Humanities and Social Sciences **2017**
HSS, vol. XXII, 24 (3/2017), pp. 221-235 **July-September**

Izabela OLEKSIEWICZ[1]

ROLA SŁUŻB SPECJALNYCH W POLITYCE ZWALCZANIA CYBERTERRORYZMU RP

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. Stworzyło to również nowe pole dla działalności terrorystycznej, na którym organizacje państwowe i międzynarodowe muszą przeciwstawiać się pomysłowości tych, dla których walka jest celem samym w sobie.
Z kolei, bezpieczeństwo informacyjne niejednokrotnie rozważa się jako element systemu informatycznego, jako synonim bezpieczeństwa komputerowego, telekomunikacyjnego, czy bezpieczeństwa sieciowego. Umiejętnie prowadzona polityka bezpieczeństwa informacyjnego staje się zatem gwarantem bezpieczeństwa militarnego, finansowego, gospodarczego, zarówno w skali lokalnej pojedynczego państwa, jak i na arenie międzynarodowej, co znajduje odpowiedź w opracowanych i wdrażanych przez państwo polskie strategiach oraz programach rządowych w zakresie bezpieczeństwa informacyjnego.
Dlatego w niniejszym artykule zostanie zwrócona uwaga na istniejące regulacje prawne w zakresie zwalczania cyberterroryzmu w Polsce. Podjęta będzie próba ukazania, jak istotnym elementem bezpieczeństwa wewnętrznego jest w dzisiejszym świecie cyberprzestrzeń. Ponadto starano się w znaleźć odpowiedź na pytanie, czy obecne rozwiązania prawne w zakresie bezpieczeństwa informacyjnego są skutecznym narzędziem w walce z zagrożeniem, jakim jest cyberterroryzm oraz stworzono propozycje nowych rozwiązań prawnych mających służyć wzmocnieniu polityki antycyberterrorstycznej Polski, a tym samym bezpieczeństwa wewnętrznego dzisiejszej Unii Europejskiej.

Słowa kluczowe: bezpieczeństwo informacyjne, cyberterroryzm, służby specjalne, polityka antycyberterrorystyczna.

1. WPROWADZENIE

Współczesne pojmowanie bezpieczeństwa zakłada jego kompleksowe traktowanie. Obecnie zwraca się uwagę na militarne i pozamilitarne aspekty tej problematyki oraz jej personalne i strukturalne konteksty. Bezpieczeństwo jest potrzebą podmiotową, to znaczy, że może dotyczyć danego rodzaju podmiotów, od jednostek po wielkie grupy społeczne, włączając w to struktury organizacyjne (instytucje) reprezentujące pojedynczych ludzi i grupy społeczne (państwa, narody, system międzynarodowy). Bezpieczeństwo jest pierwszoplanowym zadaniem państwa. Jego zapewnienie jest konieczne do stworzenia określo-

[1] Dr hab. Izabela Oleksiewicz, prof. PRz, kierownik Zakładu Nauki o Bezpieczeństwie, Wydział Zarządzania, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Al. Powstańców Warszawy 8, 35-959 Rzeszów; e-mail: oleiza@prz.edu.pl.

nych warunków do działalności i rozwoju społeczeństwa. Podstawowe interesy narodowe są niezmienne i oparte na całościowej koncepcji bezpieczeństwa, uwzględniającej aspekty polityczne, ekonomiczne, społeczne, militarne. Z kolei, ich realizacja stanowi dla państwa i jego mieszkańców potrzebę nadrzędną. Bezpieczeństwo jest określoną wartością społeczną, cywilizacyjną, kulturową, polityczną, ekonomiczną i ekologiczną, a z drugiej zaś wartością egzystencjalną, moralną i duchową. Przy tym jest to wartość fundamentalna, do której nie dąży się ze względu na nią samą, ale z uwagi na inne wartości, które ona zabezpiecza[2].

Bezpieczeństwo, które jest formą niepodzielną, zależy zarówno od czynników wewnętrznych poszczególnych państw czy narodów, jak i zewnętrznych, czyli międzynarodowych[3].

Za punkt wyjścia do zdefiniowania systemu bezpieczeństwa państwa można przyjąć określony poziom zapewnienia tego bezpieczeństwa. Przy czym trzeba mieć świadomość, że o stanie idealnego bezpieczeństwa państwa można mówić jedynie teoretycznie, gdyż pomimo nawet chwilowego uzyskania stanu braku zagrożeń nie można wykluczyć możliwości pojawienia się nowych. Ich źródłem bowiem są różnego rodzaju sprzeczności interesów międzyludzkich. Zagrożenia stanowią splot destrukcyjnych zdarzeń i burzą ustalony ład oraz porządek państwa. Dlatego też te dwie kategorie: „bezpieczeństwo" i „zagrożenie" są ze sobą ściśle skorelowane poprzez działalność ludzką, która z jednej strony dąży do ograniczenia istniejących zagrożeń, z drugiej strony zaś wyzwala wciąż nowe[4].

W najbardziej ogólnym ujęciu pojęcie „bezpieczeństwo" oznacza stan, w którym nie są popełniane przestępstwa, zwłaszcza przeciwko życiu, zdrowiu i mieniu, zaś pojęcie porządku stan, w którym nie są popełniane wykroczenia[5]. Pojęcia te powinny występować łącznie, gdyż, jak słusznie podkreśla to część przedstawicieli doktryny *criminal justice*, ich treści zachodzą na siebie w pewnym obszarze[6].

Przyjmując z kolei szerokie rozumienie bezpieczeństwa – utożsamiające je nie tylko z zapewnieniem nienaruszalnego trwania, lecz również z zagwarantowaniem swobody rozwoju – zauważyć można, że rozumienie to obejmuje także dążenie do wolności i dobrobytu, traktowanych jako wartości zależne od bezpieczeństwa, ale zarazem je warunkujące. W największym skrócie stwierdzić można, że bezpieczeństwo jest tożsame z zapewnieniem realizacji żywotnych interesów. W potocznym jednak rozumieniu bezpieczeństwo utożsamiane jest najczęściej ze sferą militarną, wolność ze sferą polityczną (także w sensie poli-

---

[2] K. Prokop, *Ocena norm konstytucyjnych dla realizacji skutecznego systemu bezpieczeństwa narodowego, ze szczególnym uwzględnieniem stanu wojny. Ocena stanu obecnego i rekomendacje na przyszłość*. Materiał opracowany na potrzeby SPBN, BBN, Warszawa 2011.

[3] A. Kerdoun, *La dimension environnementale de la securité dans l'espace méditerranéen*, „Les Cahiers de l'Orient" Juillet 2008, nr 91, s. 63.

[4] J. Pawłowski (red.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2002, s. 139.

[5] Por. J. Widacki, P. Sarnecki, *Ustrój i organizacja Policji w Polsce oraz jej zadania w ochronie bezpieczeństwa i porządku (reforma Policji – cz. I)*, Warszawa–Kraków 1997, s. 7–15.

[6] Por. L. Falandysz, *Pojęcie porządku publicznego w prawie karnym i karnoadministracyjnym*, „Palestra" 1969, nr 2, s. 64; J. Zaborowski, *Administracyjno-prawne ujęcie pojęć bezpieczeństwo publiczne i porządek publiczny. Niektóre uwagi w świetle unormowań prawnych 1983–1984*, „Zeszyty Naukowe ASW" 1985, nr 41; J. Świtka, M. Kuć, G. Gozdór (red.), *Społeczno-moralna potrzeba bezpieczeństwa i porządku publicznego*, Lublin 2007, s. 166.

tyki gospodarczej), a dobrobyt oczywiście ze sferą gospodarczą. Rozumienie to upowszechniło się w życiu publicznym i dlatego przedstawiane analizy nawiązują do niego[7].

Ujmując kompleksowo problem zapewnienia bezpieczeństwa państwa, można przyjąć, że system bezpieczeństwa państwa to zbiór wzajemnie powiązanych elementów (ludzi, organizacji, urządzeń) wydzielonych w celu zapewnienia bezpieczeństwa państwa, tzn. zapewnienia nienaruszalności terytorialnej oraz stworzenia warunków do swobodnego i stabilnego rozwoju państwa we wszystkich sferach jego działalności. Tak rozumiany system bezpieczeństwa państwa ma z jednej strony gwarantować stabilność bytu narodu w trwałych granicach państwa, a z drugiej przeciwdziałać wszelakim zagrożeniom mogącym ograniczać lub uniemożliwiać swobodny i stabilny rozwój w dziedzinach życia społecznego.

Oczywiście struktura systemu bezpieczeństwa państwa powinna zależeć od realizowanych zadań i procesów zachodzących w środowisku bezpieczeństwa państwa. Dlatego też można próbować dokonywać podziału obszaru bezpieczeństwa państwa na wiele różnych podsystemów. W zależności od wymagań i zastosowanych kryteriów podziału wyodrębnić można odpowiednią liczbę podsystemów bezpieczeństwa. Należy pamiętać, że dokonując takowego podziału, trzeba mieć na uwadze dziedziny związane ze strukturą procesu zapewnienia bezpieczeństwa państwa[8].

Najprostszy jest podział klasyczny, zakładający istnienie dwóch podsystemów: bezpieczeństwa zewnętrznego i bezpieczeństwa wewnętrznego. Jednakże w dobie wieloaspektowych i przenikających się nawzajem szans i zagrożeń można uznać taki podział za anachroniczny. Źródłami zagrożeń są różnego rodzaju sprzeczności interesów międzyludzkich, a relacje państw na arenie stosunków międzynarodowych w dobie globalizacji powodują wzajemne przenikanie się tych zagrożeń[9].

Współcześnie takie podejście do problemu zapewnienia bezpieczeństwa państwa gwarantuje z dużym prawdopodobieństwem wykorzystanie pojawiających się szans oraz przeciwdziałanie wielowymiarowym wyzwaniom pojawiającym się w środowisku bezpieczeństwa państwa.

Pojęcie bezpieczeństwa narodowego rozszerza tradycyjne rozumienie bezpieczeństwa państwa związanego z realizacją funkcji państwa na rzecz zachowania terytorium, suwerennej władzy, przetrwania narodu oraz ładu wewnętrznego i porządku prawnego, a także wsparcie realizacji celów i interesów właściwych jednostkom i grupom społecznym, z grupa państwową łącznie[10]. Bezpieczeństwo narodowe jako wartość narodowa i cel zarazem przenika wszystkie inne cele zgodnie z tezą postawioną przez K. Neumana „(...) bez bezpieczeństwa wszystko jest niczym”[11].

Logiczną konsekwencją jakości bezpieczeństwa narodowego jest również jakość państwa, jego organów, jak i jakość przepisów prawnych regulujących tę sferę. Brak stosownej,

---

[7] J. Stańczyk, *Zmiany systemowe w postsocjalistycznych państwach Europy Środkowej i Wschodniej*, „Studia Europejskie” 1997, nr 3, s. 37.

[8] Patrz szerzej: M. Kulisz, *Zarządzanie systemem bezpieczeństwa państwa*, Rocznik Bezpieczeństwa Międzynarodowego 2010/2011, s. 100.

[9] *Ibidem*, s. 98.

[10] Zob. W. Kitler, *Obrona narodowa III RP. Pojęcie. Organizacja. System*, Warszawa 2002. Por. też: M. Brzeziński, *Rodzaje bezpieczeństwa państwa* [w:] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, red. S. Sulowski, M. Brzeziński, Warszawa 2009, s. 38–39.

[11] K. Neuman, *Die Bundeswehr in einer Welt im Umbruch*, Wolf Jobst Verlag GmbH, Berlin 1994 [w:] *O bezpieczeństwie w Europie*, red. B. Ferenz, „Myśl Wojskowa” 1996, nr 2, s. 149.

normatywnej terminologii prowadzi do różnego rozumienia przede wszystkim przez organy tworzące system bezpieczeństwa narodowego tych samych pojęć. Znaczącym mankamentem jest niejasne określenie roli podmiotów decyzyjnych podczas występowania stanów zagrożenia. Często ich działania są chaotyczne, gdyż prawodawca nie ustanowił właściwych mechanizmów współpracy na różnych szczeblach zarządzania w terenie. Brak mechanizmów koordynacyjnych, z czym mamy do czynienia w obecnym stanie prawnym, prowadzi do wzrostu kosztów publicznych, które są ponoszone przy działaniach prewencyjnych, przy przeciwdziałaniu zagrożeniu, w działaniach interwencyjnych w trakcie zdarzenia, jak i przy usuwaniu skutków. Brak jest jasno określonych przesłanek odpowiedzialności za zaniedbania, w tym także legislacyjne, a także podmiotów tej odpowiedzialności podlegających[12].

W obecnie obowiązującym polskim systemie prawnym brak jest jednego aktu prawnego, który całościowo obejmowałby problematykę bezpieczeństwa narodowego. Prawo regulujące tę sferę obejmuje nie tylko regulacje związane z bezpieczeństwem *sensu stricto*, lecz także i te, które wspomagają realizację celów bezpieczeństwa narodowego. W dzisiejszych uwarunkowaniach, gdy bezpieczeństwa nie rozpatruje się tylko przez pryzmat zagrożeń militarnych i działalności obronnej państwa, gdy wiele dziedzin aktywności państwa (i społeczeństwa) wiąże się z zapewnieniem wolności od zagrożeń oraz niezakłóconych warunków bytu i rozwoju, działalność prawodawcza w różnych sferach krzyżuje się i nawzajem przenika.

System prawa Rzeczypospolitej Polskiej, którego treść wiąże się z problematyką bezpieczeństwa, jest niezwykle bogaty w ogromną liczbę aktów bezpośrednio regulujących lub pośrednio wspierających tę dziedzinę. Jej ewolucja jest od wielu lat naturalną konsekwencją przejścia od myślenia w kategoriach bezpieczeństwa militarnego do bezpieczeństwa wszechstronnego, a co za tym idzie – rozszerzenia koncepcji bezpieczeństwa poza aspekty suwerenności, integralności terytorialnej i ładu wewnętrznego. W konsekwencji polskie prawo, w ujęciu przedmiotowym, reguluje problematykę bezpieczeństwa w różnych jego przejawach, a głównie: politycznym; militarnym; ekonomicznym; społecznym; ekologicznym; kulturowym; ideologicznym; publicznym i powszechnym oraz informacyjnym.

Brak definicji legalnej systemu bezpieczeństwa narodowego wiąże się z zasadniczą zasadą jedności państwa i prawa, a w konsekwencji z regułą, w myśl której organy państwa działają według zasad i w granicach prawa państwowego. Prawo służy realizacji funkcji państwa, pośród których znajdują się również funkcje z zakresu bezpieczeństwa, zaś zakres działania władzy i administracji pokrywać się musi z zakresem norm prawnych. Zatem nie ma SBN, bo nie ma źródła prawa, które stanowiłoby podstawę istnienia takiego systemu.

Brak regulacji prawnych i odpowiedniej organizacji aparatu zarządzającego w tym zakresie wiąże się z tym, że mimo wydania przez Radę Ministrów rozporządzenia w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym[13], nie można jednoznacznie stwierdzić, że jego postanowienia dotyczą wszystkich możliwych stanów i warunków funkcjonowania państwa. Podstawę ustawową do jego wydania stanowiła ustawa o powszechnym obowiązku obrony RP, a więc ustawa *stricte* obronna, a ta z kolei reguluje

[12] W. Kitler, M. Czuryk, M. Karpiuk, *Aspekty prawne bezpieczeństwa narodowego RP. Część Ogólna*, Warszawa 2013, s. 18 i n.

[13] Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym (Dz.U. z 2004 r., nr 98, poz. 978).

przede wszystkim kwestie przeciwdziałania zewnętrznym, polityczno-militarnym zagrożeniom bezpieczeństwa państwa oraz działania państwa w czasie konfliktu zbrojnego (wespół z ustawą regulującą kwestie stanu wojennego).

2. ISTOTA POLITYKI ANTYCYBERTERRORYSTYCZNEJ

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[14]. 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[15].

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[16].

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 narzędzie do ich przeprowadzenia. Wydaje się, iż prawdziwa definicja powstaje dopiero po połączeniu obu tych podejść[17].

Mianem „cyberprzestępczości" określa się takie formy posługiwania się sieciami telekomunikacyjnymi, siecią komputerową, Internetem, których celem jest naruszenie jakiego-

[14] D. Denning, *Is Cyber Terror Next?*,www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc.
[15] D. Denning, *Cyberterrorism*, Global Dialogue, Autumn 2000.
[16] L. Więcaszek-Kuczyńska, *Zagrożenia bezpieczeństwa informacyjnego*, Obronność. Zeszyty Naukowe 2(10) 2014, s. 211.
[17] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 17.

kolwiek dobra chronionego prawem[18]. Cyberprzestępczość od klasycznej przestępczości odróżnia przede wszystkim działanie w środowisku związanym z technologią komputerową i wykorzystanie sieci komputerowych do popełniania przestępstwa[19]. Jej wyróżnikiem nie jest natomiast ochrona jakiegoś jednego wspólnego dobra[20]. 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)[21]. 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.

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.

3. REALIZACJA POLITYKI ANTYCYBERTERRORYSTYCZNEJ PRZEZ POLSKIE SŁUŻBY SPECJALNE

Obecnie w realizacji jest już kolejny taki program opracowany na lata 2017–2022[22]. Stanowi on kontynuację działań zapoczątkowanych w programie ochrony cyberprzestrzeni

[18] Zob. R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa 2011, s. 63 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, Warszawa 2013, s. 333.

[19] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 20.

[20] Por. też: I. Oleksiewicz, *Rola instytucji w walce z cyberterroryzmem w Polsce* [w:] *Służby i formacje w ochronie bezpieczeństwa państwa*, red. I. Oleksiewicz, Rzeszów 2015, s. 32.

[21] Szerzej: M. Świderski, B*ezpieczeństwo wewnętrzne i jego uwarunkowania* [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska- Sosnowska, Warszawa 2009, s. 58.

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

na lata 2011–2016[23]. Jego celem jest implementacja dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.[24] w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (zwanej dalej Dyrektywą NIS). 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 dotyczących 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.

W Polsce dwie agencje odgrywają wiodącą rolę w działaniach antyterrorystycznych: Agencja Bezpieczeństwa Wewnętrznego (ABW)[25] i Policja[26]. Chociaż nie jest jasny podział ich obowiązków to, 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:

---

[23] Por. Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011–2016, http://bip. msw.gov.pl/bip/programy/19057,dok.html (dostęp: 25.10.2015 r.).

[24] Dz.U. UE 2016 L194.

[25] Jest to instytucja powstała na mocy ustawy z dnia 24 maja 2002 r. (Dz.U. z 2002 r., nr 93, poz. 829).

[26] Została utworzona ustawą z dnia 6 kwietnia 1990 r. (Dz.U. z 1990 r., nr 30, poz. 179 ze zm.). Ustawa nie zawiera wprost zapisu mówiącego o zwalczeniu terroryzmu, ale Policja czyni to na podstawie przepisów zawartych w kodeksie karnym, np. art. 163, 165–168 k.k.

- 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 odpowiadania 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[27].

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

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 publicznej, stosowanego do określanie poziomu bezpieczeństwa aplikacji „www" instytucji publicznych oraz usuwania wykrytych nieprawidłowości, zanim zostaną wykorzystane przez cyberprzestępców[28].

Jako szczególnie ważną i konieczną należy uznać propozycję ustalenia odpowiedzialności za ochronę cyberbezpieczeństwa RP[29], 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[30].

Centralne Biuro Śledcze Policji (CBŚP), 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.[31]. Inne instytucje biorące udział w antyterrorystycznej działalności to:

- Agencja Wywiadu (AW)[32];
- Generalny Inspektor Informacji Finansowej (GIIF)[33];
- Straż Graniczna (SG)[34];
- Biuro Ochrony Rządu (BOR)[35].

---

[28] M. Młotek, M. Siedlarz, *Rządowy Zespół Reagowania na Incydenty Komputerowe. CERT.GOV.PL*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 4/2011, s. 161.

[29] J. Cymerski, *Terroryzm a bezpieczeństwo Rzeczypospolitej*, Warszawa 2013, s. 144.

[30] Por. A. Żebrowski, *Służby specjalne a bezpieczeństwo państwa na przełomie XX/XXI wieku* [w:] *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa*, red. M. Pietraś, H. Chałupczak, J. Misiągiewicz, Zamość 2016, s. 84–85.

[31] Ustawa weszła w życie 9 października 2014 roku (Dz.U. z 2014 r., nr 0, poz. 1199).

[32] Została powołana na mocy ustawy z dnia 24 maja 2002 r. o utworzeniu ABW i AW (tekst jedn. Dz.U. z 2010 r., nr 29, poz. 154).

[33] Swoje uprawnienia uzyskał dzięki ustawie o przeciwdziałaniu z dnia 16 listopada 2000 r. (Dz.U. z 2003 r., nr 153, poz. 1505 ze zm.). GIIF ma z kolei za zadanie w 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 informacji, które mogą mieć związek m. in. z finansowaniem terroryzmu.

[34] Zastała powołana na podstawie ustawy z 12 października 1990 r. (Dz.U. z 2005 r., 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.

[35] Powstał na mocy ustawy z dnia 16 marca 2001 r. (Dz.U. z 2004 r., nr 163, poz. 1712 ze zm.). Jego podstawowym zadaniem jest ochrona osób, obiektów i urządzeń służących użyteczności publicznej, a mogących stać się potencjalnym celem ataku terrorystycznego. Stąd też ochronie BOR pod-

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 zaliczane 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 organy, które nie biorą udział w działaniach operacyjnych Rada Bezpieczeństwa Narodowego (RBN) oraz Biuro Bezpieczeństwa Narodowego (BBN). RBN jest organem doradczym Prezydenta Rzeczypospolitej Polska i jest odpowiedzialna za określenie generalnego planu i celów dotyczące bezpieczeństwa, stosunków międzynarodowych i sił zbrojnych. Z kolei, Biuro Bezpieczeństwa Narodowego jest częścią Kancelarii Prezydenta i w myśl art. 11 ustawy o powszechnym obowiązku obrony RP[36] zapewnia mu wsparcie w zakresie wypełniania zadań odnośnie do nienaruszalności granic i niepodległości naszego państwa.

4. WNIOSKI

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.

Zlikwidować należy Kolegium ds. Służb Specjalnych. Istnienie tej instytucji wydaje się sugerować specjalny status służb specjalnych w państwie, co w sytuacji dzisiaj faktycznego,

legają: 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.

[36] Tekst jedn. Dz. U. z 2012 r., poz. 461 ze zm.

a w przyszłości również *de iure*, ich podporządkowania ministrom konstytucyjnym nie znajduje uzasadnienia. Kolegium jest obecnie instytucją czysto fasadową.

Należy przyjąć ustawę o czynnościach operacyjno-rozpoznawczych. Poprzez określenie w jednym akcie prawnym terminologii, procedur operacyjnych, a także zasad i zakresu koordynacji działań, uzyskać należy optymalizację wykorzystania służb. Unifikacja w tych zakresach pozwoli podnieść efektywność szkolenia, współdziałania oraz ułatwi przepływ kadr pomiędzy służbami;

Należy budować platformy współdziałania służb i innych instytucji w pojawiających się obszarach zagrożeń o szczególnej wadze dla bezpieczeństwa państwa (np. cyberprzestępczość, terroryzm, zorganizowana przestępczość). Platformy takie powinny być prowadzone z założeniem ewolucyjnego kształtowania ich form organizacyjnych. Przykładem takiego działania jest powołanie CAT w obrębie ABW (jednostki niejako antysystemowej z punktu widzenia organizacji administracji), poprzez skonstruowanie jej w oparciu o delegowanych przez macierzyste organizacje funkcjonariuszy wraz z uprawnieniami dostępu do posiadanych przez ich macierzyste organizacje zasobów informacyjnych, w trybie online.

Należy ujednolicić uprawnienia funkcjonariuszy różnych służb, procedury ich działania i pragmatyki służbowe. W rezultacie osiągnięta powinna zostać 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 CBŚP) i ograniczyć ich aktywność tylko do śledztw proaktywnych, tj. takich, które zmierzają do uprawdopodobnienia faktu popełnienia przestępstwa.

Należy 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:

1) 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,
2) 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 dotyczą-

cych praw osadzonych – wyposażenie SW w ograniczone uprawnienia do pracy operacyjno-rozpoznawczej;

3) 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[37].

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.

LITERATURA

[1] Brzeziński M., *Rodzaje bezpieczeństwa państwa* [w:] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, red. S. Sulowski, M. Brzeziński, Warszawa 2009.

[2] Cymerski J., *Terroryzm a bezpieczeństwo Rzeczypospolitej*, Warszawa 2013.

[3] Denning D., *Cyberterrorism*, Global Dialogue, Autumn 2000.

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

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. 9 Dz. U. UE 2016 L194).

[6] Falandysz L., *Pojęcie porządku publicznego w prawie karnym i karnoadministracyjnym*, „Palestra" 1969, nr 2.

[7] Gierszewski J., *Bezpieczeństwo wewnętrzne. Zarys systemu*, Warszawa 2013.

[8] Gryz J., *Teoretyczne aspekty współczesnego bezpieczeństwa międzynarodowego* [w:] *Współczesny wymiar bezpieczeństwa. Między teorią a praktyką*, red. J. Pawłowski, Warszawa 2011.

[9] Guzik-Makaruk E.M., *Regulacje prawne przewidziane w prawie policyjnym* [w:] *Przestępczość zorganizowana*, red. E.W. Pływaczewski, Warszawa 2011.

[10] http://www.cert.gov.pl/portal/cer/27/15/O_nas.html (dostęp: 25.10.2016 r.).

[11] Karkoszka A., *Zespół systemu bezpieczeństwa narodowego*, Strategiczny przegląd bezpieczeństwa narodowego 2010, www.demoseuropa.eu › W mediach › 2010 (dostęp: 21.08.2015 r.).

[37] 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*, Chicago 2014, p. 13–28.

[12] Kerdoun A. , *La dimension environnementale de la securité dans l'espace méditerranéen*, „Les Cahiers de l'Orient" Juillet 2008, nr 91.

[13] Kitler W., Czuryk M., Karpiuk M., *Aspekty prawne bezpieczeństwa narodowego RP. Część Ogólna*, Warszawa 2013.

[14] Kitler W., *Obrona narodowa III RP. Pojęcie. Organizacja. System*, Warszawa 2002.

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

[16] Kulisz M., *Zarządzanie systemem bezpieczeństwa państwa*, Rocznik Bezpieczeństwa Międzynarodowego 2010/2011.

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

[18] Neuman K., *Die Bundeswehr in einer Welt im Umbruch*, Wolf Jobst Verlag GmbH, Berlin 1994 [w:] Ferenz B. (red.), *O bezpieczeństwie w Europie*, „Myśl Wojskowa" 1996, nr 2.

[19] Oleksiewicz I., *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.

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

[21] Pawłowski J. (red.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2002.

[22] Płusa T., *Organizacja bezpieczeństwa w stanach zagrożenia* [w:] *Zarządzenie kryzysowe w administracji*, red. R. Częścik, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel, Warszawa–Dęblin 2014.

[23] *Polska strategia zintegrowanego zarządzania granicą*, „Przegląd Rządowy", lipiec 2000, nr 7(109).

[24] Prokop K., *Ocena norm konstytucyjnych dla realizacji skutecznego systemu bezpieczeństwa narodowego, ze szczególnym uwzględnieniem stanu wojny. Ocena stanu obecnego i rekomendacje na przyszłość*. Materiał opracowany na potrzeby SPBN, BBN, Warszawa 2011.

[25] Raport NIK z 20.03.2013 r. https://www.nik.gov.pl/plik/id,5308,vp,6885.pdf (dostęp: 21.08.2016 r.).

[26] Rozporządzenie Prezesa Rady Ministrów z dnia 11 kwietnia 2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa (Dz.U. z 2011 r., nr 86, poz. 471 ze zm.).

[27] Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym (Dz.U. z 2004 r., nr 98, poz. 978).

[28] Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011–2016, http://bip. msw.gov.pl/bip/programy/19057,dok.html (dostępność 25.10.2015 r.).

[29] 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.).

[30] Stańczyk J., *Zmiany systemowe w postsocjalistycznych państwach Europy Środkowej i Wschodniej*, „Studia Europejskie" 1997, nr 3.

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

[32] Świtka J., Kuć M., Gozdór G. (red.), *Społeczno-moralna potrzeba bezpieczeństwa i porządku publicznego*, KUL, Lublin 2007.
[33] Ustawa z dnia 12 października 1990 r. o Straży Granicznej (tekst jedn. Dz.U. z 2017 r., poz. 2365).
[34] Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (tekst jedn. Dz.U. z 2017 r., poz. 736).
[35] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2016 r., poz. 922).
[36] Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (tekst jedn. Dz.U. z 2016 r., poz. 1483).
[37] Ustawa z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (tekst jedn. Dz.U. z 2017 r., poz. 1920).
[38] Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (tekst jedn. Dz.U. z 2017 r., poz. 2195).
[39] Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (tekst jedn. Dz.U. z 2017 r., poz. 1993).
[40] Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego (tekst jedn. Dz.U. z 2009 r., nr 85, poz. 716).
[41] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jedn. Dz.U. z 2017 r., poz. 209).
[42] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tekst jedn. Dz.U. z 2016 r., poz. 1167).
[43] Widacki J., Sarnecki P., *Ustrój i organizacja Policji w Polsce oraz jej zadania w ochronie bezpieczeństwa i porządku (reforma Policji – część I)*, Warszawa–Kraków 1997.
[44] Więcaszek-Kuczyńska L., *Zagrożenia bezpieczeństwa informacyjnego*, Obronność. Zeszyty Naukowe 2(10) 2014.
[45] Zaborowski J., *Administracyjno-prawne ujęcie pojęć bezpieczeństwo publiczne i porządek publiczny. Niektóre uwagi w świetle unormowań prawnych 1983–1984*, „Zeszyty Naukowe ASW" 1985, nr 41.
[46] Żebrowski A., *Służby specjalne a bezpieczeństwo państwa na przełomie XX/XXI wieku* [w:] *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa*, red. M. Pietraś, H. Chałupczak, J. Misiągiewicz, Zamość 2016.

THE ROLE OF SPECIAL SERVICES IN COMBATING THE COUNTER TERRORISM POLICY IN POLAND

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 acquired in a laborious fashion becomes available in a short time both for those for whom they are a source of knowledge and for those who treat them as tools against others. It also created a new field for terrorist activity, where state and international organizations have to oppose the ingenuity of those for whom the struggle is an end in itself.
On the other hand, information security is often considered as an element of the IT system as a synonym for computer security, telecommunications and network security. 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.

Therefore, this publication is an attempt to characterize the determinants of this phenomenon and an analysis of the latest legal solutions in the fight against cyberterrorism in Poland. The attempt tries to show how important element of internal security is in today's world cyber-space. Moreover, an attempt has been made to find an answer to the question whether the current legal solutions of Poland in the area of security are an effective tool in the fight against cyberterrorism. Proposing the new legal solutions aimed at strengthening Poland's counter-cybernetism policy, and thus the internal security of today's European Union.

Keywords: information security, cyber terrorism, special services, counter-cybernetism policy.

DOI: 10.7862/rz.2017.hss.55

Przesłano do redakcji: kwiecień 2017 r.
Przyjęto do druku: wrzesień 2017 r.