Doctrina
Studia Społeczno-Polityczne
14/2017
PL ISSN 1730-0274

Izabela Oleksiewicz
Politechnika Rzeszowska, Wydział Zarządzania

Cyberterroryzm jako naczelne wyzwanie dla systemu bezpieczeństwa narodowego RP

Cyberterrorism as a major challenge to the national security system of the Republic of Poland

Abstrakt: Ogromna dynamika współczesnego świata sprawia, że dokonując interpretacji aktów prawnych nie można ograniczać się do ich literalnego brzmienia. Warto posługiwać się wykładnią dynamiczną, która pozwala uwzględnić rzeczywisty stan rzeczy, chyba że sprzeciwia się temu wyraźnie brzmienie przepisu. Jednocześnie nie należy zapominać o innych regulacjach prawnych dotyczących problematyki bezpieczeństwa co nieraz powoduje sporą trudność interpretacyjną. Gwałtowny rozwój technologii teleinformatycznych pod koniec XX w. stał się przyczyną znacznego zmniejszenia odległości między ludźmi. Informacje dotychczas zdobywane w mozolny sposób stają się dostępne w krótkim czasie zarówno dla tych, dla których stanowią one źródło wiedzy, jak i dla tych, którzy traktują je jako narzędzie przeciwko innym. Umiejętnie prowadzona polityka bezpieczeństwa informacyjnego staje się zatem gwarantem bezpieczeństwa militarnego, finansowego, gospodarczego, zarówno w skali lokalnej, jak i na arenie międzynarodowej, co znajduje odpowiedź w opracowanych i wdrażanych przez państwo polskie strategiach oraz programach rządowych w zakresie bezpieczeństwa informacyjnego. Założeniem niniejszej publikacji jest ukazanie braku istnienia regulacji prawnych jednoznacznie sankcjonujących funkcjonowanie sformalizowanej struktury organizacyjnej o nazwie: system bezpieczeństwa narodowego przy jednoczesnym wskazaniu, że 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. Należy więc stwierdzić, że polityka antycyberterrorystyczna Polski jest nie tylko odpowiedzią, ale

i naczelnym wyzwaniem dla poprawnego funkcjonowania systemu bezpieczeństwa narodowego RP.

W publikacji Autorka rozważa zmianę struktury aparatu państwowego odpowiedzialnego za sprawy wewnętrzne. Stara się przedstawić czytelnikowi wady i zalety zmian, jakie jej zdaniem są konieczne w polskiej rzeczywistości.
Słowa kluczowe: cyberterroryzm, bezpieczeństwo narodowe RP, polityka antycyberterrorystyczna

Abstract: Taking also into account the enormous dynamics of today's world, interpretation of legal acts cannot be limited to their literal interpretation. It is worth to use a dynamic one that allows to take into account the actual state of affairs, unless the wording of the provision is clearly opposed. At the same time, it is important not to forget about the others legal regulations concerning safety issues which often cause considerable interpretation difficulties. The rapid development of information and communication technology at the end of the twentieth century has led to a significant reduction in distance between people. The information so far obtained in a laborious manner becomes available in a short time both for those for whom they are a source of knowledge and for those who treat it as tool against the others. A well-guided information security policy is thus becoming a guarantor of military, financial and economic security, both locally as well as internationally, which is reflected in governmental strategies and governmental programs in information security. The purpose of this publication is to show the absence of legal regulations that explicitly sanction the functioning of a formal organizational structure called the national security system while indicating that the cause of anti-cyberterrorist policy is also the lack of appropriate mechanisms and regulations in this regard, so we are dealing with process of institutionalization. It should be stated that the anti-terrorist policy of Poland is not only an answer but also a major challenge for the proper functioning of the national security system of Poland.

In this publication the Author discusses the change in the structure of the state apparatus responsible for internal affairs. The Author tries to present to a reader the advantages and disadvantages of the changes which in her opinion are necessary in Polish reality.
Keywords: cyberterrorism, national security of Poland, anti-cyberterrorism policy

Podstawy prawne kierowana bezpieczeństwem narodowym Polski

Na samym wstępie należałoby się zastanowić nad umiejscowieniem w systemie prawa unormowań dotyczących bezpieczeństwa narodowego. Analizując regulacje prawne z tego obszaru można, po pierwsze, wskazać na celowościowy charakter norm prawnych w tym zakresie. Podstawowe znaczenie w tym zakresie mają regulacje

normatywne, zawarte w art. 2 Konstytucji RP[1], który stanowi, że *Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społeczne*j. W związku z tym Rzeczpospolita Polska, jako państwo prawne, powinna posiadać stosowne rozwiązania normatywne pozwalające na optymalne i długotrwałe zapewnienie społeczeństwu braku stanu zagrożenia. Kolejna podstawa prawna wynika z art. 5 Konstytucji stanowiącego, że *Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju* oraz art. 31 ust. 3 stwierdzającego, że *ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw*[2].

Z kolei, art. 134 Konstytucji określa kompetencje Prezydenta RP w dziedzinie bezpieczeństwa i obronności państwa[3]. Ustanawia

---

[1] Dz.U. z 1997 r., nr 78, poz. 483 z późn. zm.

[2] G.L. Seidler, H. Groszczyk, J. Malarczyk, A. Pieniążek, *Wstęp do nauki o państwie i prawie*, Lublin 2009, s. 163–164. Patrz też: W. Kitler, M. Czuryk, M. Karpiuk, *Aspekty prawne bezpieczeństwa narodowego RP. Część szczegółowa,* Warszawa 2013, s. 14.

