejszym poziomem zagrożenia jest tzw. *complex–coordinated*. Cyberterroryści dokonują tu skoordynowanych ataków mających na celu totalną destrukcję zintegrowanego systemu obronnego, mają możliwość tworzenia skomplikowanych narzędzi, które służą do niszczenia celów w cyberprzestrzeni a także analizę celów będących przedmiotem ataku. Mogą dowodzić, kontrolować a także samodoskonalić się.

## Realizacja polityki ancybertyterrorystycznej w RP

Nowy terroryzm – cyberterroryzm jest produktem ery informatyzacji. Podstawową cechą jest sieciowość, co oznacza nie tylko odejście od klasycznej struktury hierarchicznej organizacji, ale przede wszystkim brak stałej lokalizacji, bez terytorialności. Działania i koordynacja elementów systemu nie są formalnie skodyfikowane przez relacje hierarchiczne, lecz wyłaniają się i zmieniają w zależności od konkretnego zadania. Kolejną z cech takich organizacji jest to, że więzy zewnętrzne i wewnętrzne nie stanowią skutku decyzji biurokratycznych, lecz efekt wspólnych norm, wartości, interesów i wzajemnego zaufania (Aleksandrowicz, 2008, s. 33-34).

Na tle krajów unijnych Polska jest dopiero na początku budowy zintegrowanego systemu bezpieczeństwa cyberprzestrzeni. Jednym z jego elementów jest przyjęta przez Komitet Stały Rady Ministrów w dniu 25 czerwca 2013 r. *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* (www.cert.gov.pl, 2017). Zawiera ona koncepcję systemu zarządzania cyberprzestrzenią oraz definiuje zależności między poszczególnymi organami i instytucjami państwowymi, a także ich wyspecjalizowanymi komórkami odpowiedzialnymi za zapewnienie odpowiedniego poziomu bezpieczeństwa teleinformatycznego w cyberprzestrzeni. Nie jest to jednak dokument o charakterze trans sektorowym, a jedynie rządowym (Adamczuk, Riedel, 2015, s. 286).

*Polityka Ochrony Cyberprzestrzeni* jako cel strategiczny wskazuje osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. Jego realizacja powinna odbywać się poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami cyberprzestrzeni Rzeczypospolitej Polskiej. Do celów szczegółowych zalicza się natomiast zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa, zwiększenie zdolności do zapobiegania i zwalczania zagrożeń w cyberprzestrzeni, ograniczanie skutków incydentów godzących w bezpieczeństwo teleinformatyczne, jednoznaczne określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo w cyberprzestrzeni, stworzenie i realizacja spójnego systemu zarządzania bezpieczeństwem w cyberprzestrzeni, stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni, a także zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni.

*Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej* przede wszystkim określa cel strategiczny, który osiąga się przez realizację zadań o charakterze operacyjnym

i przygotowawczym w dziedzinie cyberbezpieczeństwa. Zawiera ocenę zagrożeń, ryzyka i szans w dynamicznie rozwijającym się środowisku cyberbezpieczeństwa (w jego wymiarze zewnętrznym i wewnętrznym, krajowym i międzynarodowym), identyfikuje najważniejsze zadania operacyjne dla zapewnienia cyberbezpieczeństwa w sektorze publicznym, prywatnym i obywatelskim oraz rekomenduje zadania preparacyjne mające na celu doskonalenie, rozwój i transformację systemu cyberbezpieczeństwa, z uwzględnieniem podsystemu kierowania oraz publicznych i prywatnych ogniw wykonawczych[6].

Obecnie w realizacji jest już kolejny program Strategii Cyberbezpieczeństwa RP opracowany na lata 2017-2022 (*Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2017-2022*). Stanowi on kontynuację działań zapoczątkowanych w programie ochrony cyberprzestrzeni na lata 2011-2016[7]. Jego celem jest implementacja dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. (Dz. U. UE 2016 L 194) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii zwanej dalej Dyrektywą NIS[8]. Główne założenia Strategii zostały skierowane na:

- potrzebę zapobiegania i reagowania w odniesieniu do incydentów oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa,
- stworzenie zasad dobrej współpracy pomiędzy sektorami publicznym i prywatnym,
- umiejętne podejście do oceny ryzyka wystąpienia ataku w cyberprzestrzeni,
- edukację, informację i szkolenie dotyczące cyberbezpieczeństwa,
- działania odnoszące się do planów badawczo-rozwojowych w zakresie bezpieczeństwa teleinformatycznego,
- współpracę międzynarodową w zakresie cyberbezpieczeństwa.

