Acta Politica Polonica nr 2/2019 (48) | www.wnus.edu.pl/ap | DOI: 10.18276/ap.2019.48-02 | 19–32

Zjawisko europeizacji w kontekście polityki bezpieczeństwa cybernetycznego Unii Europejskiej

Marek Górka
dr

Politechnika Koszalińska, Wydział Humanistyczny
e-mail: marek_gorka@wp.pl

Martyna Gibka
dr

Politechnika Koszalińska, Wydział Humanistyczny
e-mail: martyna.gibka@gmail.com

Słowa kluczowe europeizacja, integracja europejska, globalizacja, polityka bezpieczeństwa cybernetycznego, cyfryzacja, cyberzagrożenia

Abstrakt Polityka bezpieczeństwa UE przechodzi przez proces zmian, które nie tylko wpłynęły na jej politykę, ale również na pojawienie się nowych podmiotów, co doprowadza do znaczącej ewolucji w odniesieniu do wymiaru polityki UE. Zarówno konkretne wydarzenia, jak i długoterminowe procesy o charakterze cyfrowym ożywiły i wzmocniły dyskurs na forum UE o rosnącym zagrożeniu cybernetycznym. Celem artykułu jest zasugerowanie, że perspektywa bezpieczeństwa cybernetycznego jest w stanie wyjaśnić i wzbogacić o nowe aspekty proces europeizacji. W kontekście analizowanego tematu dokonana zostaje próba opisu koncepcji europeizacji i jej zastosowania w obszarze polityki bezpieczeństwa cybernetycznego.

The phenomenon of Europeanisation in the context of the cyber security policy of the European Union

Keywords Europeanisation, European integration, globalisation, cyber security policy, digitisation, cyber threats

Abstract EU security policy is undergoing a process of change that has not only affected its policies but also the emergence of new actors, which clearly shows that there is a significant evolution in relation to the EU policy dimension. Both specific events and long-term digital processes have revived and strengthened the EU discourse on the growing cyber threat. The aim of the article is to suggest that the cyber security perspective can clarify and enrich the process of Europeanisation with new aspects. In the context of the analysed topic, an attempt is made to describe the concept of Europeanisation and its application in the area of cyber security policy.

Wprowadzenie

Unia Europejska została zmuszona do radykalnego przemyślenia swojego podejścia do ochrony sieci i bezpieczeństwa informacji w następstwie coraz większej liczby cyberincydentów. Pierwszym, symbolicznym wydarzeniem był atak grupy hakerów powiązanych z rosyjskim rządem na estońską infrastrukturę w maju 2007 roku. Od tego czasu nastąpiło wiele głośnych przypadków naruszeń bezpieczeństwa cybernetycznego nie tylko na obiekty infrastruktury krytycznej państw europejskich, ale również na organy UE, w tym na Komisję Europejską, Parlament Europejski (PE) i Europejską Służbę Działań Zewnętrznych (ESDZ). Nastąpił również wzrost dostępności narzędzi powodujących zakłócenia w internecie, które jednocześnie zaczęły być coraz większym wyzwaniem dla rozwoju europejskiej gospodarki cyfrowej (ENISA, 2016). Rosnące zagrożenie dla UE oraz obywateli, rządów i przedsiębiorstw spowodowały, że bezpieczny rozwój i korzystanie z cyfrowych technologii stało się kluczowym filarem polityki UE.

Trudno znaleźć dziedzinę życia, w której technologie informacyjno-komunikacyjne (ICT) nie mają obecnie zastosowania – począwszy od systemów administracyjnych i bankowych, przez służbę zdrowia, edukację, sieci społecznościowe, łańcuchy dostaw, po przetwarzanie informacji w chmurze i internet przedmiotów (IoT). Dowodem na poświęcanie coraz większej uwagi temu zagadnieniu przez UE jest m.in. publikacja *Strategii jednolitego rynku cyfrowego* (Komisja Europejska, 2015a) oraz inicjatywy podejmowane w ramach partnerstwa publiczno-prywatnego (PPP) (Komisja Europejska, 2016a), które mają na celu budowanie konkurencyjności europejskiej gospodarki.

Założenia badawcze

Pojęcie europeizacji użyte zostaje w artykule jako perspektywa służąca do badania nowej dynamiki politycznej w dziedzinie bezpieczeństwa europejskiego. W związku z tym podejmowana w pracy refleksja zawiera również spostrzeżenia wskazujące na różne formy i stopnie upolitycznienia bezpieczeństwa cybernetycznego (Costa, 2019, s. 790–802; Hegemann, 2018, s. 175–190; Wagner, 2018, s. 537–563).

Celem artykułu jest pokazanie, że dziedzina bezpieczeństwa europejskiego z czasem doszła do etapu obejmującego szerszy – niż uprzednio – zakres aktorów, aren i argumentów. Prowadzi to do wielu wniosków i otwartych pytań, które wyznaczają dalszy kierunek badań empirycznych i koncepcyjnych. W związku z tym warto zastanowić się, w jaki sposób Unia Europejska wpływa nie tylko na decyzje polityczne państw członkowskich, ale także na proces kształtowania polityki w zakresie bezpieczeństwa cybernetycznego. Czy w tym przypadku zmienia się także polityka UE i czy prowadzi ona do wzrostu znaczenia polityki bezpieczeństwa cybernetycznego? Na czym dokładnie polega europeizacja w kontekście coraz bardziej dynamicznego procesu cyfryzacji? Celem podjętej analizy jest poszukiwanie odpowiedzi na te pytania głównie na poziomie teoretycznym, a także wyjaśnienie zachodzących procesów w oparciu o wybrane wydarzenia z obszaru polityki bezpieczeństwa.

Aby móc udowodnić i wskazać, że dokonująca się mobilizacja instytucji UE oraz państw członkowskich wokół zagadnień związanych z cyberbezpieczeństwem przyczynia się do lepszego zrozumienia procesu europeizacji, w artykule opisano najważniejsze regulacje odno-

szące się do cyberbezpieczeństwa. Analiza tematu rozpoczyna się od charakterystyki pojęcia europeizacji – z odwołaniem do teoretycznych argumentów w literaturze. Następnie badany jest proces cyfryzacji w odniesieniu do najważniejszych regulacji UE w zakresie bezpieczeństwa cybernetycznego. Artykuł dowodzi, że europeizacja, obok tradycyjnych czynników w obszarze polityki, gospodarki i społeczeństwa, jest realizowana w oparciu o preferencje polityczne na płaszczyźnie bezpieczeństwa cybernetycznego. Dlatego też autorzy artykułu wskazują na możliwość podejmowania badań nad cyberbezpieczeństwem, które mogą okazać się przydatne dla przyszłych analiz dotyczących europeizacji.