[3] Strategia obronności z 2009 r. w pkt 57 wprowadziła pojęcie „systemu obronnego państwa" o następującej treści: *System obronny państwa stanowi skoordynowany zbiór elementów kierowania i elementów wykonawczych, a także realizowanych przez nie funkcji i procesów oraz zachodzących między nimi relacji. SOP tworzą wszystkie siły i środki przeznaczone do realizacji zadań obronnych, odpowiednio do tych zadań zorganizowane, utrzymywane i przygotowywane*. Z kolei, od 2004 roku w strukturze SOP występował podsystem kierowania bezpieczeństwem narodowym, w tym obroną państwa. Natomiast wymieniona wyżej strategia obronności wprowadziła pojęcie podsystemu kierowania obronnością państwa. Z powyższego wynika, że mamy do czynienia z dylematem organizacyjno-prawnym, na który nakłada się kwestia tworzenia systemu kierowania bezpieczeństwem narodowym wynikającego z regulacji art. 6 ust. 1 pkt 3 oraz ust. 2 pkt 2 ustawy o powszechnym obowiązku obrony RP. Nowa Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej została przyjęta 5 listopada 2014 r., a jej treści są rozwijane w Polityczno-Strategicznej Dyrektywie Obronnej Rzeczypospolitej Polskiej oraz Strategii Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej Szerzej: S. Koziej, *Prezydentura Bronisława Komorowskiego – synteza działalności w dziedzinie bezpieczeństwa narodowego RP*, Kwartalnik „Bezpieczeństwo Narodowe" 2014, nr 34, s. 15.

najwyższe zwierzchnictwo Głowy Państwa nad Siłami Zbrojnymi. Należy też zauważyć, że przepisy o podległości wojska Głowie Państwa znajdują się w wielu państwach i ich konstytucjach, które odnoszą się do różnych systemów rządów. Samo więc przyznanie Prezydentowi najwyższego zwierzchnictwa nad Siłami Zbrojnymi RP nie daje mu formalnie dodatkowych, czy też szczególnych uprawnień i możliwości wpływania na kształt polityki obronnej państwa[4].

Ponadto, ustawa z dnia 5 marca 2015 r.[5] doprecyzowuje kompetencje Naczelnego Dowódcy Sił Zbrojnych – organu wykonawczego Prezydenta RP w zakresie kierowania obroną państwa. Ma on podlegać bezpośrednio głowie państwa, a w jego kompetencjach będą wyłącznie kwestie związane z obroną państwa. Utrwalone zostały również główne zadania tzw. kandydata na stanowisko Naczelnego Dowódcy Sił Zbrojnych. Powinien on m.in. uczestniczyć w ćwiczeniach i grach strategicznych, a także brać udział w procesie planowania operacyjnego użycia sił zbrojnych i przygotowania wojennego systemu dowodzenia. Nowe regulacje poszerzają też kompetencje szefa Sztabu Generalnego Wojska Polskiego na czas wojny[6] o wsparcie Prezydenta RP w kierowaniu obroną państwa. Ma to zapewnić merytoryczną ciągłość planowania, przygotowywania i realizacji zadań operacyjnych, także po powołaniu podległego Prezydentowi RP Naczelnego Dowódcy Sił Zbrojnych i przejęciu przez niego dowodzenia.

Natomiast zgodnie z art. 146 ust. 4 pkt 8 i 11 konstytucji, to Rada Ministrów zapewnia bezpieczeństwo zewnętrzne państwa oraz

[4] Uzupełniając zmiany organizacyjne, Prezydent B. Komorowski podpisał 1 kwietnia 2015 r. ustawę o zmianie ustawy o powszechnym obowiązku Obrony Rzeczypospolitej Polskiej, usprawniającą kierowanie obroną państwa w czasie wojny. Nowe przepisy określają m.in. ramy czasowe obowiązywania konstytucyjnego pojęcia „czas wojny". Zgodnie z nowelizacją, o ustanowieniu jego początku i końca – w razie konieczności obrony państwa – postanawiałby Prezydent RP na wniosek Rady Ministrów. W ten sposób precyzyjnie określono przedział czasowy, w którym mogłyby być stosowane istotne z punktu widzenia państwa i obywateli regulacje dotyczące czasu wojny. Szerzej: S. Koziej, *Prezydentura Bronisława Komorowskiego – synteza...*, s. 16.

[5] Ustawa z dnia 5 marca 2015 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. z 2015 r., poz. 529).

[6] Nowe przepisy określają m.in. ramy czasowe obowiązywania konstytucyjnego pojęcia „czas wojny". Zgodnie z nowelizacją, o ustanowieniu jego początku i końca – w razie konieczności obrony państwa – postanawiałby Prezydent RP na wniosek Rady Ministrów. W ten sposób precyzyjnie określono przedział czasowy, w którym mogłyby być stosowane istotne z punktu widzenia państwa i obywateli regulacje dotyczące czasu wojny.

sprawuje ogólne kierownictwo w dziedzinie obronności. Natomiast Prezydent stojący na straży suwerenności i bezpieczeństwa państwa oraz niepodzielności i nienaruszalności jego terytorium (art. 126 ust. 2) – może wpływać na kształt tej polityki, ale decydujący głos należy do rządu. Jedynie w sytuacjach największych zagrożeń (sytuacjach krytycznych dla państwa) konstytucja uzależnia podjęcie określonych decyzji od zgody Prezydenta. Chodzi tu zwłaszcza o możliwość wprowadzenia stanu wyjątkowego i wojennego.

