Spis treści

Wstęp

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, co oznacza, 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 określonych 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 z jednej strony określoną wartością społeczną, cywilizacyjną, kulturową, polityczną, ekonomiczną i ekologiczną, 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[1]. Bezpieczeństwo, które jest formą niepodzielną, zależy zarówno od czynników wewnętrznych poszczególnych państw czy narodów, jak i zewnętrznych, czyli międzynarodowych[2].

Za punkt wyjścia do zdefiniowania systemu bezpieczeństwa państwa można przyjąć określony poziom zapewnienia tego bezpieczeństwa. Trzeba przy tym mieć świadomość, że o stanie idealnego bezpieczeństwa państwa można mówić jedynie teoretycznie, gdyż pomimo nawet chwilowego uzy-

---

[1] 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.

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

skania stanu braku zagrożeń nie można wykluczyć możliwości pojawienia się nowych. Ich źródłem bowiem są różnego rodzaju sprzeczności interesów międzyludzkich. Zagrożenia stanowią splot destrukcyjnych zdarzeń, burzą ustalony ład i porządek państwa. Dlatego też te dwie kategorie: „bezpieczeństwo" i „zagrożenie" są ze sobą ściśle skorelowane przez działalność ludzką, która z jednej strony dąży do ograniczenia istniejących zagrożeń, z drugiej zaś wyzwala wciąż nowe[3].

W najbardziej ogólnym ujęciu pojęcie „bezpieczeństwo" oznacza stan, w którym nie są popełniane przestępstwa, zwłaszcza przeciwko życiu, zdrowiu i mieniu, pojęcie porządku natomiast to stan, w którym nie są popełniane wykroczenia[4]. Pojęcia te powinny występować łącznie, gdyż, jak słusznie podkreśla część przedstawicieli doktryny *criminal justice*, ich treści zachodzą na siebie w pewnym obszarze[5].

Przyjmując z kolei szerokie rozumienie bezpieczeństwa – utożsamiające je nie tylko z zapewnieniem nienaruszalnego trwania, lecz również z zagwarantowaniem swobody rozwoju – można zauważyć, że rozumienie to obejmuje także dążenie do wolności i dobrobytu, traktowanych jako wartości zależne od bezpieczeństwa, ale zarazem je warunkujące. W największym skrócie można stwierdzić, że bezpieczeństwo jest tożsame z zapewnieniem realizacji żywotnych interesów. W potocznym jednak rozumieniu bezpieczeństwo jest najczęściej utożsamiane ze sferą militarną, wolność ze sferą polityczną (także w sensie polityki gospodarczej), a dobrobyt ze sferą gospodarczą. Rozumienie to upowszechniło się w życiu publicznym i dlatego przedstawiane analizy nawiązują do niego[6].

Ujmując kompleksowo problem zapewnienia bezpieczeństwa państwa, można przyjąć, że system bezpieczeństwa państwa to zbiór wzajemnie

---

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

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

[5] Por. L. Falandysz, *Pojęcie porządku publicznego w prawie karnym i karno-administracyjnym*, „Palestra" 1969, nr 13/2(134), 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.

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

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, z drugiej natomiast przeciwdziałać wszelkim zagrożeniom mogącym ograniczać lub uniemożliwiać swobodny i stabilny rozwój we wszystkich dziedzinach życia społecznego.

Oczywiście struktura systemu bezpieczeństwa państwa powinna zależeć od realizowanych zadań i procesów zachodzących w środowisku bezpieczeństwa państwa, dlatego można próbować dokonywać podziału obszaru bezpieczeństwa państwa na wiele różnych podsystemów. W zależności od wymagań i zastosowanych kryteriów podziału można wyodrębnić odpowiednią liczbę podsystemów bezpieczeństwa. Należy pamiętać, że, dokonując takiego podziału, trzeba mieć na uwadze dziedziny związane ze strukturą procesu zapewnienia bezpieczeństwa państwa[7].