Bezpieczeństwo europejskie, które w coraz większym stopniu ewoluuje wokół pojęć związanych z technologią cybernetyczną, kształtuje koncepcje współczesnej europeizacji. Warto więc wskazać również, że debata na temat zmian w polityce europejskiej nie powinna już wykluczać bezpieczeństwa cybernetycznego, a raczej podkreślać specyficzne problemy procesu cyfryzacji w tym obszarze (De Wilde, Leupold, Schimdtke 2016, s. 1–10). Z tego względu istnieje potrzeba lepszego zrozumienia interakcji wielu podmiotów zaangażowanych na różnych poziomach polityki bezpieczeństwa. W artykule podjęto próbę usystematyzowania i opisania podstawowych ram interakcji między podmiotem bezpieczeństwa (Unią Europejską) a podmiotem odbiorców (państwa członkowskie). Reasumując, artykuł sugeruje możliwość rozwoju badań nad europeizacją na podstawie badań stopnia kompatybilności ram instytucjonalnych europejskiego bezpieczeństwa cybernetycznego.

Użyteczność pojęcia europeizacji postrzegana jest w kontekście rosnącego wzrostu cyfryzacji życia publicznego, co może być przyczynkiem do postawienia hipotezy o poszerzeniu tego zjawiska o wymiar cybernetyczny. Warto także zastanowić się, czy zachodzące zmiany, będące efektem zastosowania nowych technologii, nie będą czynnikiem ewoluującym dotychczasową politykę bezpieczeństwa o nowe praktyki. A co za tym idzie, czy obecny model interakcji państw członkowskich, który jest efektem czynników ekonomicznych, politycznych i kulturowych, nie zostanie wzbogacony o aspekt cyfrowy.

Głównym zadaniem tego artykułu jest także próba wskazania, w jaki sposób europeizacja łączy się ze zjawiskiem rewolucji technologicznej. Za jeden z czynników dynamizujących europeizację bezpieczeństwa cybernetycznego można uznać rozprzestrzenianie się złośliwego oprogramowania, w tym spamu, oprogramowania szpiegującego czy też działań polegających na wyłudzaniu danych (Komisja Europejska, 2006a, s. 4). Drugim czynnikiem jest technologiczny rozwój. Telefonia komórkowa oraz tzw. internet rzeczy, polegający na obsłudze urządzeń przez komputer i sieć technologiczną, stanowią wyzwanie dla integralności i bezpieczeństwa UE oraz stwarzają dodatkowe możliwości do ataku przez cyberprzestępców.

Polityka bezpieczeństwa cybernetycznego, tak jak zapewne każdy inny obszar polityki państwa, jest wynikiem czynników – pochodzących zarówno z wewnętrznej polityki państwa, jak i mających swoje źródła poza państwem – które mogą być względem siebie konkurencyjne lub się uzupełniać. Dlatego w niniejszym artykule pojęcie europeizacji definiowane jest jako dostosowywanie wymiaru cyberbezpieczeństwa na poziomie państwa do modelu polityki cyberbezpieczeństwa w UE.

W ramach podjętej analizy zasygnalizowano, w jakim stopniu uwspólnotowienie prowadzi do zmian instytucjonalnych i politycznych na poziomie państw członkowskich oraz w jakim zakresie generuje ono coraz większą zbieżność w polityce krajowej poprzez zdefiniowane nor-

my, dyrektywy i ustawy, a także powszechnie artykułowane oświadczenia. W tym kontekście europeizacja rozumiana jest jako przenikanie wymiaru europejskiego na płaszczyznę krajową. Założenie o uzyskaniu identycznych wyników procesu europeizacji w różnych państwach z dużym prawdopodobieństwem może jednak okazać się błędne. Wynika to przede wszystkim z faktu, że wpływy UE są konfrontowane w każdym państwie z innym systemem administracyjnym, gospodarczym, a także z odmiennym zbiorem kultury politycznej i norm społecznych.

Innymi słowy, europeizacja nie oznacza ujednolicenia norm i zasad ponad granicami, ponieważ różnice w polityce i kulturze poszczególnych państw prowadzą do różnych wyników, które są efektem dostosowań tych samych zasad generowanych przez UE. Na przykład dyrektywa NIS była różnie interpretowana w poszczególnych państwach na podstawie odmiennego systemu administracyjnego, kultury politycznej czy choćby oczekiwań społecznych. Należy więc pamiętać, że proces adaptacji zależy od państwa. Istnieje wiele zmiennych, które mogą mieć wpływ na stopień zachodzących zmian (Börzel, 2005; Ladrech, 2010; Michalski, 2013). Państwo jest przedmiotem licznych splecionych i konkurencyjnych bodźców, wynikających zarówno ze strony podmiotów działających w granicach państwa, jak międzynarodowych.

Definiowanie europeizacji

W nauce toczy się dyskusja, w jaki sposób należy zdefiniować pojęcie europeizacji (Olsen, 2001). Dokonano wielu badań, które miały wyjaśnić, w jaki sposób poszczególne instytucje, przepisy prawne, polityczne lub czynniki socjologiczne mogą mieć wpływ na m.in. procesy stosowania prawa UE (Ruszkowski, 2019; Jupille, Caporaso 2009; Slepcevic, 2009).

Europeizacja postrzegana jest jako proces, poprzez który główni aktorzy polityczni, jak np. partie polityczne, grupy interesu, administracja państwowa oraz ustawodawca, dostosowują się do skutków integracji europejskiej (Ladrech, 2005; Green Cowles, Caporaso 2001; Knill, 2001; Olsen, 2003).