Po drugie, należy podzielić uwagę o charakterze ogólnym odnoszącą się do wszystkich norm konstytucyjnych zawartych w Konstytucji Rzeczypospolitej Polskiej w zakresie bezpieczeństwa i obronności państwa oraz zakresu kompetencji w tym zakresie naczelnych organów. Uwaga ta odnosi się do potrzeby uregulowania, przy ewentualnych pracach nad zmianą konstytucji, swego rodzaju uporządkowania kwestii, dotyczących bezpieczeństwa i obronności państwa oraz Sił Zbrojnych RP w odrębnym rozdziale konstytucji. Konstytucja również powinna w sposób niebudzący żadnych wątpliwości, jasny, logiczny i precyzyjny określać zasady podległości Sił Zbrojnych RP konstytucyjnym organom państwowym oraz określać kompetencje tychże organów w sferze obronności i bezpieczeństwa państwa, zwłaszcza w czasie wojny.

Po trzecie, dokonując analizy norm prawnych nie można ograniczać się do ich literalnego brzmienia. Często konieczna jest wykładnia rozszerzająca w celu pełnej konstrukcji norm prawnych. Nie należy zapominać o innych regulacjach oprawnych dotyczących problematyki bezpieczeństwa[7] co nieraz powoduje sporą trudność interpretacyjną.

Po czwarte, w toku interpretacji aktów prawnych należy posługiwać się wykładnią dynamiczną, która pozwala interpretującego uwzględnić rzeczywisty stan rzeczy, biorąc również pod uwagę ogromną dynamikę dzisiejszego świata, chyba, że sprzeciwia się temu wyraźnie brzmienie przepisu[8].

Ważniejszą kwestią, a także dylematem jest odpowiedź na pytanie, czy system obronny państwa można traktować zamiennie jako

[7] I. Oleksiewicz, *Znaczenie norm prawnych w systemie bezpieczeństwa narodowego RP*, [w:] J. Gryz (red.) *Zarys teorii bezpieczeństwa państwa*, Warszawa 2016, s. 112.
[8] Wyrok SN z dnia 16 maja 2001 r., I PKN 389/2000, OSNP 2003/5, poz. 119.

system bezpieczeństwa narodowego. Odpowiedź jest jednoznacznie przecząca – nie. Stwierdzić jednak należy, że jest on obecnie najdoskonalszą formą organizacyjną odrębnego systemu działającego w obszarze bezpieczeństwa narodowego, a co za tym idzie najlepszą podstawą do budowania Systemu Bezpieczeństwa Narodowego. W konsekwencji można więc stwierdzić, że w Polsce podejmuje się działania z zakresu bezpieczeństwa narodowego, do których istnieją podstawy prawne[9].

Kolejną ważną kwestią konstytucyjną w zakresie bezpieczeństwa i obronności państwa jest problem związany ze stanem wojny, który zgodnie z konstytucją nie jest uważany za jeden ze stanów nadzwyczajnych. Artykuł 116 Konstytucji ujmujący kwestię stanu wojny znajduje się w rozdziale IV, regulującym pozycję ustrojową Sejmu i Senatu[10], a więc poza rozdziałem o stanach nadzwyczajnych. W zamierzeniu twórców konstytucji ma on regulować wyłącznie relacje międzynarodowe Rzeczypospolitej Polskiej, natomiast skutki ogłoszenia stanu wojny w prawie wewnętrznym ma regulować stan wojenny jako jeden ze stanów nadzwyczajnych. Tezę te potwierdzają przesłanki ogłoszenia stanu wojny i wprowadzenia stanu wojennego, przy czym w przypadku zewnętrznego zagrożenia państwa, możemy mieć do czynienia jedynie z przesłanką wprowadzenia stanu wojennego, a nie ogłoszenia stanu wojny. Mając z kolei na uwadze relacje, jakie zachodzą między stanem wojny a stanem wojennym można stwierdzić, że do dnia dzisiejszego nie do końca jest zrealizowane powiązanie skutków ogłoszenia stanu wojny z aktem wprowadzenia stanu wojennego[11].

Analiza przepisów prawa w zakresie bezpieczeństwa narodowego RP prowadzi z kolei do wniosku, że:

1) w rozumieniu prawa RP zapewnienie bezpieczeństwa jest jednym z zasadniczych celów narodowych;

---

[9] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, s. 18. Por też: W. Fehler, I.T. Dziubek, *Bezpieczeństwo wewnętrzne państwa. Ekspertyza przygotowana na zlecenie Ministerstwa Rozwoju Regionalnego*, Narodowa Strategia Spójności, Warszawa 2010.

[10] Por. B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, wyd. 2, Warszawa 2012, s. 1087 i n.

[11] Por. T. Bryk, Przegląd *regulacji stanów nadzwyczajnych w przepisach Konstytucji RP*, „Przegląd Prawa Konstytucyjnego" 2011, nr 1, s. 225–226.