Najprostszy jest podział klasyczny zakładający istnienie dwóch podsystemów: bezpieczeństwa zewnętrznego i bezpieczeństwa wewnętrznego. Jednak w dobie wieloaspektowych i przenikających się nawzajem szans oraz zagrożeń taki podział można uznać 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[8]. 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 oraz grupom społecznym, łącznie z grupą państwową[9]. Bezpieczeństwo narodowe jako wartość narodowa

---

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

[8] Ibidem, s. 98.

[9] Zob. W. Kitler, *Obrona narodowa III RP. Pojęcie. Organizacja. System*, Warszawa 2002. Por. też: M. Brzeziński, *Rodzaje bezpieczeństwa państwa*, [w:] *Bezpieczeństwo*

i zarazem cel przenika wszystkie inne cele, zgodnie z tezą postawioną przez K. Neumana „(…) bez bezpieczeństwa wszystko jest niczym”[10].

Logiczną konsekwencją jakości bezpieczeństwa narodowego jest również jakość państwa, jego organów oraz przepisów prawnych regulujących tę sferę. Brak stosownej, normatywnej terminologii prowadzi do różnego rozumienia tych samych pojęć przede wszystkim przez organy tworzące system bezpieczeństwa narodowego. Znaczącym mankamentem jest niejasne określenie roli podmiotów decyzyjnych podczas występowania stanów zagrożenia. Często ich działania są chaotyczne, bowiem prawodawca nie ustanowił właściwych mechanizmów współpracy na różnych szczeblach zarządzania w terenie. Brak mechanizmów koordynacyjnych, z którym się spotykamy w obecnym stanie prawnym, prowadzi do wzrostu kosztów publicznych ponoszonych podczas działań prewencyjnych, przy przeciwdziałaniu zagrożeniu, w działaniach interwencyjnych w trakcie zdarzenia, a także podczas usuwania ich skutków. Brak jest jasno określonych przesłanek odpowiedzialności za zaniedbania, w tym także legislacyjne, jak również podmiotów podlegających tej odpowiedzialności[11].

Poprawne funkcjonowanie społeczeństwa jest dzisiaj w dużym stopniu uzależnione od funkcjonowania nowoczesnych technik i technologii informacyjnych. Komputery i sieci komputerowe są powszechnie wykorzystywane w gospodarce, w administracji i gospodarstwach domowych. Urządzenia te stają się sukcesywnie niezbędne do sterowania wszystkimi nowoczesnymi procesami zarządzania, administrowania, kontroli oraz dostarczania towarów i usług. Poza niekwestionowanymi korzyściami niosą jednak liczne zagrożenia. Jednym z nich jest jakościowa przemiana przestępczości. Tradycyjne formy i sposoby popełniania przestępstw są zastępowane przez formy wykorzystujące wszelkie możliwości nowoczesnych technologii. Klasyczną przestępczość powoli wypiera więc cyberprzestępczość.

Mianem cyberprzestępczości określa się takie formy posługiwania się sieciami telekomunikacyjnymi, siecią komputerową czy Internetem, których celem jest naruszenie jakiegokolwiek dobra chronionego pra-

---

wewnętrzne państwa. Wybrane zagadnienia, red. S. Sulowski, M. Brzeziński, Warszawa 2009, s. 38–39.

[10] K. Neuman, *Die Bundeswehr in einer Welt im Umbruch*, Berlin 1994; B. Ferenz (red.), *O bezpieczeństwie w Europie*, „Myśl Wojskowa” 1996, nr 2, s. 149.

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

wem[12]. Cyberprzestępczość od klasycznej przestępczości odróżnia przede wszystkim działanie w środowisku związanym z technologią komputerową i wykorzystanie sieci komputerowych do popełniania przestępstwa[13]. Jej wyróżnikiem nie jest natomiast ochrona jakiegoś jednego wspólnego dobra[14]. 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.