W tych podejściach europeizacja opisuje zmiany wewnętrzne spowodowane wpływem generowanym przez UE. Nie wolno jednak w tym kontekście zapominać, że państwa członkowskie tworzą UE i w związku z tym uczestniczą w kształtowaniu polityki UE, do której w następnym etapie muszą się dostosowywać. Można zatem rozpatrywać zjawisko europeizacji jako interaktywny proces zmian zachodzący zarówno na szczeblu krajowym, jak i europejskim. Europeizacja będzie zatem procesem zachodzącym i na poziomie krajowym, i na poziomie europejskim, a także w stosunku do państw i podmiotów trzecich. A zatem europeizacja nie ogranicza się tylko do państw członkowskich UE, ale dotyczy również wymogów stawianych wobec państw kandydujących do UE, jak również inicjuje zmiany wewnętrzne w państwach trzecich (Jacoby, 2001). Okazuje się zatem, że państwa nienależące do UE nie mogą uniknąć nacisków politycznych i gospodarczych, aby dostosować się do wyzwań UE (Dupont, Sciarini, Lutterbeck, 1999). W tym względzie europeizację można również uznać jako wynik procesu, w ramach którego polityka UE rozszerza swój zakres poza granice państw członkowskich. Dotyczy to także organizacji funkcjonujących na arenie europejskiej, takich jak Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE) czy Rada Europy, których polityka jest w dużym stopniu powiązana z UE.

Zgodnie z sugestiami badaczy należy oddzielić europeizację od innych powiązanych pojęć, w szczególności od integracji europejskiej (Pacześniak, Riedel, 2010). Europeizacja nie jest więc synonimem integracji europejskiej, która dotyczy wyjaśnienia, dlaczego państwa narodowe zgadzają się na rezygnację z części swojej suwerenności w celu połączenia w organizacje ponadnarodowe jak np. UE. Integracja – jako proces polityczny – skupia się na tym, co dzieje się z państwem i jego suwerennością, podczas gdy europeizacja analizuje to, co dzieje się z państwowymi instytucjami i podmiotami (Boerzel, 2003). W literaturze przedmiotu wydzielono więc linię demarkacyjną, zachowując termin „integracja" na rzecz rozwoju polityki na poziomie ponadnarodowym, odnosząc natomiast termin „europeizacja" do opisania konsekwencji tego procesu dla państwa członkowskiego (Bulmer, Lequesne, 2002). Skutkiem europeizacji jest więc modyfikacja lub adaptacja wymagań europejskich na poziomie państwa.

Badania w zakresie europeizacji skupiają się na roli, jaką odgrywają państwa członkowskie na szczeblu UE. Analiza tego zjawiska dotyczy również wpływu krajowych preferencji politycznych i interesów na rozwój instytucjonalny oraz kształtowanie polityki na szczeblu europejskim – innymi słowy, badania prowadzone są w celu znalezienia odpowiedzi na pytanie, w jakim stopniu państwa członkowskie kształtują swoje preferencje na poziomie UE w ramach powstawania nowych europejskich struktur (Boerzel, 2003).

Zmiana polityki państwa nie jest generowana wyłącznie na poziomie UE, ale może pośrednio wynikać z działań europejskich sąsiadów lub innych podmiotów funkcjonujących w przestrzeni publicznej. Państwa członkowskie UE są nie tylko biernymi odbiorcami zasad, procedur, paradygmatów politycznych artykułowanych ze strony UE, ale stanowią podmiot upubliczniający własne preferencje na poziomie UE.

Głównym wyzwaniem metodologicznym w badaniach nad europeizacją jest zdefiniowanie oraz wyizolowanie zjawisk będących efektem czynników krajowych i globalnych, mających wpływ na decyzje polityczne. Na poziomie państwa modyfikacje mogą również wystąpić z innych przyczyn, takich jak projekty reform (np. sił zbrojnych), zmiany polityczne w wyniku wyborów, wpływ grup nacisku (np. organizacji zrzeszających przemysł zbrojeniowy) lub też nastroje i oczekiwania społeczne będące pokłosiem innych wydarzeń politycznych.

Badacze zauważają, że państwa kandydujące do UE nie są poddawane tylko presji politycznej wynikającej z chęci przystąpienia do struktur europejskich, lecz uczestniczą także w innych procesach politycznych, gospodarczych czy też społecznych, determinujących ich dynamikę i kształt reform wewnętrznych (Börzel, Risse, 2012).

W analizach badawczych obok europeizacji wskazuje się także proces globalizacji i podkreśla się, że oba zjawiska kształtują zachodzące zmiany i dlatego też można je rozważać w sposób uzupełniający (Schmidt, 2002; Verdier, Breen, 2001). Z pewnością w badaniach nad europeizacją cyberbezpieczeństwa nie sposób zdecydowanie określić instytucjonalnych i ideowych nacisków odpowiedzialnych za proces ewolucji w przestrzeni publicznej.

Oprócz europeizacji należy więc uwzględnić inne procesy i czynniki, będące efektem oddziaływań instytucji międzynarodowych, takich jak Międzynarodowy Fundusz Walutowy, Bank Światowy, Światowa Organizacja Handlu (WTO) czy też Organizacja Współpracy Gospodarczej i Rozwoju (OECD), które odgrywają kluczowe rolę w zarządzaniu polityką międzynarodową poprzez regulacje, sugestie polityczne i wzajemne kontakty.

Współczesne wyzwania polityki bezpieczeństwa UE

W ramach stopniowego procesu, trwającego co najmniej od lat 90. XX wieku, UE stała się widocznym podmiotem zarządzania bezpieczeństwem. Już pod koniec zimnej wojny europejski dyskurs o bezpieczeństwie zaczął przesuwać się w kierunku międzynarodowych zagrożeń bezpieczeństwa, które – w świecie postępującej globalizacji – zacierają podział na bezpieczeństwo wewnętrzne i zewnętrzne.

Znaczący dla polityki bezpieczeństwa był etap ewolucji UE po „11 września", który wymusił ustanowienie UE jako podmiotu bezpieczeństwa w obliczu międzynarodowych zagrożeń. Stopniowo też polityka UE została głęboko powiązana z szerszymi kryzysami politycznymi związanymi z problemami transnarodowymi, takimi jak: cyberzagrożenia, przestępczość zorganizowana, „kryzys uchodźczy" czy też brexit. Kwestie bezpieczeństwa zostały w związku z tym przeniesione na szczyt politycznego programu i głęboko powiązane z kryzysami politycznymi i debatami na temat integracji europejskiej.

W tym kontekście Komisja Europejska coraz częściej zaczęła używać bezpieczeństwa jako kluczowej narracji w komunikatach publicznych: „Unia dąży do zapewnienia ludziom życia w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, bez granic wewnętrznych. Europejczycy muszą mieć pewność, że dokądkolwiek się przeprowadzą w Europie ich wolność i bezpieczeństwo są dobrze chronione" (Komisja Europejska, 2015a).