Do podmiotów odpowiedzialnych za zapewnienie bezpieczeństwa cyberprzestrzeni w Polsce zalicza się Ministerstwo Spraw Wewnętrznych, Ministerstwo Administracji i Cyfryzacji, Ministerstwo Obrony Narodowej, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego oraz podmioty sektora prywatnego.

---

[6] W *Doktrynie* dostrzeżono też dylemat, jakim jest próba zapewnienia równowagi między środkami bezpieczeństwa a swobodami obywatelskimi. Podkreślono, że działania na rzecz cyberbezpieczeństwa muszą być podejmowane z uwzględnieniem ochrony praw człowieka i obywatela, a także poszanowaniem prawa do wolności słowa oraz prywatności. Proporcjonalność środków bezpieczeństwa w stosunku do zagrożeń powinna być oparta na efektywnej i wiarygodnej analizie ryzyka.

[7] Por. Rządowego Programu Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016, http://bip. msw.gov.pl/bip/programy/19057,dok.html (dostępność 25.10.2015 r.).

[8] Dyrektywa określa, jakim obowiązkom z zakresu bezpieczeństwa będą podlegać operatorzy usług kluczowych (sektory krytyczne, takie jak energetyka, transport, opieka zdrowotna i finanse) oraz dostawcy usług cyfrowych (internetowe platformy handlowe, wyszukiwarki, usługi przetwarzania w chmurze). Dyrektywa wymaga, aby każdy kraj UE posiadał strategię bezpieczeństwa sieci i informacji. Choć Polska posiada bardzo ważny dokument poświęcony cyberbezpieczeństwu (Polityka Ochrony Cyberprzestrzeni), zdecydowanie jakościowo nie spełnia on wymagań postawionych przez dyrektywę. Między innymi brakuje mu jasno określonych celów, priorytetów, konkretnych działań, mechanizmów współpracy, określenia odpowiedzialności poszczególnych aktorów. Dlatego właśnie Ministerstwo Cyfryzacji aktualnie pracuje nad strategią cyberbezpieczeństwa RP.

Odpowiedzialność za przeciwdziałanie i zwalczanie terroryzmu na terytorium RP jest obecnie rozproszona na kilka resortów i instytucji, które nie są w sposób należyty ze sobą skoordynowane. Zakres kompetencji dwóch służb zajmujących się zwalczaniem najpoważniejszej przestępczości terrorystycznej Policji i Agencji Bezpieczeństwa Wewnętrznego powinien zostać na tyle precyzyjnie określony, aby odpowiedzialność tych służb za ściganie poszczególnych rodzajów przestępstw nie budziła wątpliwości. Pozwoli to na bardziej racjonalne wydawanie środków budżetowych, a zarazem będzie zapobiegać sytuacjom, w których służby prowadzą niepotrzebnie działania w tych samych sprawach, podczas gdy inne ważne kwestie pozostają poza obszarem ich zainteresowania. ABW powinno stać się służbą wyspecjalizowaną w przeciwdziałaniu zagrożeniom terrorystycznym, w kontrwywiadzie i w ochronie informacji niejawnych. Ponadto ABW powinno zgodnie z ustawą odpowiadać za ściganie najpoważniejszych przestępstw przeciwko interesom ekonomicznym państwa.

Za kreowanie polityki bezpieczeństwa teleinformatycznego związaną z funkcjonowaniem systemów i sieci teleinformatycznych resortu odpowiada pełnomocnik ministra obrony narodowej do spraw bezpieczeństwa cyberprzestrzeni. Organizatorem systemów i sieci teleinformatycznych jest natomiast Szef Inspektoratu Systemów Informacyjnych. Ważną rolę w obszarze bezpieczeństwa cyberprzestrzeni pełni także Narodowe Centrum Kryptologii, które jako organ SZ RP, zajmuje się wdrażaniem rozwiązań kryptograficznych na potrzeby polskiej administracji publicznej i wojska. Do głównych zadań NCK należy realizacja zadań związanych z prowadzeniem badań, projektowaniem, budową, wdrażaniem, użytkowaniem oraz ochroną narodowych technologii kryptologicznych a także wytwarzanie nowych produktów dla państwa przez zespolenie potencjału naukowego i przemysłowego w obszarze zaawansowanych technologii informatycznych i kryptograficznych (Zarządzenie, 2013, s. 3).