Cyberprzestępczość jest stosunkowo nowym zjawiskiem, rozprzestrzeniającym się w zawrotnym tempie w społeczeństwach dobrze zinformatyzowanych i mocno usieciowionych. Stanowi bardzo poważne i trudne do zwalczania zagrożenie. Decydują o tym szczególne właściwości, jakimi cechuje się to zjawisko. Pierwsza z cech – transgraniczność – powoduje, że działania cyberprzestępców z łatwością przenikają bariery, którymi są granice państw. Bardzo często cyberprzestępcy prowadzą swoje działania w jednym miejscu, a ich skutki ujawniają się zupełnie gdzie indziej, w miejscu oddalonym o setki kilometrów, nierzadko w innym kraju lub na innym kontynencie. Uniemożliwia to określenie systemu prawnego, według którego miałoby następować ściganie takich przestępstw, a jednocześnie znacznie utrudnia wyznaczenie podmiotów odpowiedzialnych za podejmowanie działań ochronnych i zapobiegawczych. Kolejną cechą jest anonimowość, która z pewnością nie ułatwia szybkiego ustalenia sprawców przestępstw oraz wykrycia sposobów ich działania. Nie jest to całkowicie niemożliwe, wymaga jednak żmudnych poszukiwań i wdrożenia dobrze przemyślanych i zaplanowanych działań. Wygoda i szybkość, jaką zapewnia

---

[12] Zob. R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa 2011, s. 63 i n.; A. Gniadek, *Cyberprzestępczość i cyberterroryzm – zjawiska szczególnie niebezpieczne*, [w:] *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. T. Jemioła, J. Kisielnicki, K. Rajchel, 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, Warszawa 2013, s. 333.

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

[14] Ibidem, s. 21.

korzystanie z nowoczesnych technik komputerowych i sieciowych, sprzyja natomiast ogromnemu narastaniu tej formy przestępczości w państwach najbardziej rozwiniętych[15].

To wszystko sprawia, że ochrona przed zagrożeniami związanymi z cyberprzestępczością jest niezwykle trudna i wymaga podejmowania licznych przedsięwzięć, w tym także wymagających wieloaspektowej i szeroko zakrojonej współpracy międzynarodowej. Dla skuteczności tej ochrony niezbędna jest współpraca poszczególnych państw mająca na celu ustalenie wspólnej polityki przeciwdziałania cyberprzestępczości, a następnie jej konkretyzacja przez określenie niezbędnych priorytetów oraz jednolitych zasad wspólnego działania. Wyznaczone w ten sposób ogólne zasady wymagają implementacji do prawa wewnętrznego państw, stając się podstawą instytucjonalnego i funkcjonalnego systemu instrumentów do walki z cyberprzestępczością. Stworzenie skutecznego systemu przeciwdziałania cyberprzestępczości nie jest proste. Wymaga pogłębionej analizy zjawiska w dłuższej perspektywie czasowej, a przy tworzeniu takiego systemu mogą wystąpić liczne problemy z dostosowaniem ogólnych wytycznych prawa międzynarodowego bądź unijnego do prawa wewnętrznego.

Konstrukcja współczesnego modelu społeczeństwa informacyjnego, którego niezaprzeczalnym katalizatorem są technologie stosowane podczas komunikacji elektronicznej, przybierającej w wyniku konwergencji formę cyfrową, wyzwala potrzebę refleksji nad fenomenem informacji. Cyberprzestrzeń jest w tym modelu równoległą przestrzenią niefizyczną, niekonkurencyjną w stosunku do przestrzeni trójwymiarowej. Budulcem cyberprzestrzeni są dane i informacje, które kreują mikrokorelacje, oddziaływując wzajemne między sobą.