W 2015 roku Jean-Claude Juncker podkreślił, że „potrzebujemy unii rynków kapitałowych, unii energetycznej, unii gospodarczej i walutowej, ale uważamy również, że potrzebujemy unii bezpieczeństwa" (Juncker, 2016).

Szczyt Rady Europejskiej w Bratysławie w 2016 roku podkreślił znaczenie bezpieczeństwa, także w wymiarze społecznym, co stanowiło odpowiedź na coraz większe obawy obywateli wobec współczesnych zagrożeń. Perspektywa ta została powtórzona w *Deklaracji rzymskiej* z marca 2017 roku, w której państwa członkowskie uznały bezpieczeństwo jako jeden z podstawowych priorytetów UE (Rada Europejska, 2016).

W tym kontekście należy zaznaczyć, że bezpieczeństwo jest coraz częściej wykorzystywane jako znacznie szersza metafora projektu europejskiego. Na przykład w czerwcu 2018 roku Niemiecka kanclerz Angela Merkel oświadczyła: „Europa obiecała swoim obywatelom nie tylko pokój, ale także bezpieczeństwo" (Merkel, 2018).

Warto zauważyć, że następuje coraz większe upolitycznienie bezpieczeństwa, które wzrasta, gdy uczestniczące w debacie strony reprezentują coraz bardziej zróżnicowane lub sprzeczne poglądy na dany temat, trafiając w ten sposób do dyskursu politycznego (Grande, Hutter, 2016). W tym kontekście szczególnie ważna staje się uwaga, że bezpieczeństwo, które do tej pory stanowiło wyjątkowy konsensus w debacie politycznej, staje się ważną osią sporu politycznego. Polityka bezpieczeństwa jest więc areną szerszych debat koncentrujących się na kwestiach tożsamości i suwerenności. Dotychczasowe kontrowersje dotyczące bezpieczeństwa europejskiego odzwierciedlają stare i nowe polityczne rozterki w UE, podobnie jak ma to miejsce na szczeblu państw członkowskich. Konflikt „więcej Europy" kontra „mniej Europy" jest coraz bardziej znany z innych dziedzin integracji europejskiej.

Współczesne wyzwania, takie jak „kryzys uchodźczy", potęgują wzrost populizmu i eurosceptycyzmu, co prowadzi do kontestowania decyzji w zarządzaniu polityką bezpieczeństwa wśród

wielu przedstawicieli państw członkowskich (Börzel, Risse, 2018). Z jednej strony podkreślanie UE jako podmiotu gwarantującego bezpieczeństwo pozycjonuje ją jako źródło władzy. Z drugiej strony polityka bezpieczeństwa UE w coraz większym stopniu dotyczy kwestii delikatnych, które zmuszają do zadawania pytań dotyczących tożsamości narodowej i europejskiej. Wiele krytycznych podejść do bezpieczeństwa umiejscawia ten problem w samym centrum współczesnego sporu politycznego. W takich przypadkach krytyka dotyczy nie tylko adekwatności konkretnych polityk UE, ale służy jako przestrzeń do szerszych zmagań politycznych dotyczących bardziej tradycyjnych koncepcji tożsamości narodowej.

Zmiany w obszary polityki bezpieczeństwa cybernetycznego UE

Cyberbezpieczeństwo jako zjawisko, ale także jako istotny element polityki europejskiej, weszło do leksykonu UE w wyniku m.in. zwiększonej liczby zagrożeń dla bezpieczeństwa informacji i sieci, a także coraz bardziej dynamicznego procesu cyfryzacji obejmującego przestrzeń publiczną. Zagrożenia terrorystyczne ułatwiły zmianę w postrzeganiu znaczenia informacji i systemów sieciowych w Europie (Carrapico, Barrinha, 2017). W wyniku tego kwestie ekonomiczne, które wiodły dotychczas prym w dyskursie na temat przyszłości Europy, zostały uzupełnione o treści bezpośrednio odwołujące się do bezpieczeństwa UE.

Bezpieczeństwo europejskie było i jest silnie upolitycznione w tym sensie, że często zachęca do budowania sojuszy bądź inicjuje podziały pomiędzy państwami członkowskimi na forum UE. Sama już dyskusja publiczna, np. na temat granic cyberbezpieczeństwa w stosunku do wolności, zmusza do zabrania stanowiska przez poszczególne rządy.

W literaturze przedmiotu padają sugestie, że UE staje się rzeczywistym aktorem bezpieczeństwa opartym na nowych kompetencjach, a także ma możliwości tworzenia narracji dotyczącej bezpieczeństwa (Carrapico, 2014; Sperling, Webber, 2019). W tym przypadku polityka bezpieczeństwa UE definiowana jest jako zarządzanie ryzykiem za pośrednictwem wyspecjalizowanych agencji, nowoczesnych technologii i „specjalistów ds. bezpieczeństwa" (Balzacq, 2008; Neal, 2009).

Zarządzanie bezpieczeństwem UE w dużej mierze kształtowane jest poza otwartym konfliktem politycznym i interesem publicznym. Początkowo badania nad polityką w tym obszarze koncentrowały się głównie na państwie narodowym jako centrum politycznym. Niektórzy badacze twierdzą jednak, że wraz z postępującą globalizacją i przeniesieniem władzy na poziom instytucji międzynarodowych UE stała się tematem rosnącej uwagi publicznej i stanęła przed nowymi wymaganiami i zadaniami, których realizacja nie może odbyć się za pomocą tradycyjnych form politycznych (DeWilde, Leupold, Schmidtke, 2016).

W szczególności, aby uchwycić przyszły kierunek bezpieczeństwa europejskiego i ogólnie integracji europejskiej, warta uwagi badawczej jest dynamika rozwoju polityki cyberbezpieczeństwa. Za sprawą coraz większej dominacji w życiu codziennym technologii cyfrowych dotychczasową politykę bezpieczeństwa zaktualizowano o zagrożenia wymierzone w funkcjonowanie gospodarki rynkowej, społeczeństwa obywatelskiego, systemu medialnego czy też przestępstwa przeciwko własności prywatnej w internecie. To zjawisko jest silnie powiązane z rosnącym znaczeniem kwestii bezpieczeństwa cybernetycznego dla każdej nowoczesnej gospodarki usługowej, a tym samym dla wszystkich państw członkowskich UE.

Wielość podmiotów uczestniczących obecnie w polityce europejskiej, za sprawą postępu cybertechnologicznego, zmusza także do zastanowienia się, czy dotychczasowy wzór zarządzania UE nie ulega zmianom w kierunku zdecentralizowanego modelu polityki, opartego na równym partnerstwie między rządem, sektorem prywatnym, społeczeństwem obywatelskim i ekspertami technicznymi. Grupy pozarządowe, takie jak przedstawiciele branży internetowej, społeczeństwa obywatelskiego lub społeczności technicznej, coraz częściej uczestniczą w procesach decyzyjnych. W ten sposób koordynacja europejska staje się bardziej otwarta, dzięki czemu kierunek zmian ma charakter znacznie bardziej oddolny.

Współczesne zagrożenia oznaczają również, że bezpieczeństwo europejskie w coraz większym stopniu realizowane jest na innych płaszczyznach przy współpracy z wieloma podmiotami. Wiele organizacji aktywnych i zainteresowanych bezpieczeństwem europejskim w coraz większym stopniu wykracza poza dotychczasowe ramy instytucjonalne, w ten sposób problematyczny staje się obszar zaangażowania organizacji pozarządowych czy też organizacji prywatnych. Można przypuszczać, że w niedalekiej przyszłości będzie nasilać się spór na temat kwestii bezpieczeństwa narodowego, w którym z jednej strony istnieć będzie wyraźny nacisk na rolę państwa, a z drugiej – obecny będzie pogląd, aby dopuścić podmioty niepaństwowe do odpowiedzialności za bezpieczeństwo cybernetyczne państwa i społeczeństwa.

Ponadto tradycyjne rozróżnienie między sektorem prywatnym a publicznym coraz bardziej zanika w powstającej polityce cybernetycznej. Bez wiedzy technologicznej, będącej najczęściej domeną prywatnych firm, trudno zidentyfikować odpowiednie zagrożenia i odpowiednio na nie reagować. Wiele prywatnych podmiotów jest również odpowiedzialnych za krytyczną infrastrukturę cyfrową, dostawy usług cybernetycznych czy też za funkcjonowanie sektora energetycznego i transportowego.

Zaangażowanie tych firm w zarządzanie ryzykiem i kryzysami, a także procesy identyfikacji zagrożeń, to decydująca część utrzymania bezpieczeństwa publicznego. Okazuje się zatem, że instytucje te odgrywają dużą rolę w procesie europeizacji cyberbezpieczeństwa, przyjmując oraz wpływając na normy i ustalenia unijne, ale i także kształtując rzeczywistość gospodarczą innych państw.

Wybrane regulacje oraz instytucje UE w zakresie cyberbezpieczeństwa

Stopniowo zaczęto zauważać potrzebę zmian w obszarze regulacji prawnych. Wskazano, że ataki na systemy informatyczne, będące wynikiem bądź to przestępczości zorganizowanej, bądź działalności terrorystycznej, skierowane na infrastrukturę krytyczną państw członkowskich wymagają reakcji na poziomie Unii Europejskiej (Komisja Europejska, 2005).

Komunikat Komisji Europejskiej *Strategia na rzecz bezpiecznego społeczeństwa informacyjnego* (Komisja Europejska, 2006b) oraz kolejne dokumenty propagowały szerszą inicjatywę w ramach europejskiej agendy cyfrowej (Komisja Europejska, 2010), której celem było „opracowanie globalnej strategii w Europie, opartej na kulturze bezpieczeństwa" (Komisja Europejska, 2006). Oznaczało to podejście wielu zainteresowanych stron i budowanie wspólnotowej polityki bezpieczeństwa, która radziłaby sobie nie tylko z objawami, ale także z podstawowymi przyczynami cyberzagrożeń na poziomie indywidualnym oraz instytucjonalnym.

Z biegiem czasu ochrona przed cyberprzestępczością stała się jednym z najwyższych priorytetów dla UE. Według Komisji Europejskiej był to także impuls do podjęcia „wysiłków na rzecz opracowania nadrzędnej strategii UE na rzecz wzmocnienia obronności cyfrowej" (Komisja Europejska, 2012a).

Strategia bezpieczeństwa cybernetycznego UE ogłoszona w 2013 roku stała się centralnym punktem regulacji międzynarodowych i ważnym instrumentem dla państw członkowskich. Dokument ten potwierdził złożoność problemu i potrzebę zaangażowania różnorodnych podmiotów, co oznaczało budowę kompleksowej polityki cyberbezpieczeństwa. Podkreślono także, że ze względu na potencjał i charakter transnarodowy zagrożeń cybernetycznych skuteczna reakcja poszczególnych rządów wymaga zaangażowania na szczeblu UE. W ten sposób strategia uzasadniała rolę UE, której obrona cybernetyczna obejmowałaby wiele zadań spoczywających na organach takich jak: ENISA, Europol, Komisja Europejska i inne. Co ciekawe, strategia jest pierwszym dokumentem wyjaśniającym potrzebę ugruntowania w unijnej polityce – oprócz wysiłków związanych z walką z cyberprzestępczością oraz zapewnieniem bezpieczeństwa dla sieci i informacji – „zdolności do cyberobrony". Odzwierciedla ona zatem priorytety tych podmiotów w ramach instytucji UE, które były odpowiedzialne za rozwój różnych aspektów polityki bezpieczeństwa cybernetycznego, jak m.in. Europejska Agencja Obrony czy Europejska Służba Działań Zewnętrznych, na których spoczywa odpowiedzialność za cyberobronę.

Obok *Strategii bezpieczeństwa cybernetycznego Unii Europejskiej* z 2013 roku drugim ważnym dokumentem jest *Dyrektywa dotycząca bezpieczeństwa sieci i systemów informatycznych* (NIS). Dokument ten został przyjęty po długich dyskusjach w sierpniu 2016 roku (Rada Unii Europejskiej, 2017). Jego celem jest przygotowywanie państw członkowskich wobec incydentów cybernetycznych poprzez m.in. powołanie Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSRIT), których głównym zadaniem jest zapobieganie i wykrywanie możliwych cyberataków oraz łagodzenie ich konsekwencji.