W Polsce dwie agencje odgrywają wiodącą rolę w działaniach antyterrorystycznych Agencja Bezpieczeństwa Wewnętrznego (ABW) (Dz. U., 2002) i Policja (Dz. U., 1990). Chociaż nie jest jasny podział ich obowiązków, te dwie instytucje współpracują ze sobą bardzo ściśle, ponieważ terroryzm stanowi poważne zagrożenie dla dobra publicznego każdego państwa. Agencja Bezpieczeństwa Wewnętrznego jest służbą specjalną, odpowiedzialną za kwestie związane z ochroną bezpieczeństwa wewnętrznego państwa i jego konstytucyjnego porządku. Głównym zadaniem ABW jest zwalczanie różnego rodzaju zagrożenia dla bezpieczeństwa wewnętrznego państwa, takiego jak przestępstwo szpiegostwa, terroryzmu, handlu narkotykami na skalę międzynarodową. Działania pozwalające zapobiegać rozwojowi przestępczości zorganizowanej, wynikają z uprawnień operacyjno-rozpoznawczych oraz dochodzeniowo-śledczych, które pomagają wykryć przestępstwo, a także ścigać jego sprawców. Czynności operacyjno-rozpoznawcze i analityczno-informacyjne natomiast służą głównie w celach pozyskania informacji dla zapewnienia bezpieczeństwa państwa i wspomnianego wcześniej ładu zagwarantowanego Konstytucją RP. Istotne jest jednak, że Agencja Bezpieczeństwa Wewnętrznego, w sprawnym zwalczaniu przestępczości zorganizowanej nie posługuje się żadnymi instrumentami o prawnym podłożu. Wszystko wynika z braku konkretnych uregulowań ustawowych, które miałyby zagwarantować taki status.

Wydział Zwalczania Terroryzmu został założony w Agencji Bezpieczeństwa Wewnętrznego 19 września 2005 r. w związku ze zmianą Rozporządzenia Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. w sprawie instytucji Agencja Bezpieczeństwa Wewnętrznego. Wydział ma za zadanie:

- gromadzenie informacji na temat zjawiska terroryzmu oraz monitorowanie zjawiska terroryzmu na świecie i wynikających stąd zagrożeń dla Polski,
- opracowywanie koncepcji przeciwdziałania zjawiskom związanym z terroryzmem oraz opiniowanie projektów i programów w tym zakresie,
- przygotowywanie informacji i materiałów związanych z problematyką terroryzmu dla potrzeb Ministra – Szefa Międzyresortowego Centrum ds. Zwalczania Przestępczości Zorganizowanej i Międzynarodowego Terroryzmu,
- sporządzanie analiz i prognoz stanu zagrożenia terroryzmem,
- analizowanie przepisów prawnych dotyczących problematyki terroryzmu oraz przygotowywanie propozycji zmian legislacyjnych w zakresie usprawnienia metod i form zwalczania terroryzmu,
- organizowanie szkoleń i konferencji poświęconych problematyce przeciwdziałania terroryzmowi oraz przygotowywanie materiałów edukacyjnych z tego zakresu,
- udział w organizowaniu współpracy z organami innych państw w zakresie przeciwdziałania terroryzmowi.

W ramach funkcjonowania ABW powołano Centrum Antyterrorystyczne Bezpieczeństwa Wewnętrznego (CAT) jako jednostkę koordynacyjno-analityczną w zakresie przeciwdziałania terroryzmowi i zwalczania go. Do głównych jego zadań należy: wspomaganie procesów decyzyjnych w przypadku realnego zagrożenia atakiem terrorystycznym; koordynowanie działań operacyjno-rozpoznawczych w zakresie zwalczania terroryzmu; wykonywanie czynności analityczno-informatycznych w zakresie sporządzania raportów sytuacyjnych i syntetycznych oraz przygotowanie informacji dla kierownictwa państwa; udział w opracowaniu i nowelizowaniu procedur związanych z zarządzaniem kryzysowym na wypadek ataku terrorystycznego; wspomaganie po zamachach terrorystycznych działań służb i instytucji uczestniczących w obronie antyterrorystycznej RP; współpraca z strukturami UE i NATO w tym zakresie.