Pomiędzy przestrzenią trójwymiarową a cyberprzestrzenią natomiast występują makrokorelacje. Ich charakter jest interpersonalny. Makrokorelacje są każdą postacią komunikacji zachodzącej pomiędzy jednostkami. Polegają na wprowadzaniu do cyberprzestrzeni informacji w różnej postaci formatu utrwalenia, a ich odbiór jest połączony z określoną projekcją w ludzkim umyśle oraz ich wykorzystaniem. Proces makrokorelacji ma charakter ciągły, niezależny od przestrzeni i w znacznie mniejszym zakresie niż dotychczasowe metody relacji interpersonalnych

[15] Szerzej: M. Polinceusz, M. Pomykała, *Ochrona cyberbezpieczeństwa w Polsce. Kierunki zmian legislacyjnych na przestrzeni ostatnich lat*, [w:] *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, red. P. Bogdalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel, Warszawa 2013, s. 660–661.

zależny od czasu. Najbardziej bezpośrednią konsekwencją jego powstania jest społeczeństwo informacyjne. Jest on sprzęgnięty z przemianami technologicznymi, mając niewątpliwie swoje humanistyczne i przyrodnicze (antropologiczne) konsekwencje.

Ludzkie stosunki kwalifikowane jurydycznie są w przestrzeni nowych zjawisk poddane innemu wartościowaniu. Takie ujęcie ludzkiej zbiorowości wywodzi się z uświadomienia intensywności społecznych oddziaływań i nowej płaszczyzny dla ich urzeczywistniania – cyberprzestrzeni. Zasięg nowej formy koegzystencji jednostek, kwalifikowanej wybiórczo i niespójnie przez normy prawne, jest wręcz globalny. Jego układ jest równoległy i „niekonkurencyjny" w stosunku do desygnatów innych form opisu ludzkich zbiorowości. Mimo że włączamy się w jego byt przez uruchomienie środków komunikacji określonego rzędu, ma on charakter permanentny ze względu na skalę konsekwencji swych oddziaływań. Należy oczekiwać, że fundamentalne instytucje prawne organizujące i urzeczywistniające egzystencję społeczeństw będą ulegać przemianom, których ramy określą nurty ewolucji modelu zbiorowości informacyjnej.

Głównym celem badania będzie, po pierwsze, próba ukazania, jak istotnym elementem bezpieczeństwa Unii Europejskiej powinna być umiejętnie prowadzona polityka cyberbezpieczeństwa na poziomie unijnym i poszczególnych państw członkowskich. Ma to z kolei znaczący wpływ na bezpieczeństwo wewnętrzne zarówno tych państw, jak i całej UE. Analiza istoty polityki cyberbezpieczeństwa pozwoli na wykazanie, że istnieje polityka ochrony cybeprzestrzeni UE, która podlega ciągłej ewolucji, oraz że mamy do czynienia z procesem, który nie został zakończony i trwa nadal. Nie należy zapominać, że Unia Europejska, będąc organizacją międzynarodową, implementuje w życie normy prawa międzynarodowego publicznego i działa na ich podstawie. Z kolei prawo unijne należy traktować jako *lex specialis* w stosunku do prawa międzynarodowego publicznego.

Po drugie, w niniejszej monografii zostaną porównane normy prawa unijnego na tle prawa krajowego w Polsce i RFN. Wybór tych dwóch państw członkowskich UE został podyktowany kilkoma względami. Pierwszym jest ich geopolityczne położenie w Unii Europejskiej (oba państwa znajdują się w środku Europy i są państwami sąsiadującymi), kolejnym natomiast jest odmienność implementacji polityki ochrony cyberprzestrzeni UE i sposób jej realizacji na poziomie państwowym, co przekłada się na skuteczność zwalczania tego zjawiska. Trzecim i chyba najważniejszym jest wskaźnik

zagrożenia cyberatakiem, który w przypadku RFN plasuje się na trzecim miejscu w Europie, a w przypadku Polski na przedostaniem miejscu. Te wszystkie uwarunkowania dają podstawę do podjęcia analizy badawczej, która będzie miała charakter instytucjonalno-prawny.

Podmiotem niniejszej analizy jest Unia Europejska ze szczególnym uwzględnieniem dwóch wcześniej wspomnianych państw: Polski oraz Niemiec, przedmiotem zaś są działania podjęte w ramach polityki cyberbezpieczeństwa w wymiarze instytucjonalno-prawnym zarówno na poziomie UE, jak i na poziomie państwowym.