Dyrektywa NIS jest pierwszym europejskim aktem prawnym, który wskazuje na potrzebę zgłaszania incydentów cybernetycznych we wszystkich państwach członkowskich. Dostrzec więc można, że regulacje UE zmierzają w kierunku obowiązkowego zgłaszania incydentów i ataków cybernetycznych, bowiem dobrowolne i nieformalne środki okazują się często niewystarczające do pełnego uczestnictwa sektora prywatnego w zapewnieniu cyberbezpieczeństwa.

Wraz ze *Strategią cyberbezpieczeństwa UE*, *Europejską agendą bezpieczeństwa* (Komisja Europejska, 2015b) oraz *Wspólnymi ramami dotyczącymi przeciwdziałania zagrożeniom hybrydowym* (Komisja Europejska, Europejska Służba Działań Zewnętrznych, 2016) UE buduje model zarządzania ryzykiem związanym z cyberzagrożeniami. Bezpieczeństwo cybernetyczne jest również uznawane za priorytetowy obszar w komunikacie UE dotyczącym uruchomienia Europejskiego Funduszu Obrony (Komisja Europejska, 2017a). W 2017 roku UE przyjęła również ramy wspólnej polityki dotyczącej reakcji na działania cybernetyczne (Komisja Europejska, 2017b). W wielu dokumentach, w tym także w strategii cyberbezpieczeństwa UE, dostrzegalny jest proces europeizacji, który polega na transpozycji prawodawstwa UE do prawa krajowego i wdrożenia skutecznych zasad, które pociągają za sobą zmiany w krajowej polityce cyberbezpieczeństwa.

Ważnym etapem na drodze rozwoju procesu europeizacji cyberbezpieczeństwa było utworzenie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) w 2004 roku. Odegrała

ona kluczową rolę w zdefiniowaniu najlepszych praktyk oraz w określeniu działań zwiększających współpracę między wszystkimi zainteresowanymi stronami. W pierwotnym mandacie z 2005 roku powierzono tej instytucji również wsparcie dla krajowych zespołów reagowania na incydenty komputerowe (CERT), dla których ustanowiono programy oraz grupę roboczą ds. współpracy (Parlament Europejski, Rada Unii Europejskiej, 2004). ENISA, podobnie jak cały proces rozwoju polityki cyberbezpieczeństwa UE, została utworzona ze względu na rosnącą liczbę zagrożeń cybernetycznych, które powodowały szkody finansowe i podważały zaufanie do instytucji publicznych, co negatywnie wpływało na plany UE dotyczące rozwoju handlu elektronicznego (e-commerce). W wyniku przedłużenia mandatu przez Komisję Europejską w 2017 roku ENISA uzyskiwała coraz większe kompetencje pozwalające na działania operacyjne, a także na podejmowanie inicjatyw na dużo większą skalę, odgrywając w ten sposób rolę w paneuropejskim systemie bezpieczeństwa cybernetycznego (Komisja Europejska, 2017). Istotny wpływ tej instytucji przejawia się także w procesie zarządzania bezpieczeństwem, polegającym na ułatwieniu interakcji pomiędzy instytucjami publicznymi a podmiotami prywatnymi.

Kolejnym etapem w europeizacji bezpieczeństwa cybernetycznego był komunikat w sprawie ochrony teleinformatycznej infrastruktury krytycznej (CIIP) (Komisja Europejska, 2009), który został uwzględniony równolegle do zmian przepisów UE dotyczących komunikacji elektronicznej (Parlament Europejski, Rada Unii Europejskiej, 2009). Ta zmiana obejmowała głównie art. 13a, który wprowadzał obowiązek zgłaszania wszelkich naruszeń systemów bezpieczeństwa przez krajowy organ regulacyjny (co było znaczącą zmianą w stosunku do poprzedniego zapisu z 2006 roku, który pozostawiał dobrowolność w tym zakresie), przy czym ENISA jest podmiotem, który ma wspierać państwa członkowskie we wdrażaniu art. 13a poprzez wytyczne techniczne dotyczące zgłaszania incydentów (ENISA, 2013).

Można przypuszczać, że ustawiczny wzrost cyberprzestępczości spowodował, że priorytetem strategicznym w zakresie utrzymania bezpieczeństwa cybernetycznego stała się rola Europejskiego Centrum ds. Cyberprzestępczości (EC3) działającego przy Europolu.

Zadaniem EC3 jest dostosowanie zadań do działań innych odpowiednich agencji UE, takich jak Europejska Jednostka Współpracy Sądowej (Eurojust), ENISA i Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL). Ma to zapewnić, że zadania, w tym szkolenia, budowanie zdolności, analiza strategiczna oraz wsparcie techniczne, określone w ramach *Europejskiej multidyscyplinarnej platformy przeciwko zagrożeniom przestępstwami* (EMPACT), będą skutecznie realizowane (Europol, 2014). Cykl polityki EMPACT został stworzony przez Radę UE w 2010 roku w celu przeciwdziałania „najważniejszym zagrożeniom przestępczym w sposób spójny i metodologiczny, poprzez optymalną współpracę między odpowiednimi służbami państw członkowskich, instytucji UE i agencji UE, a także odpowiednimi organizacjami i państwami trzecimi" (Komisja Europejska, 2014).

Jednym z namacalnych aspektów EC3 jest utworzenie we wrześniu 2014 roku wspólnej grupy zadaniowej ds. cyberprzestępczości (J-CAT), złożonej z oficerów łącznikowych policji z państw członkowskich oraz funkcjonariuszy organów ścigania z państw z poza UE. J-CAT podlega bardzo specyficznym ramom prawnym, które zapewniają elastyczne i szybkie reakcje, omijające przeszkody biurokratyczne i prawne wynikające m.in. z odrębnych norm państw członkowskich.

Pod względem zarządzania bezpieczeństwem EC3 i osadzony w nim J-CAT zapewniły nowy sposób wykonywania zadań – z udziałem podmiotów publicznych i prywatnych, zarówno krajowych, jak i międzynarodowych – co pozwala na skuteczne i terminowe podjęcie działań przeciwko cyberprzestępcom. Nowe praktyki zarządzania bezpieczeństwem wskazują zatem na ponadnarodowe procesy zachodzące w zakresie ochrony cybernetycznej.