Warto również zaznaczyć, że z dniem 1 lutego 2008 r. został powołany Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL). Jest to jednostka działająca w strukturach Agencji Bezpieczeństwa Wewnętrznego, a będąca częścią Departamentu Bezpieczeństwa Teleinformatycznego. Jej główną misją jest nauka i szkolenie, instytucji państwowych funkcjonujących w Polsce, skutecznej ochrony przed atakami z sieci. Jednakże do jej zadań należy również: koordynowanie reakcji na zdarzenia dotyczące ataków w Internecie, wydawanie i ogłaszanie alarmów, zajmowanie się przyjętymi zgłoszeniami, w tym kompletowanie dowodów przez specjalnie powołany do tego zespół biegłych sądowych, zajmowanie się incydentami w systemach, które znajdują się pod ochroną ARAKIS-GOV, wykonywanie badań dotyczących bezpieczeństwa w sieci (www.cert.gov, 2013).

Działalność zespołu zaowocowała stworzeniem systemu ARAKIS-GOV jako narzędzia służącego do wczesnego ostrzegania o zagrożeniach w sieci Internet oraz wdrożeniem Programu badania bezpieczeństwa witryn internetowych administracji publicz-

nej, stosowanego do określanie poziomu bezpieczeństwa aplikacji „www" instytucji publicznych oraz usuwania wykrytych nieprawidłowości, zanim zostaną wykorzystane przez cyberprzestępców (Młotek, Siedlarz, 2011, s. 161).

Jako szczególnie ważną i konieczną należy uznać propozycję ustalenia odpowiedzialności za ochronę cyberbezpieczeństwa RP, z podaniem zakresów zadań, odpowiedzialności i zmian w strukturach organizacyjnych niektórych organów administracji (w tym: Prezesa Rady Ministrów, Ministra Spraw Wewnętrznych, Ministra Obrony Narodowej, Agencji Bezpieczeństwa Wewnętrznego) oraz powołania pełnomocników ds. ochrony cyberprzestrzeni (pełnomocnika rządu, pełnomocników w podmiotach administracji, zalecenie utworzenia takiej roli u przedsiębiorców). Działania te przyczyniłyby się do stworzenia trwałego systemu koordynacji i wymiany informacji, pomiędzy podmiotami odpowiedzialnymi za ochronę cyberprzestrzeni oraz władającymi zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa.

Centralne Biuro Śledcze Policji (CBŚP)[9], które zajmuje się najpoważniejszymi przestępstwami zorganizowanymi o charakterze transgranicznym, kryminalnym, narkotykowym i ekonomicznym oraz terroryzmem zastąpiło Centralne Biuro Śledcze KGP, czyli komórkę organizacyjną dotychczas funkcjonującą w strukturze Komendy Głównej Policji na podstawie nowelizacji ustawy o policji z dnia 26 czerwca 2014 r. (Dz. U. 2014). Inne instytucje biorące udział w antyterrorystycznej działalności to: Agencja Wywiadu (AW) (Dz. U. 2002); Generalny Inspektor Informacji Finansowej (GIIF)[10]; Wojskowe Służby Informacyjne (WSI)[11]; Straż Graniczna (SG)[12]; Biuro Ochrony Rządu (BOR)[13].

---

[9] Komendant CBŚP jest powoływany i odwoływany przez Ministra Spraw Wewnętrznych na wniosek Komendanta Głównego Policji. Zastępców nowej jednostki będzie powoływał szef Policji, na wniosek Komendanta Centralnego Biura Śledczego Policji. Centralne Biuro Śledcze Policji będzie funkcjonowało na wzór komend wojewódzkich oraz komendy stołecznej. Komendant CBŚP będzie posiadał uprawnienia m.in. w zakresie czynności operacyjno-rozpoznawczych dotyczących kontroli operacyjnej oraz odnoszących się do czynności kontrolowanego przejęcia przedmiotów pochodzących z przestępstwa, czynności kontrolowanego wręczenia korzyści majątkowej, przedłużania tych czynności i ich kontynuowania oraz przekazywania prokuratorowi zgromadzonych materiałów. Komendant nowej jednostki będzie mógł także występować z wnioskami o udostępnienie danych telekomunikacyjnych oraz danych osób korzystających z usług pocztowych. Patrz szerzej: E.M. Guzik-Makaruk, *Regulacje prawne przewidziane w prawie policyjnym*, [w:] *Przestępczość zorganizowana*, pod. red. E.W. Pływaczewskiego, Wydawnictwo C.H. Beck, Warszawa 2011, s. 281 i n.