Ramy czasowe monografii obejmują politykę cyberbezpieczeństwa Unii Europejskiej po wejściu w życie Traktatu z Lizbony. Wszelkie działania podjęte w tej materii przed jego uchwaleniem traktowane są jako geneza polityki będącej przedmiotem badania.

Na podstawie przeprowadzonej analizy zagadnienia, poddano weryfikacji kilka tez badawczych. Po pierwsze, należy przyjąć, że istnieje polityka cyberbezpieczeństwa w obu wymienionych państwach, która podlega stałej ewolucji i zmierza do harmonizacji przepisów w regulacjach przyjętych w prawie UE, chociaż proces ten nie został zakończony i postępuje z różną prędkością w przypadku obu państw. Ewolucja polityki jest reakcją na wzrost niestabilności i zagrożeń w tym obszarze oraz brak istnienia odpowiednich mechanizmów i regulacji w tym zakresie. Trzeba będzie przeprowadzić badanie wstępne, które pozwoli określić przyczyny istnienia zjawiska cyberterroryzmu w Unii Europejskiej oraz stwierdzić, jaki wpływ zjawisko cyberterroryzmu wywiera na politykę i strategię Unii Europejskiej.

Po drugie, należy założyć, że przyczyną powstania polityki jest również brak istnienia odpowiednich mechanizmów i regulacji w tym obszarze, w związku z czym mamy do czynienia z procesem instytucjonalizacji. W tym miejscu można również postawić twierdzenie, że umiejętne połączenie polityki i strategii warunkuje pomyślność działań w każdej ze sfer aktywności państwa: społeczno-kulturowej, ekonomicznej i bezpieczeństwa, w tym również w obszarze ochrony cyberprzestrzeni.

Po trzecie, nowe zjawiska technologiczne w dziedzinie przesyłania danych i informacji modelują sfery wzajemnych ludzkich oddziaływań, więc na tym gruncie zasadzają się zwyczaje i potrzeby regulacji prawnych. Skoro zjawisko cyberterroryzmu ma charakter transgraniczny, to polityka ochrony cyberprzestrzeni powinna się opierać na współpracy międzypaństwowej i koordynacji działań, które stanowią nieodzowny element

skutecznej odpowiedzi na samo zagrożenie, jakim jest cyberterroryzm. Z drugiej strony technologie informacyjne w przestrzeni współczesnych ludzkich zbiorowości wywołały potrzebę uruchomienia wielu instytucji, które nie miały dotąd precedensu w dziejach systemów prawnych albo przeobraziły instytucje tak dalece, że stosowanie dotychczasowego opisu doktrynalnego stało się niemożliwe.

W związku z tym nasuwają się zasadnicze pytania: w jakim kierunku powinna zmierzać współczesna polityka zwalczania cyberterroryzmu na gruncie instytucjonalno-prawnym UE oraz w jakim zakresie umiejętnie prowadzona polityka cyberbezpieczeństwa UE jest w stanie wywrzeć wpływ na bezpieczeństwo poszczególnych państw członkowskich, uwzględniając tu przykład Polski i RFN?

Na strukturę monografii składają się cztery rozdziały. W pierwszym zatytułowanym *Istota polityki cyberbezpieczeństwa Unii Europejskiej* wyjaśniono pojęcie zjawiska cyberterroryzmu, cyberprzestępczości i cyberwojny oraz ukazano ich wpływ na politykę bezpieczeństwa państwa w społeczeństwie informacyjnym. Przedmiotem analizy tego rozdziału jest cyberterroryzm jako zagrożenie oraz jego specyfika jako forma przemocy. W tej części rozdziału przeanalizowano cyberterroryzm jako szczególną postać zagrożenia w XXI w. z odwołaniem się do konkretnych przykładów, a także przedstawiono i przeanalizowano czynniki warunkujące to zagrożenie. Określenie przyczyny zaistnienia zjawiska cyberterroryzmu pozwoliło na wykazanie, że istnieje polityka cyberbezpieczeństwa Unii Europejskiej, która stanowi oraz współtworzy politykę bezpieczeństwa UE i podlega ciągłej ewolucji. W związku z tym mamy do czynienia z procesem, który nie został zakończony i trwa nadal.

W drugiej części pierwszego rozdziału poświęconej strategii ochrony cyberprzestrzeni Unii Europejskiej starano się ukazać, jaką rolę odgrywa strategia zarówno w polityce bezpieczeństwa Unii będącej organizacją międzynarodową, jak i na poziomie państwa. Przedstawiono również cechy, jakie posiada polistrategia bezpieczeństwa, a połączenie polityki i strategii umożliwiło zrozumienie samej istoty ryzyka strategii oraz wyjaśnienie, że polityka i strategia określają byt oraz rozwój państwa, a jednocześnie mają charakter zmienny, dynamiczny i są stale aktualizowane w ramach tzw. przeglądu strategicznego. Polityka i strategia są przy tym warunkowane przez wyzwania i zagrożenia, szanse dla bytu i rozwoju podmiotu, można zatem postawić tezę, że umiejętne połączenie polityki i strategii warunkuje pomyślność działań w każdej ze sfer aktywności państwa: społeczno-kultu-

rowej, ekonomicznej i bezpieczeństwa, w tym również w obszarze ochrony cyberprzestrzeni. Rozdział pierwszy stanowi wprowadzenie do badanego problemu.

W pierwszym podrozdziale rozdziału drugiego pt. *Podstawy prawne polityki cyberbezpieczeństwa UE* poddano analizie międzynarodowe standardy zwalczania cyberterroryzmu zawarte w różnych konwencjach międzynarodowych opracowanych zarówno przez ONZ, jak i Radę Europy. W drugiej części przedstawiono z kolei zagadnienia prawne polityki cyberbezpieczeństwa Unii Europejskiej, z podziałem na prawo pierwotne i wtórne. Ze względu na to, że prawo cyberterrorystyczne Unii Europejskiej należy traktować jako szczególny przypadek prawa międzynarodowego, pokazano wpływ prawa międzynarodowego istniejącego przed powstaniem Unii Europejskiej na obecny kształt prawa unijnego. Przeprowadzono również analizę procesu uwspólnotowienia polityki cyberbezpieczeństwa Unii Europejskiej na podstawie przyjętych rozwiązań prawnych. Analiza podstaw prawnych pozwoliła na wykazanie zależności polityki cyberbezpieczeństwa od poziomu integracji państw członkowskich, a także związku funkcjonalnego zachodzącego pomiędzy harmonizacją przepisów prawa państwowego z prawem unijnym w dziedzinie bezpieczeństwa, ponieważ proces ten nie został zakończony i trwa nadal.

Rozdziały trzeci i czwarty poświęcono implementacji polityki cyberbezpieczeństwa w Polsce i RFN. Analiza implementacji polityki cyberbezpieczeństwa na przykładzie Polski i Niemiec umożliwi poznanie i porównanie strategii, instrumentów, instytucji i podstaw prawnych, za pomocą których Unia Europejska realizuje funkcje ochronne na poziomie wewnątrzpaństwowym, oraz zależność problemów bezpieczeństwa wewnętrznego UE, a tym samym polityki cyberbezpieczeństwa od poziomu integracji państw członkowskich.

W tych rozdziałach zostaną omówione i porównane strategie narodowe obu państw, przedstawione i ocenione instrumenty stosowane przez Polskę i RFN w polityce cyberbezpieczeństwa. Zwrócono tutaj uwagę przede wszystkim na aspekt zgodności polityki wewnętrznej danego państwa członkowskiego w tej kwestii z polityką ochrony cyberprzestrzeni Unii Europejskiej. Co więcej, zostały uwzględnione takie zagadnienia, jak dostosowanie przepisów prawa wewnętrznego do prawodawstwa unijnego przy jednoczesnym przestrzeganiu prawa. Pozwoliło to na wskazanie, które z analizowanych państw członkowskich prowadzi politykę cyberbezpieczeństwa bardziej zgodną z polityką UE.

Taki układ monografii pozwala na przejrzyste i jasne przedstawienie problematyki. To z kolei daje możliwość wyprowadzenia wniosków i zaprezentowania wizji pewnych zmian w polityce cyberbezpieczeństwa.

Podstawę źródłową przeprowadzonej analizy stanowią dokumenty Unii Europejskiej regulujące problematykę cyberterroryzmu oraz akty wewnętrzne Polski i RFN. Dzięki wykorzystaniu aktów prawnych (przede wszystkim traktatów, konwencji, rezolucji i dyrektyw) oraz materiałów znajdujących się na stronach: ONZ, Rady Europy, Unii Europejskiej, parlamentów wybranych państw członkowskich, Centrum Europejskiego w Natolinie, możliwa była wnikliwa analiza podjętego tematu. Dostęp do materiałów źródłowych (przeważnie angielsko- i niemieckojęzycznych) był możliwy dzięki nieograniczonym możliwościom Internetu, głównie dostępowi do bazy danych serwisu europa.eu. Ze względu na szybko ewoluującą politykę Unii Europejskiej wobec procesu cyberterroryzmu, bardzo istotne były liczne materiały pokonferencyjne, prasowe i artykuły naukowe związane z tym zagadnieniem, opublikowane w Internecie.

Tak wiele materiałów udało się pozyskać dzięki wieloletniemu procesowi gromadzenia literatury. W tym czasie zapoznano się z wieloma pozycjami naukowymi, przede wszystkim literaturą obcojęzyczną.

Praca ma charakter interdyscyplinarny, obejmuje zagadnienia z zakresu: nauk o bezpieczeństwie, stosunków międzynarodowych, prawa międzynarodowego i unijnego. Było to podstawą do szerokiej i wnikliwej analizy materiałów oraz tekstów źródłowych. Przy przedstawianiu zjawiska cyberterroryzmu w Unii Europejskiej wykorzystano kilka metod badawczych, ponieważ złożoność polityki ochrony cyberbezpieczeństwa uniemożliwia zastosowanie tylko jednej z nich. Punkt wyjścia do badań stanowiły kwerendy źródłowe i studia literaturowe, mające na celu wspólne określenie profilów kompetencyjnych, kluczowych z punktu widzenia wyzwań cyberbezpieczeństwa. Następnie poddano analizie i ocenie najważniejsze prawne i polityczne dokumenty programowe UE, Polski i RFN pod kątem zawartych w nich wizji społeczeństwa 4.0, ze szczególnym uwzględnieniem wyzwań dla cyberbezpieczeństwa. W badaniu odwołano się do metody ilościowej w celu stwierdzenia, jak wraz z rozwojem cyfryzacji i technologii kształtowała się na przestrzeni czasu polityka ochrony cyberprzestrzeni Unii Europejskiej. Za pomocą analizy czynnikowej ustalono wpływ poszczególnych czynników na zjawisko cyberterroryzmu. Następnie zastosowano metodę decyzyjną, aby zobaczyć, jaki wpływ wywierają poszczególne instrumenty stosowane przez Unię w ramach polityki

ochrony cyberprzestrzeni na zjawisko cyberterroryzmu. Wykorzystano także metodę porównawczą w celu ustalenia zgodności polityki wewnętrznej wybranych państw członkowskich z polityką ochrony cyberprzestrzeni Unii Europejskiej. Zastosowano również technikę prognostyczną do przedstawienia wizji rozwoju polityki ochrony cyberprzestrzeni Polski i RFN. Z kolei technika analizy dokumentów pozwoliła na zbadanie zawartości aktów prawnych regulujących problematykę terroryzmu w Unii Europejskiej. Jako końcową wybrano metodę syntezy całości zjawiska na podstawie dotychczas przeprowadzonych obserwacji.