Przywołane powyżej przykłady instytucji działających w obszarze cyberbezpieczeństwa udowadniają, że państwa narodowe nadal odgrywają ważną rolę, gwarantując bezpieczeństwo narodowe i ochronę prywatności, ale ich możliwości działania, szczególnie w cyberprzestrzeni, są bardzo ograniczone, dlatego niezwykle ważne jest to, aby różne przepisy krajowe były zharmonizowane na poziomie międzynarodowym. Cyberprzestępstwa mogą bowiem być popełniane z obszaru innego państwa, w którym brakuje podstaw prawnych dla jakiejkolwiek formy ścigania szkodliwych działań. A zatem prawodawstwo w dziedzinie bezpieczeństwa cybernetycznego przekracza granice państw narodowych.

Podsumowanie

W ostatnich latach wszystkie państwa UE zintensyfikowały działania i wysiłki na rzecz poprawy ochrony instytucji państwowych oraz prywatnych przedsiębiorstw przed atakami internetowymi. Z pewnością określenie zakresu prerogatyw państwa a UE oraz innych organizacji międzynarodowych, a także próby określenia ośrodka decyzyjnego będą wzbogacać dyskusje na temat procesu europeizacji cyberbezpieczeństwa. Wyzwaniem pozostaje poszukiwanie odpowiedzi na pytanie, jak rozwinie się zarządzanie bezpieczeństwem cybernetycznym na poziomie UE i w jakim stopniu proces europeizacji zdeterminuje politykę cyfrową państw członkowskich.

Roczne raporty dotyczące zagrożeń cybernetycznych publikowane przez ENISA wskazują na potrzebę zapewnienia kontynuacji i zintensyfikowania wspólnych działań w zakresie cyberbezpieczeństwa, które objęte będą programem UE. W podobnym tonie zaktualizowana została strategia cyberbezpieczeństwa UE we wrześniu 2017 roku przez Komisję Europejską. Zasygnalizowano w niej wzrost zagrożeń, które z pewnością będą dynamizować proces europeizacji cyberbezpieczeństwa.

Można zatem zauważyć, jak zmiana środowiska bezpieczeństwa przyczyniła się do rozwoju platform zarządzania bezpieczeństwem, instrumentów i agencji, które wpisują się w proces europeizacji bezpieczeństwa cybernetycznego UE. Polityka wobec cyberprzestępczości oraz ochrona sieci i systemów informatycznych wpływa również w istotny sposób na funkcjonowanie prawa i ekonomii państw członkowskich. Ponadto można argumentować, że w obszarach cyberbezpieczeństwa istnieją dowody na to, że UE była w stanie ćwiczyć własne kompetencje, dzięki czemu kształtowała swoją tożsamość jako podmiot cyberbezpieczeństwa. Można zaobserwować, jak postrzeganie cyberzagrożeń lub interpretacja zaistniałych cyberincydentów może wpływać na pojawianie się nowych inicjatyw związanych z zarządzaniem cyberzagrożeniami, jak np. EC3 i J-CAT, oraz przekształcania i poszerzanie zadań agencji takich jak ENISA, zajmujących się bezpieczeństwem sieci i systemów informacyjnych. Innymi słowy cyberincydenty mogą być czynnikiem inicjującym innowacyjne działania w zakresie polityki bezpieczeństwa cybernetycznego na poziomie UE.

Przestawione w artykule normatywne i polityczne konsekwencje opisanych tendencji uzasadniają dalszą analizę w kontekście następnych badań nad procesem europeizacji cyberbezpieczeństwa. Wzrost znaczenia cyberprzestrzeni wyraźnie umożliwia UE pełnienie funkcji polegającej na zarządzaniu bezpieczeństwem w zakresie wprowadzania zarówno modelu interakcji pomiędzy podmiotami, jak i wzoru regulacji kształtujących politykę bezpieczeństwa cybernetycznego wśród państw członkowskich.

Bibliografia

Balzacq, T. (2008). The policy tools of securitization: information exchange, EU foreign and interior policies. *Journal of Common Market Studies*, *46 (1)*, 75–100.

Börzel, T. (2003). *Shaping and Taking EU Policies: Member State Responses to Europeanizatio*n *(No. p0035)*. Pobrane z: https://ideas.repec.org/p/ erp/queens/p0035.html (18.09.2019).

Börzel, T.A. (2005). Europeanization: How the European Union Interacts with Its Member States. W: S. Bulmer, Ch. Lequesne (red.), *The Member States of the European Union* (s. 45–69). Oxford: Oxford University Press.

Börzel, T., Risse, T. (2018). From the Euro crisis to the Schengen crisis: European integration theories, politicization and identity politics. *Journal of European Public Policy*, *25 (1)*, 83–108.

Börzel, T.A., Risse, T. (2003). Conceptualizing the Domestic Impact. W: K. Featherstone, C. Radaelli (red.), *The Politics of Europeanization*. Oxford: Oxford University Press.

Börzel, T.A., Risse, T. (2012). From Europeanisation to diffusion. *West European Politics*, *35(1)*, 1–19.

Carrapico, H. (2014). Analysing the European Union's responses to organised crime through different securitisation lenses. *European Security*, *23 (4)*, 601–617.

Carrapico, H., Barrinha, A. (2017). The EU as Coherent (Cyber) Security Actor? *Journal of Common Market Studies*, *6 (55)*, 1–19.

Costa, O. (2019). The politicisation of EU external relations. *Journal of European Public Policy*, *26 (5)*, 790–802.

De Wilde, P., Leupold, A., Schmidtke, H. (2016). Introduction: the differentiated politicisation of European governance. *West European Politics*, *39 (1)*, 3–22.

Dupont, C., Sciarini, P., Lutterbeck, D. (1999). Catching the EC Train: Austria and Switzerland in Comparative Perspective. *European Journal of International Relations*, *5 (2)*, 191–224.

ENISA (2013). *Wytyczne techniczne dotyczące zgłaszania incydentów*. Pobrane z: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0 (22.09.2019).

ENISA (2016). *Sprawozdanie na temat krajobrazu zagrożeń w 2016 r.* Pobrane z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 (24.08.2019).

Europol (2014). *Europejskie Centrum ds. Cyberprzestępczości (EC3) – Sprawozdanie za pierwszy rok*. Pobrane z: https://www.europol.europa.eu/content/european-cybercrime-center-ec3-firstyear-report (20.09.2019).

Grande, E., Hutter, S. (2016). Introduction: European integration and the challenge of politicisation. W: S. Hutter, E. Grande, H. Kriesi (red.), *Politicising Europe: integration and mass politics* (s. 3–31). Cambridge: Cambridge University Press.