[10] Swoje uprawnienia uzyskał dzięki ustawie o przeciwdziałaniu z dnia 16 listopada 2000 r. (Dz. U. z 2003 r., Nr 153, poz. 1505 z późn. zm.). GIIF ma z kolei za zadanie zapobiegać potencjalnemu przestępstwu finansowania terroryzmu określonego w art.165a k.k. Na podstawie przepisów ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu uzyskuje, gromadzi, przetwarza i analizuje informacje, które mogą mieć związek m. in. z finansowaniem terroryzmu.

[11] Powstały w 1991 z przekształcenia Wojskowych Służb Wywiadowczych (WSW). Początkowo działały na podstawie zarządzenia ministra obrony narodowej wydanego na mocy ustawy o powszechnym obowiązku obrony RP.

[12] Została powołana na podstawie ustawy z 12 października 1990 r. (Dz. U. 2005 Nr 234, poz. 1997 ze zm.). Do jej zadań należy zapobieganie nielegalnym migracjom osób podejrzanych o działalność terrorystyczną, przechwytywanie nielegalnych transportów zawierających szkodliwe substancje chemiczne, materiały jądrowe i wybuchowe.

[13] Powstało na mocy ustawy z dnia 16 marca 2001 r. (Dz. U. 2004 Nr 163, poz. 1712 z późn. zm.). Jego podstawowym zadaniem jest ochrona osób, obiektów i urządzeń służących użyteczności publicznej, a mo-

Agencja Wywiadu działa zapewniając bezpieczeństwo zewnętrzne państwa za pośrednictwem konkretnego katalogu zadań, wyliczonych w ustawie o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Do zadań tych wliczane jest zgodnie z art. 6 ust. 1 ustawy :

1) uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego;

2) rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczypospolitej Polskiej;

3) rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej;

4) rozpoznawanie międzynarodowego obrotu bronią, amunicją i materiałami wybuchowymi, środkami odurzającymi i substancjami psychotropowymi oraz towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także rozpoznawanie międzynarodowego obrotu bronią masowej zagłady i zagrożeń związanych z rozprzestrzenianiem tej broni oraz środków jej przenoszenia.

Dodatkowo, należy tu wymienić dwa inne organa, które nie biorąudział w działaniach operacyjnych: Rada Bezpieczeństwa Narodowego (RBN) oraz Biuro Bezpieczeństwa Narodowego (BBN). RBN jest organem doradczym Prezydenta Rzeczypospolitej Polska i jest odpowiedzialne za określenie generalnego planu i celów dotyczących bezpieczeństwa, stosunków międzynarodowych i sił zbrojnych. Biuro Bezpieczeństwa Narodowego jest częścią Kancelarii Prezydenta i w myśl art. 11 ustawy o powszechnym obowiązku obrony RP (Dz. U. 2012) zapewnia mu wsparcie w zakresie wypełniania zadań odnośnie nienaruszalności granic i niepodległości naszego państwa.

## Wnioski

Zauważyć można tendencję przechodzenia od tradycyjnej formy terroryzmu sponsorowanego przez rządy do modelu, w którym Internet i inne nowoczesne technologie są wykorzystywane m.in. do propagandy, zbierania funduszy i rekrutacji nowych członków.

Internet, z uwagi na globalny zasięg, może być wykorzystywany do wzniecania niepokojów, szerzenia nienawiści, jak i do prowadzenia wojny psychologicznej. Motywy przewodnie propagandy terrorystów to: deprecjonowanie przeciwnika i dyskredytacja jego sił oraz gloryfikacja wysiłku własnego. Ważne jest też rozprzestrzenianie wśród islamistów przeświadczenia o tym, iż ich państwo jest miejscem wojny między chrześcijaństwem a islamem oraz nakłanianie rządów do wycofania się wojsk z Bliskiego Wschodu.