2) brak jest jednak regulacji prawnych sankcjonujących istnienie sformalizowanej struktury organizacyjnej o nazwie: system bezpieczeństwa narodowego;
3) znaczący postęp organizacyjny występuje w zakresie budowania jednolitego systemu kierowania bezpieczeństwem narodowym;
4) ze względu na brak spójności przepisów prawa i jednolitości organizacyjnej, dostrzega się brak efektu systemowego w osiąganiu celów bezpieczeństwa narodowego;
5) z powyższych powodów występuje również brak więzi między potencjalnymi elementami równie potencjalnego systemu bezpieczeństwa narodowego;
6) mimo uchybień, o których mowa wyżej, to właśnie dzięki istnieniu stosownych przepisów prawa realizowane są w Polsce cele i interesy bezpieczeństwa narodowego;
7) istnieją regulacje prawne sankcjonujące funkcjonowanie szczegółowych systemów bezpieczeństwa w ogóle, m.in. systemów: obronnego państwa; ochrony granicy państwowej; ochrony informacji niejawnych; ochrony państwa i porządku konstytucyjnego; ochrony przeciwpożarowej; ratowniczo-gaśniczy; Państwowe Ratownictwo Medyczne; ochrony danych osobowych;
8) w wykonaniu postanowień stosownych ustaw przyjęto odpowiednie strategie, m.in.: Strategię bezpieczeństwa narodowego RP czy Strategię obronności RP;
9) w realizacji celów bezpieczeństwa narodowego, dzięki istnieniu stosownych przepisów prawa krajowego korzysta się z licznych środków i narzędzi polityki bezpieczeństwa;
10) prawo konstytucyjne i inne gałęzie prawa oraz poszczególne rodzaje prawa regulującego bezpośrednio dziedzinę bezpieczeństwa narodowego umożliwiają podjęcie stosownych kroków organizacyjnych w celu zbudowania stosownego systemu; jedyna przeszkoda tkwi w braku stosownej woli politycznej;
11) złożoność regulacji prawnych w dziedzinie bezpieczeństwa narodowego potwierdza opinię, że rozpatrywanie poszczególnych jego dziedzin (rodzajów) powinno mieć przede wszystkim charakter teoretyczno-poznawczy, gdyż związki między nimi o charakterze normatywnym, organizacyjnym i funkcjonalnym są wyraźne i procesowo coraz bardziej złożone;

12) jedną z formalnych przeszkód we właściwym rozumieniu bezpieczeństwa narodowego oraz – w konsekwencji – w budowaniu wspomnianego wyżej systemu jest - niestety - brak instytucjonalnych możliwości do prowadzenia szczegółowych i interdyscyplinarnych analiz jego stanu[12].

Kompetencje prawne służb i organów ochrony państwa w zakresie bezpieczeństwa narodowego Polski

W 2002 roku przeprowadzono reformę służb rozwiązując Urząd Ochrony Państwa i powołując w to miejsce Agencję Bezpieczeństwa Wewnętrznego i Agencje Wywiadu[13]. Pierwsza została właściwą „w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego", druga „w sprawach ochrony bezpieczeństwa zewnętrznego państwa". Ustawa definiuje szefów ABW[14] i AW[15] jako centralne organy administracji rządowej, podległe bezpośrednio Prezesowi Rady Ministrów. Szefowie ABW i AW działają przy pomocy Agencji, które są „urzędami administracji rządowej".

---

[12] Por. I. Oleksiewicz, *Znaczenie norm prawnych w systemie bezpieczeństwa narodowego RP…,* s. 120.

[13] Ustawa z 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (t.j. Dz.U. z 2010 r., nr 29; poz. 154).

[14] 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. 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. W ramach funkcjonowania ABW powołano Centrum Antyterrorystyczne Bezpieczeństwa Wewnętrznego (CAT) jako jednostkę koordynacyjno-analityczną w zakresie przeciwdziałania terroryzmowi i zwalczania go.

[15] Agencja Wywiadu działa zapewniając bezpieczeństwo zewnętrzne państwa za pośrednictwem konkretnego katalogu zadań, wyliczonych w ustawie o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Zadanie te wliczane są zgodnie w art. 6 ust. 1 ustawy.

Tak samo ustawodawca określił pozycję ustrojową i generalne zadania „przed zagrożeniami wewnętrznymi", oraz „przed zagrożeniami zewnętrznymi powołanych ustawą z 9 czerwca 2006 roku Służby Kontrwywiadu Wojskowego (SKW) i Służby Wywiadu Wojskowego(SWW[16]. Podlegają one Ministrowi Obrony Narodowej, jednakże „z zastrzeżeniem określonych w ustawie uprawnień Prezesa Rady Ministrów lub Ministra-koordynatora służb specjalnych, w przypadku jego powołania" (art. 3 ustawy). Ustawą z tego samego dnia powołano Centralne Biuro Antykorupcyjne, także sytuując jego szefa jako centralny organ administracji rządowej, jednoznacznie podległy Prezesowi Rady Ministrów[17]. W tych trzech ustawach pojawia się wyraźne określenie, że formacje te są „służbą specjalną".

Ocenę funkcjonowania służb utrudnia także nieprecyzyjnie rozdzielone (nakładające się) kompetencje[18]. Jasny jest podział pomiędzy służby cywilne i wojskowe. Przedmiot zainteresowań tych drugich został wyraźnie zawężony poprzez dodanie zwrotu, że są to służby właściwe „w sprawach ochrony przed zagrożeniami dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP (…) oraz jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej" (art. 1 i 2 ustawy).