Green Cowles, M., Caporaso, J. (red.) (2001) *Transforming Europe. Europeanization and Domestic Change*. Ithaca, NY: Cornell University Press.

Hegemann, H. (2018). Toward „normal" politics? Security, parliaments and the politicization of intelligence oversight in the German Bundestag. *British Journal of Politics and International Relations*, *20 (1)*, 175–190.

Jacoby, W. (2001). Tutors and Pupils: International Organizations, Central European Elites, and Western Models. *Governance*, *14 (2)*, 169–200.

Juncker, J.C. (2016). *Juncker after Brussels terror attack: „we feel we need a security union"*. Pobrane z: https://www.euractiv.com/section/justice-home-affairs/video/junckerafter-brussels-terror-attacks-we-need-a-security-union/ (26.08.2019).

Jupille, J. Caporaso, J. (2009). Domesticating discourses: European law, English judges and political institutions. *European Political Science Review, 1 (2)*, 205–228.

Knill, C. (2001). *The Europeanization of National Administrations. Patterns of Institutional Change and Persistence*. Cambridge: Cambridge University Press.

Komisja Europejska (2005). *Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie komunikatu Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów i2010 — Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia COM (2005) 229 końcowy*. Pobrane z: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52006AE0415 (22.09.2019).

Komisja Europejska (2006a). *Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatywy"*. Pobrane z: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52006DC0251 (4.09.2019).

Komisja Europejska (2006b). *Strategia na rzecz bezpiecznego społeczeństwa informacyjnego — Dialog, partnerstwo i przejmowanie inicjatywy COM (2006) 251 wersja ostateczna*. Pobrane z: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007AE0211 (25.09.2019).

Komisja Europejska (2009). *W sprawie ochrony krytycznej infrastruktury informatycznej – „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności"***.** Pobrane z: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52009DC0149&from=en (18.09.2019).

Komisja Europejska (2010). *A Digital Agenda for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. Pobrane z: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0245R%2801%29 (23.09.2019).

Komisja Europejska (2012). *Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością*. Pobrane z: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52012DC0140&from=EN (27.09.2019).

Komisja Europejska (2013). *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*. Pobrane z: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52013JC0001 (22.09.2019).

Komisja Europejska (2015a). *Europejska agenda bezpieczeństwa*, *COM(2015) 185 final*. Pobrane z: https://ec.europa.eu/anti-trafficking/eu-policy/european-agenda-security_en (12.09.2017).

Komisja Europejska (2015b). *European Agenda on Security*. Pobrane z: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_ security_en.pdf (26.09.2019).

Komisja Europejska (2016). *Komisja podpisuje porozumienie z przemysłem w sprawie bezpieczeństwa cybernetycznego i wzmaga wysiłki na rzecz zwalczania zagrożeń cybernetycznych*. Pobrane z: http://europa.eu/rapid/press-release_IP-16-2321_en.htm (04.09.2019).

Komisja Europejska (2017a). *Launching the European Defence Fund, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. Pobrane z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0295 (22.09.2019).

Komisja Europejska (2017b). *W sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę*. Pobrane z: https://ec.europa.eu/transparency/regdoc/rep/3/2017/PL/C-2017-6100-F1-PL-MAIN-PART-1.PDF (23.09.2019).

Komisja Europejska (2017c). *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*. Pobrane z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN (12.10.2019).

Komisja Europejska, Europejska Służba Działań Zewnętrznych (2016). *Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats: A European Union Response*. Pobrane z: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016JC0018 (26.09.2019).

Ladrech, R. (2005). The Europeanization of interest groups and political parties. W: S. Bulmer, C. Lesquesne (red.), *The Member States and the European Union* (s. 318–337). Oxford: Oxford University Press.

Ladrech, R. (2010). *Europeanization and National Politics*. Houndsmill: Palgrave Macmillan.

Merkel, A. (2018). *Europa muss handlungsfähig sein*. Pobrane z: https://www.bundeskanzlerin.de/Content/DE/Interview/2018/06/2018-06-04-merkel-fas.html (26.08.2019).

Michalski, A. (2013). Europeanization of National Foreign Policy: The Case of Denmark's and Sweden's Relations with China. *Journal of Common Market Studies*, *51 (5)*, 884–900.

Neal, A. (2009). Securitization and risk at the EU border: the origins of FRONTEX. *Journal of Common Market Studies*, *47 (2)*, 333–356.

Olsen, J.P. (2001). 'Garbage Cans, New Institutionalism, and the Study of Politics'. *American Political Science Review*, *95 (1)*, 191–198.

Olsen, J.P. (2003). Towards a European administrative space? *Journal of European Public Policy*, *10 (4)*, 506–531.

Pacześniak, A., Riedel, R. (red.) (2010). *Europeizacja – mechanizmy, wymiary, efekty*. Toruń: Adam Marszałek.

Parlament Europejski, Rada Unii Europejskiej (2004). *Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji*. Pobrane z: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32004R0460&from=EN (12.10.2019).

Parlament Europejski, Rada Unii Europejskiej (2009). W *sprawie dostępu do sieci i usług łączności elektronicznej oraz wzajemnych połączeń oraz 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej*. Pobrane z: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32009L0140&from=en (22.09.2019).

Rada Europejska (2016). *Deklaracja z Bratysławy*. Pobrane z: https://www.consilium.europa.eu/en/press/press-releases/2016/09/16/bratislava-declaration-and-roadmap/ (12.09.2017).

Rada Unii Europejskiej (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities*. Pobrane z: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf (23.09.2019).

Ruszkowski, J. (2019). *Europeizacja. Analiza oddziaływania Unii Europejskiej*. Warszawa: Difin.

Schmidt, V.A. (2002). *The Futures of European Capitalism*. Oxford: Oxford University Press.

Slepcevic, R. (2009). The judicial enforcement of EU law through national courts: possibilities and limits. *Journal of European Public Policy*, *16*, 378–394.

Sperling, J., Webber, M. (2019). The European Union, security governance and collective securitization. *West European Politics*, *42 (2)*, 228–260.

Verdier, D., Breen, R. (2001). Europeanization and globalization. Politics against markets in the European Union. *Comparative Political Studies*, *34(1)*, 227–262.

Wagner, W. (2018). Party politics at the water's edge: contestation of military operations in Europe. *European Political Science Review*, *10 (4)*, 537–563.