---

gących stać się potencjalnym celem ataku terrorystycznego. Stąd też ochronie BOR podlegają: Prezydent RP, Premier, Marszałek Sejmu i Senatu, Wicepremier, Minister Spraw Wewnętrznych i Administracji, Minister Spraw Zagranicznych, byli Prezydenci, delegacje państw obcych przebywające na terytorium RP, polskie przedstawicielstwa dyplomatyczne, urzędy konsularne, obiekty i urzędy o szczególnym znaczeniu.

Przy dużej liczbie podmiotów bezpieczeństwa i porządku publicznego zauważalny jest brak pełnej koordynacji w realizacji przypisanych im kompetencji, które często się nakładają. Szczególnie dokuczliwym, w sprawnym funkcjonowaniu tego podsystemu, jest powielanie kompetencji kierowniczych, które powinny zostać wyraźnie określone przez regulacje prawne. Te niedociągnięcia dotyczą zarówno kompetencji organów władzy publicznej szczebla centralnego, jak i terenowego. Często kompetencje organów władzy publicznej są niedookreślone lub określone zbyt ogólnikowo (Pietraś, 2007, s. 65-165).

Konieczne jest zatem stworzenie odpowiednich przepisów prawnych gwarantujących zintegrowane, kompleksowe i uporządkowane działania; kształtujących pożądaną strukturę organizacyjną, kompetencje służb; zasady koordynacji działania; siły i środki; łączność; zasady finansowania oraz obszary edukacji służb i społeczeństwa. Powinny one uwzględniać także nowe zjawiska przestępcze i nowe narzędzia jej zwalczania.

Przede wszystkim zaś powinny precyzyjnie określać odpowiedzialność poszczególnych instytucji, zasady i procedury koordynowanych przez nich zadań oraz zasady odpowiedzialności. Wydaje się, że w poszczególnych obszarach bezpieczeństwa i porządku publicznego niezbędne jest wyznaczenie liderów, instytucji specjalizujących się w gromadzeniu wiedzy (teoretycznej i praktycznej) z danego zakresu oraz koordynacji działań wszystkich elementów podsystemu obronno-ochronnego. Najlepszym tego przykładem jest zwalczania przestępczości zorganizowanej, z precyzyjnym określeniem wiodącej roli w realizacji tego zadania. Dziś zdarzają się obszary przestępczości, którymi zainteresowane są prawie wszystkie podmioty, przykładowo: terroryzm, nielegalny obrót bronią i amunicją, przestępstwa korupcyjne, przestępczość finansowa, narkotyki (Oleksiewicz, 2015,. s. 96-107).

Występująca w Polsce wielość podmiotów, a więc rozproszenie kompetencyjne, utrudnia kompleksowe rozpoznanie i identyfikację tego zagrożenia oraz efektywne dysponowanie siłami i środkami w celu przeciwdziałania tej przestępczości. Brak jednolitego sposobu rozliczania, ewidencjonowania i porównywania osiąganych wyników, w kontekście nakładania się właściwości poszczególnych służb i podmiotów powodują brak możliwości obiektywnej i porównywalnej oceny ich skuteczności (Gryz, 2016, s. 127-128).

Zlikwidować należy Kolegium ds. Służb Specjalnych. Istnienie tej instytucji wydaje się sugerować specjalny status służb specjalnych w państwie, co w sytuacji dzisiaj faktycznego, a w przyszłości również *de iure*, ich podporządkowania ministrom konstytucyjnym nie znajduje uzasadnienia. Kolegium jest obecnie instytucją czysto fasadową.

Należałoby ujednolicić uprawnienia funkcjonariuszy różnych służb, procedury ich działania oraz pragmatyki służbowe. W rezultacie powinna być osiągnięta sytuacja pozwalająca efektywnie dysponować posiadanym zasobem osobowym służb specjalnych, przy założeniu wymienności personelu pomiędzy służbami, jak i w procesie współdziałania. Na tym tle rozważyć należy propozycję uwolnienia służb specjalnych od obowiązków procesowych (powinny zostać przejęte przez CBŚ) i ograniczyć ich aktywność tylko do śledztw proaktywnych, tj. takich, które zmierzają do uprawdopodobnienia faktu popełnienia przestępstwa.

## BIBLIOGRAFIA


Adamczuk M., Riedel K., (2015), *Doktryna Cyberbezpieczeństwa RP,*[w:] Przegląd Bezpieczeństwa Wewnętrznego 12/2015.