Natomiast sam podział zadań i kompetencji nie jest już tak jasny. Stosunkowo mało wątpliwości budzi ich sprecyzowanie je w odniesieniu do służb strzegących bezpieczeństwa zewnętrznego. Tylko w dwóch przypadkach możemy mówić o nakładaniu się zadań. Jeden dotyczy rozpoznania międzynarodowego obrotu bronią, materiałami i technologiami „o znaczeniu strategicznym dla bezpieczeństwa państwa" oraz międzynarodowego obrotu bronią masowej zagłady[19]. Drugi przypadek to „rozpoznawanie i analizowanie zagrożeń

[16] Powstały w 1991 r. z przekształcenia Wojskowych Służb Wywiadowczych (WSW). Ustawa z 9 czerwca 2006 roku o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego (Dz.U. z 2009 r., nr 85, poz.716).
[17] Ustawa z 9 czerwca 2006 roku o Centralnym Biurze Antykorupcyjnym (t.j. Dz.U. z 2011 r., nr 171, poz.1016).
[18] Por. I. Oleksiewicz, *Rola instytucji w walce z cyberterroryzmem w Polsce* [w:] I. Oleksiewicz, (red.), *Służby i formacje w ochronie bezpieczeństwa państwa*, Oficyna Wydawnicza PRz, Rzeszów 2015, s. 32.
[19] Art. 6, ust 1, pkt 6 ustawy o ABW i AW; art. 6, ust. 1, pkt 3 ustawy o SKW i SWW.

występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych" mających wpływ na bezpieczeństwo państwa (AW) lub na obronność państwa oraz zdolność bojową SZ RP (SWW). Ta zbieżność kompetencyjna da się racjonalnie uzasadnić przy założeniu pełnej wymiany informacji.

Inaczej sytuacja wygląda, jeśli idzie o kompetencje pozostałych służb cywilnych. Występuje tu zjawisko powtarzania się kompetencji oraz pewnej niedbałości legislacyjnej, bowiem niektóre z nich są nazwane wprost, inne są określane poprzez odesłanie do innych ustaw i przepisów w nich zawartych, wskazywanych poprzez numer porządkowy. Jeśli chodzi o dublowanie kompetencji, to najczęściej na służby nakładany jest obowiązek ścigania przestępstw godzących w interesy ekonomiczne państwa – ABW, CBA, a ponadto policja, wywiad skarbowy oraz Żandarmeria Wojskowa w odniesieniu do osób określonych w art. 3, ust.2 ustawy[20].

Istnienie wielu podmiotów działających w ramach ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego, o nakładających się kompetencjach i rozmaitej podległości ustrojowej (obok Premiera trzech ministrów konstytucyjnych nadzoruje służby i policje, dysponujące uprawnieniami operacyjno-rozpoznawczymi oraz umundurowane i uzbrojone), rodzi także pytanie o funkcjonalność przyjętego rozwiązania. Funkcjonalność wspierają bowiem skutecznie przyjmowane instrumenty koordynacji działań oraz spójny zakres uprawnień funkcjonariuszy służb realizujących statutowe czynności.

Instrumentem koordynacji ma być według ustawy prowadzony przez Szefa ABW na potrzeby działań podejmowanych przez służby specjalne tzw. CEZOP (centralna ewidencja zainteresowań operacyjnych). Konstrukcja tego narzędzia nie obejmuje jednak wystarczająco problematyki działalności ustawowej służb. Problematyczne jest wąskie ujęcie tego procesu w zakresie podmiotowym i przedmiotowym. W tym pierwszym przypadku konstrukcja przepisu nie pozwala zintegrować tej bazy z rejestrami zainteresowań innych obok wcześniej wymienionych służb działających w obszarze bezpieczeństwa państwa (np. Policja, Żandarmeria Wojskowa, Straż Graniczna),

[20] Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. z 2011 r., nr 53, poz. 273).

w drugim zaś zawężenie mechanizmu koordynacji do niektórych tylko obszarów zainteresowań (brak koordynacji działań kontrolnych czy procesowych). Tak więc CEZOP wbrew oczekiwaniom ustawodawcy nie wyczerpuje całkowicie procedur koordynacyjnych w dalszym ciągu dopuszczając rozproszenie zasobu informacyjnego służb i dodatkowo wymaga uruchomienia w każdej sytuacji rozległej biurokratycznej procedury rozsyłania korespondencji z zapytaniami do wszelkich możliwych podmiotów ze sfery bezpieczeństwa. W rzeczywistości w istniejącym wymiarze koordynacji, coraz bardziej mamy do czynienia z biurokracją zamiast realnej współpracy.

Kolejnym problemem jest, i to pomimo nakładających się zakresów właściwości rzeczowych, niespójne ujęcie uprawnień służb (np. ABW jest uprawniona do realizacji tzw. prowokacji biernej, a CBA i Policja realizują również prowokację czynną czy też zakres uprawnień Żandarmerii Wojskowej obejmujący pełną gamę instrumentów operacyjnych wraz z uprawnieniami procesowymi w zestawieniu z ograniczonymi w tych zakresach uprawnieniami SKW)[21]. Inną sprawą jest nadmiernie uprzywilejowana rola prokuratury w stosunku do służb specjalnych prowadząca do podporządkowania sobie ich działań i zasobów. Wzrost liczby służb, fasadowość instytucji nadzoru i koordynacji i kolejne modyfikacje systemu, nie idą więc w parze ze wzrostem skuteczności działania i poziomem bezpieczeństwa. Co więcej, stwarzają wręcz iluzję siły systemu. Biorąc pod uwagę aspekty organizacyjno-etatowe oraz finansowanie służb jest to faktycznie strategia rozdrabniania posiadanych zasobów.

Służby są częścią administracji, systemu instytucji mających służyć obywatelowi. Na ich efektywność niebagatelny wpływ ma postrzeganie państwa przez społeczeństwo i zaufanie do jego instytucji. W tym kontekście znaczenie mają takie procesy jak lustracja i kontrowersje wokół niej, kontrowersje wokół weryfikacji funkcjonariuszy byłych WSI, obniżenie emerytur zweryfikowanym pozytywnie byłym funkcjonariuszom SB. Zasada zaufania do państwa i jego instytucji

[21] Szerzej: M. Świderski, B*ezpieczeństwo wewnętrzne i jego uwarunkowania*, [w:] *Bezpieczeństwo państwa,* Konstanty A. Wojtaszczyk, A. Materska-Sosnowska (red.), Warszawa 2009, s. 58. Por. też: I. Oleksiewicz, *Rola instytucji w walce z cyberterroryzmem w Polsce*, [w:] I. Oleksiewicz, (red.), *Służby i formacje w ochronie bezpieczeństwa państwa*, Rzeszów 2015, s. 35.

w efekcie kontrowersyjnego realizowania wymienionych działań uległa głębokiej erozji. Zaufania tego nie buduje również szeroko ujęty w ustawach zakres tzw. immunitetów czyli zakazu podejmowania tajnej współpracy z polskimi służbami specjalnymi przez określone kategorie osób. Zakaz w odniesieniu do reprezentantów władzy ustawodawczej czy sądowniczej jest uzasadniony systemowo. Jednak w odniesieniu do pozostałych grup osób wystarczającą barierą przed patologiami powinny być istniejące w tym względzie przepisy ogólne, w tym przepisy karne sformułowane w rozdziale 10a ustawy o ABW oraz AW.

Należy zmierzać w kierunku ograniczenia liczby służb specjalnych do 2, najwyżej 3 organizacji – wariantowo: – służba wewnętrzna, służba zewnętrzna, ewentualnie kontrwywiad wojskowy; – służba wewnętrzna, służba zewnętrzna i służba w zakresie przestępstw przeciw interesom ekonomicznym państwa (powstała z połączenia CBA i wywiadu skarbowego, zwalczającą korupcję, oszustwa i wyłudzenia podatkowe, przestępstwa giełdowe itp.).

Nadzór nad służbami specjalnymi powinien powrócić na szczebel ministrów konstytucyjnych. W gestii Premiera pozostać powinny kwestie kadrowe dotyczące kierownictw służb. Koordynację działań służb powierzyć należy ministrowi właściwemu w sprawach wewnętrznych.

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[22]. Pojęcie to odnosi się do bezprawnych ataków i zagrożeń wobec komputerów, sieci i informacji przechowywanych w nich celem, których jest zastraszenie lub zmuszenia 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, za poważne ataki na infrastrukturę krytyczną mogą być również uznane za akty cyberterroryzmu, w zależności od ich wpływu. Natomiast ataki, które zakłócające nieistotne usługi lub są przede wszystkim kosztowne do nich nie należą[23].

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 daleko idących politycznych i społecznych celów w szerokim rozumieniu tego słowa[24].

Przytoczone powyżej definicje dowodzą, że cyberterroryzm 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

[22] D. Denning, *Is Cyber Terror Next?,* www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc
[23] D. Denning, *Cyberterrorism*, Global Dialogue, Autumn 2000.
[24] K. Liedel, A. Mroczek, *Terror w Polsce analiza wybranych przypadków,* Warszawa 2013, s. 36.

narzędzie do ich przeprowadzenia. Wydaje się, iż prawdziwa definicja powstaje dopiero po połączeniu obu tych podejść[25].

Mianem „cyberprzestępczości" określa się takie formy posługiwania się sieciami telekomunikacyjnymi, siecią komputerową, Internetem, których celem jest naruszenie jakiegokolwiek dobra chronionego prawem[26]. Cyberprzestępczość od klasycznej przestępczości odróżnia przede wszystkim działanie w środowisku związanym z technologią komputerową i wykorzystanie sieci komputerowych do popełniania przestępstwa[27]. Jej wyróżnikiem nie jest natomiast ochrona jakiegoś jednego wspólnego dobra[28]. 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

[25] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.s. 17.
[26] Zob. R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011, s. 63 i n.; A. Gniadek, *Cyberprzestępczość i cyberterroryzm – zjawiska szczególnie niebezpieczne*, [w:] *Cyberterroryzm. Nowe wyzwania XXI wieku,* red. T. Jemioło, J. Kisielnicki, K. Rajchel, Wyd. WSIZIA, WSPOL, WSO AON, Warszawa 2009, s. 222 i n.; J. Kosiński, A. Waszczuk, *Cyberterroryzm a cyberprzestępczość*, [w:] *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, red. P. Bogdalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel, WSPol, WSIZiA, WSOSP, WIM, Warszawa 2013, s. 333.
[27] M. Siwicki, *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 20.
[28] Ibidem, s. 21.

realizacji innych zadań dodatkowych (np. przechowywania danych uzyskanych w wyniku przestępstwa)[29]. 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[30].

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.

Wnioski i rekomendacje

W świetle obowiązujących w Polsce przepisów nie można jednak jednoznacznie przyjąć, że istnieje formalny system bezpieczeństwa narodowego. U podstaw tej oceny legły wnioski płynące z analizy stanu prawnego, formalnej organizacji struktur realizujących zadania z zakresu bezpieczeństwa, a także relacji zachodzących w sferze kompetencyjnej i funkcjonalnej. Brak jest w Polsce przede wszystkim jednoznacznych regulacji prawnych systemu bezpieczeństwa narodowego (SBN), jeśli mielibyśmy traktować go, jako wyodrębniony ze struktury państwowej, wewnętrznie skoordynowany zbiór elementów organizacyjnych[31].

Przy dużej liczbie podmiotów bezpieczeństwa i porządku publicznego zauważalny jest brak pełnej koordynacji w realizacji przypisanych im kompetencji, które często się nakładają. Szczególnie

[29] D. Littlejohn Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Wyd. Helion 2004, s. 25.
[30] D. Skowera, *Akademia Cyberpolicyjna – Policja i organizacje międzynarodowe wobec wyzwań przestępczości internetowej*, „Zarządzanie publiczne" Zeszyty Naukowe ISP UJ 2/2006, s. 142.
[31] J. Gryz, *Bezpieczeństwo państwa. Władza – Polityka – Strategia*, Wydawnictwo AON, Warszawa 2013, s. 120 i n.

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[32].

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.

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[33].

---

[32] A. Dybczyński, *Teoria sojuszy międzynarodowych*, [w:] K. Kącka (red.), *Stosunki międzynarodowe. Wokół zagadnień teoretycznych*, Toruń 2014, s. 70-89.

[33] Por. Z. Skwarek, *Zarys teorii systemów bezpieczeństwa wewnętrznego państwa*, [w:] J. Gryz (red.) *Zarys teorii bezpieczeństwa państwa*, Warszawa 2016, s. 150-153.

- 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;
- Ujednolicić uprawnienia funkcjonariuszy różnych służb, procedury ich działania i pragmatyki służbowe. W rezultacie osiągnięta być powinna 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;
- Zbudować zintegrowany krajowy system współpracy ewidencji wszystkich zainteresowań i koordynacji działań służb (również realizowanych czynności kontrolnych i procesowych).

Ponadto w zakresie zwalczania przestępczości i ograniczania jej negatywnych skutków rekomenduje się:

- usprawnienie zinstytucjonalizowanych formy wymiany informacji pomiędzy wszystkimi podmiotami bezpieczeństwa poprzez stworzenie bazy danych o przestępczości na poziomie krajowym. Szerzej należy udostępniać i wykorzystywać dane pochodzących z wymiany międzynarodowej oraz współpracy z Europolem, Interpolem, w ramach SIS i poprzez oficerów łącznikowych. System ten powinien spełniać również funkcje analityczne i posiadać zróżnicowany dostęp zgodnie z przyznanymi uprawnieniami. Jego budowa powinna oparta być na hurtowni danych z możliwością wyszukiwania na wzór Systemu Meldunku Informacyjnego/SIO. System ten powinien zastąpić obecne Krajowe Centrum Informacji Kryminalnych, które faktycznie zawiera wyłącznie tzw. dane policyjne. Wprowadzić należy standaryzację danych i systemów pozwalającą na łączenie danych znajdujących się w odrębnych zbiorach, w celu uniknięcia dodatkowych kosztów spowodowanych potrzebą zachowania kompatybilności nowopowstających baz z już istniejącymi,

- wprowadzenie rozwiązań ograniczających zjawisko przestępczości w warunkach recydywy penitencjarnej poprzez wyraźniejsze niż dotychczas zobowiązanie Służby Więziennej do współpracy z policją i innymi służbami chroniącymi bezpieczeństwo i porządek publiczny. Rozważyć trzeba – z zachowaniem wszelkich zasad dotyczących praw osadzonych – wyposażenie SW w ograniczone uprawnienia do pracy operacyjno-rozpoznawczej;
- powołanie współpracy publiczno-prywatnej ds. zwalczania cyberprzestępczości, wraz z opracowaniem (zmianą) regulacji prawnych określających obowiązki i uprawnienia członków, wskazaniem źródeł finansowania, ustaleniem reguł współpracy krajowej i międzynarodowej (podejście międzyinstytucjonalne, a także transgraniczne), włącznie z oszacowaniem ilości przetwarzanych danych i wskazaniem rozwiązań technicznych dla takiej współpracy[34].

W dalszej perspektywie rozważyć warto zmianę struktury aparatu państwowego odpowiedzialnego za sprawy wewnętrzne, w tym dublowanie się niektórych zadań i kompetencji pomiędzy ministrem właściwym w sprawach wewnętrznych, a komendantami głównymi służb. Jedna z propozycji zakłada przekształcenie/likwidację komend głównych (Policji, Straży Granicznej, Państwowej Straży Pożarnej, Służby Więziennej) w departamenty ministerstwa właściwego do spraw wewnętrznych. Inna – ograniczenie zadań operacyjnych tych komend na rzecz wzmocnienia ogniw wojewódzkich lub odpowiednich oraz wzmocnienia analityczno-informacyjnych funkcji komend głównych. Obydwie koncepcje posiadają wady i zalety. Wydaje się, że bliższa polskim realiom jest koncepcja druga, uzupełniona o działania, które odpolitycznią szefów służb i policji, wprowadzając np. kadencyjność niepokrywającą.

Bibliografia

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, wyd. 2, Warszawa 2012.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI*

[34] I. Oleksiewicz, *Institutional aspects of anti-cybernetic policy in Poland* [in:] I. Oleksiewicz, M. Pomykała, M. Polinceusz (ed.), *Institutional and functional aspects of the national security protection*, Rambler Press, Chicago 2014, p. 13-28.

wieku. Zarys problematyki, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011.

Bryk T., Przegląd *regulacji stanów nadzwyczajnych w przepisach Konstytucji RP*, „Przegląd Prawa Konstytucyjnego" 2011, nr 1.

Cymerski J., *Terroryzm a bezpieczeństwo Rzeczypospolitej,* Warszawa 2013.

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

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

Dybczyński A., *Teoria sojuszy międzynarodowych*, [w:] Kącka K. (red.), *Stosunki międzynarodowe. Wokół zagadnień teoretycznych*, Toruń 2014.

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

Gryz J., *Bezpieczeństwo państwa. Władza – Polityka – Strategia*, Warszawa 2013.

Guzik-Makaruk E.M., *Regulacje prawne przewidziane w prawie policyjnym*, [w:] Pływaczewski E.W. (red.), *Przestępczość zorganizowana*, Wydawnictwo C.H. Beck, Warszawa 2011.

Fehler W., Dziubek I.T., *Bezpieczeństwo wewnętrzne państwa. Ekspertyza przygotowana na zlecenie Ministerstwa Rozwoju Regionalnego, Narodowa Strategia Spójności*, Warszawa 2010.

Kitler W., Czuryk M., Karpiuk M., *Aspekty prawne bezpieczeństwa narodowego RP. Część szczegółowa,* Warszawa 2013.

Kosiński J., Waszczuk A., *Cyberterroryzm a cyberprzestępczość*, [w:] Bogdalski P., Nowakowski Z., Płusa T., Rajchel J., Rajchel K. (red.), *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, Warszawa 2013.

Koziej S., *Prezydentura Bronisława Komorowskiego – synteza działalności w dziedzinie bezpieczeństwa narodowego RP*, Kwartalnik „Bezpieczeństwo Narodowe" 2015, nr 34.

Liedel K. Mroczek A., *Terror w Polsce analiza wybranych przypadków,* Warszawa 2013.

Littlejohn Shinder D., Tittel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2004.

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

Oleksiewicz I., *Institutional aspects of anti-cybernetic policy in Poland* [in:] Oleksiewicz I., Pomykała M., Polinceusz M. (ed.), *Institutional and functional aspects of the national security protection*, Rambler Press, Chicago 2014.

Oleksiewicz I., *Rola i znaczenie polityki ochrony cyberprzestrzeni RP*, [w:] Kisielnicki J., Płusa T., Rysz S.J., Rajchel J., Rajchel K. (red.), *Rola i zadania administracji publicznej w zarządzaniu bezpieczeństwem w Polsce*, Rzeszów 2017.

Oleksiewicz I., *Rola instytucji w walce z cyberterroryzmem w Polsce*, [w:] Oleksiewicz I. (red.), *Służby i formacje w ochronie bezpieczeństwa państwa*, Rzeszów 2015.

Oleksiewicz I., *Znaczenie norm prawnych w systemie bezpieczeństwa narodowego RP*, [w:] Gryz J. (red.), *Zarys teorii bezpieczeństwa państwa*, Warszawa 2016.

Seidler G.L., Groszczyk H., Malarczyk J., Pieniążek A., *Wstęp do nauki o państwie i prawie*, Lublin 2009.

Siwicki M., *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013.

Skwarek Z., *Zarys teorii systemów bezpieczeństwa wewnętrznego państwa*, [w:] Gryz J. (red.), *Zarys teorii bezpieczeństwa państwa*, Warszawa 2016.

Skowera D., *Akademia Cyberpolicyjna – Policja i organizacje międzynarodowe wobec wyzwań przestępczości internetowej*, „Zarządzanie publiczne", Zeszyty Naukowe ISP UJ 2/2006.

Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.

Suchorzewska A., *Ochrona prawna systemów systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.

Świderski M., B*ezpieczeństwo wewnętrzne i jego uwarunkowania*, [w:] Konstanty A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa,* Warszawa 2009.

Żebrowski A., *Służby specjalne a bezpieczeństwo państwa na przełomie XX/XXI wieku*, [w:] Pietraś M., Chałupczak H., Misiągiewicz J. (red.), *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa,* Zamość 2016.

Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483 z późn. zm.).

Ustawa o Policji z dnia 6 kwietnia 1990 r. (Dz.U. 1990, Nr 30, poz. 179 ze zm.).

Ustawa z dnia 16 marca 2001 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (t.j. Dz. U. z 2012 r. poz. 461 z późn. zm.).

Ustawa z dnia 5 marca 2015 r. o zmianie ustawy, usprawniającą kierowanie obroną państwa w czasie wojny (Dz. U. z 2015 r. poz. 144).

Ustawa z 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (t.j. Dz.U. z 2010 r., nr 29; poz. 154).

Ustawa z 9 czerwca 2006 roku o Centralnym Biurze Antykorupcyjnym (t.j. Dz.U. z 2011 r., nr 171, poz.1016).

Ustawa z 9 czerwca 2006 roku o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego (Dz.U. z 2009 r., nr 85, poz.716).

Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. z 2011 r., nr 53, poz. 273).

Ustawa z dnia 5 marca 2015 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. z 2015 r., poz. 529).

Ustawa o przeciwdziałaniu z dnia 16 listopada 2000 r. (Dz.U. z 2003 r., Nr 153, poz. 1505 z późn. zm.).

Ustawy z 12 października 1990 r. o Straży Granicznej (Dz.U. 2005 Nr 234, poz. 1997 ze zm.).

Wyrok SN z dnia 16 maja 2001 r., I PKN 389/2000, OSNP 2003/5, poz. 119.

Strategia Obronności z 2009 r.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 5 listopada 2014 r.

Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016, http://bip. msw.gov.pl/bip/programy/ 19057,dok.html (dostępność 25.10.2016 r.).

http://www.cert.gov.pl/portal/cer/27/15/O_nas.html (dostępność 25.10.2016 r.).