Aleksandrowicz T., (2008), *Terroryzm międzynarodowy*, Wyd. Akademickie i Profesjonalne, Warszawa.

Białoskórski R., (2011), *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa.

Denning D., (2000), *Cyberterrorism*, Global Dialogue, Autumn.

Denning D., (2017), *Is Cyber Terror Next?,* www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc.

Depa M., Pomykała M., (2014), Instytucjonalne aspekty przeciwdziałania cyberprzestępczości [w:] I. Oleksiewicz, M. Polinceusz, M. Pomykała (red.), *Nowoczesne technologie – źródło zagrożeń i narzędzie ochrony bezpieczeństwa*, Rzeszów.

Dz. U. z 2010 Nr 29, poz. 154.

Dz. U. UE 2016 L194.

Dz. U. 1990, Nr 30, poz. 179 ze zm.

Dz. U. z 2012 r. poz. 461 z późn. zm.

Dz. U. z 2002 r. Nr 93, poz. 829.

Dz. U. z 2014 r. Nr 0, poz. 1199.

Dz. U. z 2003 r., Nr 153, poz. 1505 z późn. zm.

Dz. U. 2004 Nr 163, poz. 1712 z późn. zm.

Dz. U. 2005 Nr 234, poz. 1997 ze zm.

e-Terroryzm.pl, nr 5/2013.

Gniadek A., (2009), *Cyberprzestępczość i cyberterroryzm – zjawiska szczególnie niebezpieczne* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm. Nowe wyzwania XXI wieku*, Warszawa.

Gryz J. (red.) (2016), *Zarys teorii bezpieczeństwa państwa*, Warszawa.

Kosiński J., Waszczuk A., (2015), *Cyberterroryzm a cyberprzestępczość* [w:] P. Bogdalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel (red.) *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, Warszawa.

Liedel K., Piasecka P. (2011), *Wojna cybernetyczna-wyzwanie XXI wieku,* Bezpieczeństwo Narodowe 1/2011.

Littlejohn Shinder D., Tittel E., (2004), *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Wyd. Helion.

Maj P., (2017), *Cyberterroryzm w stosunkach międzynarodowych*, [w:] http://www.politologia.pl/fck_pliki/File/consensus/consensus_1.pdf (15.04.2017).

Młotek M., Siodlarz M., (2011), *Rządowy Zespół Reagowania na Incydenty Komputerowe. CERT.GOV.PL,* Przegląd Bezpieczeństwa Wewnętrznego nr 4/2011.

Mockatis T.R., (2008), The New Terrorism: Myths and Realists, Stanford University Press.

Oleksiewicz I., (2016), *Polskie prawo karne w zakresie walki z cyberprzestępczością na tle standardów prawa UE* [w:] M. Pietraś, H. Chałupczak, J. Misiągiewicz (red.), *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa*, Zamość.

Oleksiewicz I. i in., (2015), *Bezpieczeństwo ekonomiczne w aspekcie zagrożeń współczesnego świata*, Rzeszów.

Oleksiewicz I., (2015), *Polska polityka antyterrorystyczna na tle standardów Unii Europejskiej*, [w:] „Przegląd Prawa Publicznego" nr 6, Warszawa.

Pietraś M., (2007), *Bezpieczeństwo międzynarodowe* [w:] M. Pietraś (red.), *Międzynarodowe stosunki polityczne*, Lublin.

Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2017-2022, https://mc.gov.pl/aktualnosci/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022 (dostępność 10.04.2017 r.).

Rządowy Programu Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016, http://bip.msw.gov.pl/bip/programy/19057,dok.html (dostępność 25.10.2015 r.).
Siwicki M., (2013), *Cyberprzestępczość*, Warszawa.
Skowera D., (2006), *Akademia Cyberpolicyjna – Policja i organizacje międzynarodowe wobec wyzwań przestępczości internetowej*, „Zarządzanie publiczne" [w:] Zeszyty Naukowe ISP UJ 2/2006.
Suchorzewska A., (2010), *Ochrona prawna systemów informatycznych*, Warszawa.
Verton D. (2004), *Black ice. Niewidzialna groźba cyberterroryzmu*, Katowice.
www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-
www.cert.gov.pl/portal/cer/27/15/O_nas.html (dostępność 25.10.2013 r.).
Zarządzenie nr 10/2013 Ministra Obrony Narodowej z dnia 29 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce