Uniwersytet im. Adama Mickiewicza

w Poznaniu

Wydział Nauk Politycznych i Dziennikarstwa

Robert Maciejewski

Cyberterroryzm w polityce bezpieczeństwa państwa. Problemy ochrony infrastruktury krytycznej

Praca doktorska

Promotor: prof. UAM dr hab. Maciej Walkowski

Promotor pomocniczy: dr Rafał Kamprowski

Poznań 2019

Spis treści

Wstęp

Głównym celem badawczym pracy jest próba odpowiedzi na pytanie, jaki wpływ ma zjawisko cyberterroryzmu oraz inne zagrożenia asymetryczne na rozwój regulacji prawnych, chroniących bezpieczeństwo infrastruktury krytycznej w Polsce. W zakresie objętym badaniem mieści się również próba wyodrębnienia najbardziej istotnych problemów ochrony infrastruktury krytycznej przed zagrożeniami o charakterze cyberterrorystycznym, a także próba prognozy kierunków ewolucji strategii ochrony infrastruktury krytycznej RP.

Aby osiągnąć założony cel, sformułowane zostały trzy problemy szczegółowe, w formie następujących pytań:

1. Czy możliwe jest wypracowanie jednoznacznej i kompletnej definicji infrastruktury krytycznej, uwzględniające nie tylko systemowość oraz poziom krytyczności jej elementów, ale także wpływ politycznego, społecznego i gospodarczego otoczenia IK?
2. Czy w świetle obowiązującej legislacji możliwe jest stworzenie jednolitej i kompleksowej metodyki identyfikacji poszczególnych elementów infrastruktury krytycznej?
3. Czy możliwe jest określenie prognozowanych kierunków rozwoju polityk i strategii ochrony systemów infrastruktury krytycznej w Polsce?

Przyjmując neoinstytucjonalną perspektywę badawczą, do osiągnięcia wytyczonego celu głównego wykorzystano przede wszystkim takie metody badawcze, jak analiza instytucjonalno-prawna oraz analiza porównawczą. Ważnym elementem procesu badawczego stała się także próba zaprezentowania elementów procesu historycznego nie tylko jako wprowadzenia do opisu genezy zjawisk takich jak terroryzm czy cyberterroryzm, lecz także przy analizie dokumentów strategicznych i prawnych. Dokonano między innymi przeglądu dotychczasowego stanu legislacji związanej z ochroną bezpieczeństwa cyberprzestrzeni w dokumentach strategicznych Unii Europejskiej (rozdział II), Stanów Zjednoczonych Ameryki Północnej (rozdział III) oraz Rzeczpospolitej Polskiej (rozdział IV), zwracając uwagę nie tylko na zależności ściśle chronologiczne w ramach procesu prawotwórczego konkretnego państwa czy federacji, lecz także na skutki wzajemnego wpływu. Nie sposób bowiem, zdaniem autora, dokonać istotnej poznawczo analizy aktualnych problemów ochrony infrastruktury krytycznej w kontekście zagrożenia cyberterroryzmem, pomijając kontekst uwarunkowań historycznych, politycznych czy społecznych. Znaczący nacisk położono więc szczególnie na analizę problematyki

niejednolitości identyfikacyjnej i definicyjnej zarówno zjawiska cyberterroryzmu, jak i pojęcia infrastruktury krytycznej. W ocenie autora, problematyka definiowania obu tych pojęć może być kluczowa dla poprawnej analizy faktycznej zdolności współczesnych państw do zapewnienia bezpieczeństwa infrastruktury krytycznej, zwłaszcza przed zagrożeniami o charakterze cyberterrorystycznym.

Dla analizy pochodzących z cyberprzestrzeni zagrożeń dla infrastruktury krytycznej determinującą wydaje się być komplementarna i jednoznaczna identyfikacja zasobów infrastruktury krytycznej. Głównie ona bowiem, wzbogacona o ocenę poziomu krytyczności, pozwala dokonać właściwej kategoryzacji zagrożeń, a więc i wynikowo ochrony przed nimi. Poddano zatem analizie pogląd, iż precyzyjne zdefiniowanie infrastruktury krytycznej, choć możliwe na poziomie dokumentów strategicznych powstałych w wyniku procedur legislacyjnych, nie zawsze jest osiągalne i możliwe w ujęciach teoretycznym i badawczym. Tymczasem właśnie uwzględnienie szerokiego kontekstu politycznego, społecznego i gospodarczego otoczenia infrastruktury krytycznej (ściśle związane choćby z samym pojęciem bezpieczeństwa, rozumianego jako kategoria o szczególnie multidyscyplinarnym i wieloaspektowym charakterze) winno poprzedzać definiowanie infrastruktury krytycznej jako zbioru systemów i wchodzących w ich skład elementów. Zdaniem autora nie tylko sama systemowość infrastruktury krytycznej, lecz także jej otoczenie społeczne i gospodarcze, wpływają na możliwość zarówno poprawnej identyfikacji jej elementów, jak i właściwą ocenę poziomu ich krytyczności. Podejmując próbę przeanalizowania problemów związanych z identyfikacją infrastruktury krytycznej, autor zauważa, iż niemożność ujęcia pełni zakresu definicyjnego w ramy podejścia o charakterze systemowo-technicznym nie tylko czyni o wiele trudniejszą ochronę IK, lecz wręcz stawia pod znakiem zapytania możliwość poprawnego zidentyfikowania jej w zasobach współczesnego państwa. Bardzo trudne staje się bowiem opracowanie jednolitej i kompleksowej metodyki, która może być wykorzystana dla identyfikacji poszczególnych elementów infrastruktury krytycznej.

W rozdziale VI, będącym próbą analizy instytucjonalno-prawnej strategicznych założeń ochrony infrastruktury krytycznej RP, przedstawiono w ujęciu syntetycznym najważniejsze akty prawne regulujące procedury identyfikacji i ochrony infrastruktury krytycznej w Polsce. Z uwagi na bardzo obszerny materiał badawczy dokonano zawężenia analizowanego zakresu do legislacji krajowej. Zamiarem autora było możliwie szczegółowe przedstawienie ewolucji polityki oraz strategii ochrony infrastruktury krytycznej w kontekście legislacji narodowej. Przyjęcie tej

perspektywy pozwala ocenić, w jakim stopniu wytworzenie procedur prawnych ochrony infrastruktury krytycznej przed zagrożeniami z cyberprzestrzeni stało się jednym z priorytetów stojących przed państwem, a także zdefiniować trudności, jakie stwarza konieczność realizacji tego priorytetu na poziomie legislacyjnym. Przyjęte w kolejnych odsłonach Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK) proceduralne podejście do ochrony obiektów infrastruktury krytycznej na poziomie centralnym (co implikuje dla operatorów infrastruktury krytycznej obowiązek uczestnictwa w systemie ochrony) znacząco różni się od przyjętego w większości krajów UE podejścia strukturalnego, opierającego się na stałym zmniejszeniu krytyczności infrastruktury, a także systemu partnerstwa publiczno-prywatnego, rozwijanego w USA. Decyzja o poddaniu analizie najważniejszych aktów prawnych regulujących procedury identyfikacji i ochrony infrastruktury krytycznej w Polsce skutkuje także zamieszczeniem w pracy (w rozdziale VII) szczegółowego opisu fizycznych systemów infrastruktury krytycznej RP. Z uwagi na fakt, iż część danych dotyczących fizycznych obiektów systemów pozostaje niejawna, autor skorelował informacje o tym charakterze z danymi ogólnodostępnymi, decydując się na przytoczenie w niniejszym opracowaniu tylko informacji nieobjętych klauzulami niejawności – niemniej jednak składających się na kompletny obraz aktualnych systemów infrastruktury krytycznej RP.

Dotychczasowa wiedza autora, oparta na analizie dokumentów strategicznych dotyczących ochrony infrastruktury krytycznej w Polsce, krajach UE oraz USA, wzbogacona studiami nad dotychczas opublikowaną literaturą przedmiotu, pozwala na określenie prawdopodobnych rozwiązań określonych powyżej problemów badawczych. Rozwiązania te zostały ujęte w formule hipotez roboczych o następującej treści:

1. Wypracowanie jednoznacznej oraz kompletnej definicji infrastruktury krytycznej, uwzględniającego nie tylko systemowość usług i krytyczność fizycznych obiektów, ale też otoczenie społeczne, polityczne oraz gospodarcze IK nie jest możliwe przy przyjętym obecnie w polskiej legislacji podejściu.
2. Wypracowanie jednoznacznie skutecznej oraz komplementarnej metodologii identyfikacji elementów systemów IK, przy aktualnym podejściu przyjętym w polskiej legislacji, nie jest możliwe. Aktualne rozwiązania prawne i proceduralne wydają się w niezadowalającym stopniu odpowiadać na potrzebę identyfikacji zasobów infrastruktury krytycznej w celu ich ochrony przed zagrożeniami z cyberprzestrzeni.

3. Próba prognozy kierunków rozwoju polityk i strategii ochrony systemów w Polsce przez zagrożeniami pochodzącymi z cyberprzestrzeni jest możliwa. Można założyć, iż charakter ewolucji polityk i strategii ochrony IK powinien być symetryczny i adekwatny do dynamicznie zmiennej typologii zagrożeń. Można też przyjąć, iż właśnie konieczność zapobiegania zagrożeniom o tym charakterze, stanie się dystynktywnym determinantem narodowych i międzynarodowych polityk bezpieczeństwa. Przy próbie prognozy dokonać należy:
   a) analizy przyjętych podejść do zapewnienia bezpieczeństwa systemom IK, przy założeniu stabilności kryteriów identyfikacji systemów wchodzących w skład infrastruktury krytycznej,
   b) analizy krajowej i międzynarodowej legislacji w tym zakresie,
   c) próby oceny, które z systemów infrastruktury krytycznej są w sposób szczególny narażone na zagrożenia z cyberprzestrzeni, w wyniku zdefiniowania determinantów ich krytyczności.

W toku prac badawczych wyodrębniono i opisano trzy grupy zagadnień problemowych, które w opinii autora wyznaczają kierunek dla skutecznej ochrony legislacyjnej infrastruktury krytycznej przed cyberterroryzmem i innymi zagrożeniami pochodzącymi z cyberprzestrzeni. Celem niniejszej pracy nie jest przedstawienie technicznych aspektów problematyki ochrony infrastruktury krytycznej, choć oczywiście, wynikowo, są one niezbędne dla kompletności i skuteczności procesu zapobiegania zagrożeniom. Autor skupiając się na analizie najważniejszych aktów prawnych – ustaw, polityk, strategii i innych regulujących procedury identyfikacji i ochrony infrastruktury krytycznej w Polsce (a także w UE oraz USA) – dokonał wyodrębnienia grup problemów powstałych na poziomie prawotwórczym.

W procesie badawczym uwzględniono także czynniki o charakterze geopolitycznym oraz ekonomicznym i społecznym, jednakże w zakresie ich wpływu na kształt i fluktuację międzynarodowych i polskich polityk ochrony cyberprzestrzeni. Do najistotniejszych zakresów problemowych zaliczono trudności definicyjne i identyfikacyjne systemów infrastruktury krytycznej, a także wynikające z tego niejasności w zakresie oceny krytyczności elementów systemu. Wskazano także na zagrożenia płynące z braku weryfikowalnej skuteczności obowiązujących aktów prawnych, a także niezgodność zapisów dokumentów strategicznych z aktami prawnymi wyższego rzędu.

Literatura przedmiotu, dotycząca zarówno kwestii ochrony cyberprzestrzeni, jak i zagadnień związanych z bezpieczeństwem infrastruktury krytycznej, jest stosunkowo bogata oraz różnorodna w ujęciach dyscyplinarnych. Z uwagi na bardzo szeroki zakres tematyczny podejmowany w rozdziałach analityczno-syntetyzujących, zdaniem autora utrudnione jest wskazanie kluczowych dla niniejszego opracowania monografii, niemniej jednak jako szczególnie istotne uważa on prace następujących badaczy: Andrzeja Adamskiego, Tadeusza Aleksandrowicza, Yonah Alexander, Marcina Anszczaka, John Arquilla, Akhgar Babak, Agnieszki Bógdoł-Brzezińskiej, Dorothy Denning, Anny Dziurnej, Dominiki Dziwisz, Mariana Filara, Grzegorza Gancarza, Marcina Gawryckiego, Artura Gruszczaka, Jarosława Gryza, Edwarda Haliżaka, Milton Hoenig, Bogusława Jagusiaka, Jerzego Koniecznego, Ryszarda Kośli, Stanisława Kozieja, Piotra Kwiatkiewicza, Krzysztofa Liedela, Marka Madeja, Piotra Mickiewicza, Jacka Milewskiego, David Ronfeldt, Adriana Siadkowskiego, Wiesława Smolskiego, Tomasza Szubrychta, Artura Wejksznera, Sebastiana Wojciechowskiego, Ryszarda Zenderowskiego i Ryszarda Zięby. Warto wymienić również nazwiska innych badaczy: Francesca Bosco, Jonalan Brickey, Thomas Chen, Andrew Colarik, Lecha Janczewskiego, Daniel Kuehl, Herbert Lin, Macieja Pyznara, Ryszarda Radziejewskiego, Andrew Staniforth, Przemysława Trejnisa i Zenona Trejnisa, Agnieszki Wiercińskiej-Krużewskiej.

Dziękuję także prof. UAM dr hab. Maciejowi Walkowskiemu za ogromne wsparcie w dotarciu do niezwykle interesujących źródeł, cierpliwość oraz konsekwentnie motywujące podejście.

Autor mając świadomość, iż z konieczności kompleksowe przedstawienie wielu z poruszanych zagadnień nie pozwala na wypracowanie w pełni kompleksowego ujęcia, sądzi jednak, iż odwołania do licznych publikacji krajowych i zagranicznych umożliwią zainteresowanym tą tematyką osobom precyzyjne odszukanie niezbędnych informacji, a tym samym na poszerzenie dotychczasowego stanu wiedzy.

Rozdział I

Pojęcia cyberprzestrzeni, cyberprzestępstw i cyberterroryzmu – próba reasumpcji

1.1. Cyberprzestrzeń

W dostępnej literaturze przedmiotu terminem cyberprzestrzeni określa się, rozumiany łącznie, szereg powiązań o charakterze wirtualnym, nie fizycznym i pozamaterialnym, do których wytworzenia niezbędna pozostaje technologia i infrastruktura informatyczna i telekomunikacyjna[1]. Uwzględniając ujętą w tym przekazie myśl oraz założenia niniejszego opracowania, cyberprzestrzeń będzie rozumiana jako „całość powiązań ludzkiej działalności z udziałem ICT (*Information and Communication Technology*)"[2]. Tym samym więc pojęcie „cyberprzestrzeń" określa „sieć łączącą systemy komputerowe obejmujące jednostki centralne i ich oprogramowanie, ale także dane, sposoby i środki ich przesyłania. Cyberprzestrzeń obejmuje systemy powiązań internetowych, usługi teleinformatyczne oraz systemy zapewniające prawidłowe funkcjonowanie kraju, tj. systemy transportu, łączności, systemy infrastruktury energetycznej, wodociągowej i gazowej czy ochrony zdrowia"[3].

W Polsce w zapisach ustawowych pojęcie cyberprzestrzeni zdefiniowano stosunkowo wcześnie, bo już w 2002 w roku, opisując ją jako „przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania) zapewniające przetwarzanie oraz przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne"[4]. Tomasz R. Aleksandrowicz analizując kwestię bezpieczeństwa w cyberprzestrzeni z punktu widzenie prawa międzynarodowego, zauważa, iż to właśnie cyberprzestrzeń jest aktualnie „systemem nerwowym" każdego nowoczesnego państwa. Twierdzi też, że głównie od „sprawności i bezpieczeństwa cyberprzestrzeni zależy funkcjonowanie infrastruktury krytycznej"[5].

---

[1] Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009, s. 2.

[2] Bógdoł-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 37.

[3] Tekielska P., Czekaj Ł., *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, w: *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Górka M. (red.), Warszawa 2014, s. 163.

[4] Art. 2 ust. 1b *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (tekst jednolity: Dz.U. z 2014 poz. 1815, ze zm.).

[5] Aleksandrowicz T., *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, s. 75.

Przywołaną wyżej definicję cyberprzestrzeni uzupełnić jednak należy o systematykę jej cech dystynktywnych, gdyż to one będą w istocie punktem wyjścia do dalszych rozważań na temat zagrożenia cyberprzestrzeni przestępczością informatyczną oraz cyberterroryzmem. Wymieniając jedynie najważniejsze, przyjąć należy, iż cyberprzestrzeń charakteryzuje się:

- „niezależnością od miejsca,
- niezależnością od odległości,
- niezależnością od czasu,
- niezależnością od granic,
- względną anonimowością”[6].

Same w sobie już niejako świadczą, że cyberprzestrzeń stanowi odrębny system globalnej komunikacji społecznej – system o immanentnej strukturze, dynamicznie interaktywnej i kształtującej się w wyniku podlegania co najmniej trzem równoległym procesom:

- „integracji form przekazu i prezentacji informacji, która przyniosła ucyfrowienie tak zwanej infosfery,
- konwergencji systemów informatycznych i telekomunikacyjnych oraz mediów elektronicznych,
- integracji tzw. technosfery, która doprowadziła w rezultacie do powstania globalnej zintegrowanej platformy teleinformatycznej”[7].

Cyberprzestrzeń to zatem system powiązań, obszar komunikacji, pod pewnymi względami jednoznacznie pozytywny, czyli na przykład prowadzący do rozwoju społeczeństwa informacyjnego i obywatelskiego, gospodarki narodowej, bezpieczeństwa narodowego i międzynarodowego. Nie można jednak pominąć faktu, że rozwój cyberprzestrzeni, poddanej wyżej wymienionym procesom (o charakterze ciągłym), jednocześnie może postępować w odwrotnym, negatywnym kierunku. Marian Czyżak wskazuje na następujące skutki rozwoju cyberprzestrzeni:

- „możliwość cyberinwigilacji (obostrzonej kontroli społeczeństwa za pośrednictwem narzędzi teleinformatycznych w państwach autorytarnych i totalitarnych),
- pojawienie się cyberprzestępczości (wykorzystania cyberprzestrzeni do celów kryminalnych,

[6] Aleksandrowicz T., *op. cit.*, s. 12
[7] Typologia podana [za:] Sienkiewicz P.: *Terroryzm w cybernetycznej przestrzeni*. W: Cyberterroryzm – nowe wyzwania XXI wieku. Red. T. Jemioła, J. Kisielnicki, K. Rajchel. Warszawa, Wyższa Szkoła Informatyki, Zarządzania i Administracji, 2009, oraz: Czyżak M, *Wybrane aspekty zjawiska cyberterroryzmu*, „Telekomunikacja i techniki Informacyjne”, 1-2/2010, s. 46.

w szczególności w ramach przestępczości zorganizowanej i przestępczości o charakterze ekonomicznym),

- cyberterroryzm (wykorzystania cyberprzestrzeni w działaniach terrorystycznych)
- cyberwojny (czyli użycia cyberprzestrzeni jako czwartego, obok ziemi, morza i powietrza, wymiaru pro wadzenia działań wojennych)"[8].

1.2. Bezpieczeństwo w cyberprzestrzeni

Bezpieczeństwo rozumiane zarówno jako jedna z podstawowych potrzeb człowieka, jak i kategoria społeczna, kulturowa czy psychologiczna - ale także jako paradygmat poznawczy, jest pojęciem, które może być rozpatrywane jedynie w perspektywie interdyscyplinarnej. Nie sposób wyobrazić sobie obszaru, w którym dla życia ludzkiego pojęcie bezpieczeństwa ma dystynktywne znaczenie. Należy więc uznać, iż bezpieczeństwo jest podstawą egzystencji zarówno jednostek, jak i społeczeństw, państw i innych form organizacji społecznej – wszystkich właściwie podmiotów współczesnego świata. „Bezpieczeństwo jest definiowane jako stan bądź proces gwarantujący istnienie podmiotu oraz możliwość jego rozwoju. W rozwinięciu definicji bezpieczeń-stwo opisuje się jako stan, który daje poczucie pewności istnienia i gwarancję jego zachowania oraz szansę na doskonalenie. Jest to jedna z podstawowych potrzeb człowieka.. Odznacza się brakiem ryzyka utraty czegoś dla podmiotu szczególnie cennego. Bezpieczeństwo jest naczelną potrzebą człowieka i grup społecznych umiejscowioną niemalże w podstawie piramidy Masłowa, ale jest także podstawową potrzebą państw i systemów międzynarodowych, a jego brak wywołuje niepokój i poczucie zagrożenia"[9].

Adrian K. Siadkowski, analizując definicje bezpieczeństwa, zwrócił szczególną uwagę na relację pomiędzy bezpieczeństwem jako stanem obiektywnym oraz subiektywnie rozumianym poczuciem bezpieczeństwa. Jak pisze, „bezpieczeństwo jest złożoną strukturą składającą się z psychicznych i niepsychicznych komponentów. W pewnych sytuacjach bezpieczeństwo (element obiektywny) może nie być adekwatne do poczucia bezpieczeństwa (element subiektywny)"[10]. W przypadku zagrożeń niesymetrycznych, do których niewątpliwie należy cyberterroryzm, kwestia owego „poczucia bezpieczeństwa" jest szczególnie istotna i dostrzegalna, zaimplementowana

[8] Czyżak M, *op. cit.,* s. 48.
[9] Siadkowski A.K, *Bezpieczeństwo i ochrona w cywilnej komunikacji lotniczej na przykładzie Polski, Stanów Zjednoczonych i Izraela,* Szczytno, 2013, s. 34.
[10] Ibidem.

niejako wręcz w samą strukturę semantyczną tego pojęcia. W przypadku analizy zagrożeń dla bezpieczeństwa infrastruktury krytycznej współczesnych państw można by założyć, iż punktem wyjścia do dalszych rozważań zawsze będzie zagadnienie ogólnie rozumianego bezpieczeństwa w cyberprzestrzeni. W podrozdziale tym autor nie będzie rozróżniał kategorii zagrożeń cyberprzestępczych i cyberterrorystycznych, skupi się natomiast na samym zagrożeniu dla informacji jako zasobu chronionego i proponuje przyjąć najbardziej ogólną definicję terminu 'bezpieczeństwo cyberprzestrzeni' jako „brak ryzyka utraty danych informacyjnych w cyberprzestrzeni"[11]. W konsekwencji owo bezpieczeństwo cyberprzestrzeni należy uznać za kategorię pojęciową bardzo rozległą semantycznie, nieograniczającą się jedynie do systemu infrastruktury krytycznej, ale rozumianą jako kluczowy element stabilności bezpieczeństwa całego systemu państwowego i międzynarodowego. Nie można bowiem ograniczyć pojęcia cyberprzestrzeni do granic jednego państwa, gdyż – jak wspomniano powyżej – cyberprzestrzeń zawiera w sobie niezależność od miejsca, odległości i granic. Niemniej jednak zagrożenie dla jej bezpieczeństwa należy rozpatrywać – jeśli z punktu widzenia państwa narodowego – to również jako zagrożenie dla integralnej części bezpieczeństwa narodowego jako całości. Podejście to rozwija i analizuje wielu autorów, a swoiście syntetyczną reasumpcję przyjętych przez nich założeń przedstawia Tomasz R. Aleksandrowicz. Zgodnie z wnioskami tegoż badacza, należy uwzględnić wiele uwarunkowań bezpieczeństwa informacyjnego, a przede wszystkim to, iż:

- „informacja stanowi zasób strategiczny państwa,
- informacja i wynikające z niej wiedza oraz technologie informatyczne stają się podstawowym czynnikiem wytwórczym,
- szeroko rozumiany sektor informacyjny wytwarza znaczną część dochodu narodowego[12]
- procesy decyzyjne w innych sektorach gospodarki i życia społecznego są w znacznej mierze uzależnione od systemów przetwarzania i przesyłania informacji,
- zakłócenie prawidłowości działania systemów informacyjno-sterujących nie wymaga wysokich nakładów materialnych,

[11] Pacek B., Hoffman R., *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013, s. 85.
[12] Technologie informatyczne i komunikacyjne stanowią silny czynnik wzrostu gospodarczego. W Unii Europejskiej ten sektor generuje 25% wzrostu PKB i 40% wzrostu produktywności. Takie dane podaje Komisja Europejska w dokumencie *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia* [online], Komunikat Komisji Wspólnot Europejskich do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, Bruksela, 1 VI 2005 COM(2005) 229 końcowy, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PL:PDF [dostęp: 5 V 2018].

- rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej[13],
- technologie informatyczne stały się istotnym elementem funkcjonowania bezpieczeństwa państwa, w tym sił zbrojnych[14],
- media masowe mogą być wykorzystywane jako narzędzia skutecznego zakłócania informacyjnego, np. przez prowadzenie dezinformacji"[15].

Z powyższego zestawienia można wywnioskować, że kwestia bezpieczeństwa cyberprzestrzeni to jeden z najistotniejszych czynników warunkujących i determinujących trwałość oraz nienaruszalność systemu społecznego oraz gospodarczego współczesnego państwa. Osiągnięcie bezpieczeństwa w cyberprzestrzeni pozwala bowiem nie tylko na utrwalenie stanu aktualnego, ale też umożliwia dalszy, swobodny i nieulegający zagrożeniom rozwój społeczeństwa i gospodarki. Stan bezpieczeństwa cyberprzestrzeni, czy może - jak określają go E. i M. Nowak, „stan bezpieczeństwa informatycznego", występuje wówczas, kiedy spełnione są następujące warunki traktowane bezwzględnie łącznie:

- „nie są zagrożone strategiczne zasoby państwa,
- organy władzy podejmują decyzje na podstawie wiarygodnych, istotnych dokładnych i aktualnych informacji,
- przepływ informacji pomiędzy organami państwa jest niezakłócony,
- funkcjonowanie sieci teleinformatycznych tworzących teleinformatyczną infrastrukturę krytyczną państwa jest niezakłócone,
- państwo gwarantuje ochronę informacji niejawnych
- i danych osobowych obywateli,
- instytucje publiczne nie naruszają prawa obywateli do prywatności,
- obywatele, organizacje pozarządowe i przedstawiciele środków masowego przekazu mają dostęp do informacji publicznej"[16].

1.3. Walka informacyjna w cyberprzestrzeni

W literaturze przedmiotu nie zaproponowano, jak dotąd, uzgodnionej definicji „walki informacyjnej", a te, z którymi można się zapoznać, opierają się raczej na pojęciach kojarzonych

[13] Liedel K., *Bezpieczeństwo informacyjne państwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, Liedel K. (red.), Warszawa 2011, s. 57.
[14] Balcerowicz B., *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010, s. 219
[15] Liedel K., *ibidem, s*. 57-58.
[16] Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 103

ze sferą wojskowości, co już uwidocznia się w samym tym terminie i słowie ‘walka’, aniżeli z wykładniami ekonomicznymi czy informatycznymi. W każdej ze znanych autorowi definicji podmiotem jest informacja, która w sytuacji konfliktu informacyjnego jest zarówno obiektem ataku, jak i jego narzędziem. Jak zauważa cytowany już Tomasz R. Aleksandrowicz, konflikt informacyjny „obejmuje fizyczne niszczenie infrastruktury wykorzystywanej przez przeciwnika do działań operacyjnych”[17], natomiast Piotr Sienkiewicz i Halina Świeboda dodają, iż pomimo różnorodności będących w użyciu terminów i definicji, takich jak: „cyberwar, infowar, walka informacyjna, cyberterroryzm, informacyjni wojownicy, informacyjna dominacja, *netwar*, obrona w cyberprzestrzeni (*cyberspace defence*) czy informacyjny chaos – to tylko neologizmy, dotyczące tego samego, ale bardzo szerokiego pojęcia wojny ery informacyjnej (*information age warfare)*[18].

Zatem walka informacyjna w cyberprzestrzeni, czy może raczej „konflikt cybernetyczny”, to ten rodzaj starcia między przeciwnikami (charakterystyka stron takich konfliktów przestawiona i zanalizowana zostanie w kolejnych podrozdziałach), którego wynik uzależniony jest od działań napastniczych i obronnych podejmowanych tylko i wyłącznie za pośrednictwem sieci teleinformatycznych i technologii komputerowych. Jak podaje T.R. Aleksandrowicz, „taki konflikt może przybrać postać aktywizmu (niedestrukcyjnej działalności informacyjno-propagandowej, np. na forach internetowych, czatach, portalach społecznościowych), haktywizmu (aktywizmu i działań zakłócających funkcjonowanie określonych systemów komputerowych, np. przez blokowanie dostępu do serwerów) lub cyberterroryzmu (politycznie motywowanych ataków na komputery, sieci lub systemy informatyczne w celu zniszczenia infrastruktury i wymuszenia na rządzie lub organizacji określonego działania lub zaniechania)”[19]. Wyłania się w tym miejscu niezmiernie istotna przesłanka, że cyberprzestrzeń bezwzględnie należy uznać za nową arenę konfliktów międzypaństwowych, całkowicie odmiennych w formie, narzędziach oraz realizacji od dotychczasowych doświadczeń, które to doświadczenia – z uwagi na przyjętą militarną onomastykę – na potrzeby tego opracowania nazwać możemy konwencjonalnymi. Zagrożenie tą nową formą konfliktu niewątpliwie będzie stale rosnąć – dynamicznie i wprost proporcjonalnie do dynamiki rozwoju technologii informatycznych. Walka

[17] Aleksandrowicz T., *op. cit.*, s. 14
[18] Sienkiewicz P., Świeboda H., *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, w: *Bezpieczeństwo teleinformatyczne państwa…*, s. 80-82.
[19] Aleksandrowicz T., *op. cit.*, s. 16

informacyjna w cyberprzestrzeni jest jednym z elementów (a w każdym razie – może być) konfliktu militarnego (i to niekoniecznie międzypaństwowego). Konflikty hybrydowe, czyli wrogie działania prowadzone w warunkach pokoju, to idealny przykład wykorzystania cyberprzestrzeni do walki z przeciwnikiem. Co istotne, walka informatyczna niekoniecznie wykorzystywana jest jako uzupełnienie czy wstęp do terenowych działań militarnych – często jest ona samoistna, bez użycia broni konwencjonalnej czy oddziałów wojskowych. Cele atakowane w takim konflikcie często nie mają bezpośredniego znaczenia militarnego, ale są częścią systemu infrastruktury krytycznej[20] przeciwnika, jak na przykład sieci łączności czy przesyłowe sieci energetyczne.

1.4. Cyberprzestępczość

1.4.1. Ujęcia normatywne a niejednolitość definicyjna

Na wstępie warto zauważyć, iż w polskim systemie prawnym nie ma, jak dotąd, jasno i jednoznacznie sformułowanej definicji cyberprzestępczości. W literaturze przedmiotu istnieje ogromne zróżnicowanie co do zakresu semantycznego terminu, jakim powinno się określać grupę przestępstw z wykorzystaniem technik oraz systemów informatycznych i teleinformatycznych. Rosnąca dynamika rozwoju technik cybernetycznych i komputerowych sprawia, iż nie sposób nie zgodzić się z poglądem wyrażonym przez Andrzeja Adamskiego – i to już w roku 2000 – iż „ciągły postęp techniczny nie sprzyja trwałości formułowanych w piśmiennictwie definicji przestępczości komputerowej"[21]. Niemniej jednak uznać należy, iż w sensie najogólniejszym cyberprzestępstwa rozumiane są jako „przestępstwa niemożliwe do dokonania poza środowiskiem komputerowym", czyli są to:

- „zmiany dokonywane z użyciem komputera na oprogramowaniu i zbiorach danych,
- zamachy dokonywane na urządzeniach systemów informatycznych oraz ich kradzież,
- zamachy dokonywane za pośrednictwem systemów informatycznych,
- kradzież materiałów służących do eksploatacji systemów komputerowych,

[20] Pojęciu infrastruktury krytycznej poświęcony został osobny rozdział, z uwagi jednak na fakt, iż jest ono często używane również w rozdziale go poprzedzającym, autor uważa za pomocne krótkie zdefiniowanie tego terminu. W polskim ustawodawstwie 'infrastruktura krytyczna' definiowana jest jako systemy i powiązane ze sobą funkcjonalnie obiekty wchodzące w ich skład, w tym obiekty budowlane, urządzenia, instalacje, usługi ważne dla bezpieczeństwa państw i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje następujące systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe; zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i telekomunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. Zob. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (tekst jednolity: Dz.U. z 2013 r. poz. 1166).

[19] Adamski A., *Prawo karne komputerowe*, Warszawa 2000, s. 32.

- nieuprawnione uzyskanie dostępu do komputera (*hacking*)"[22].

Do kategorii cyberprzestępstw zalicza się także i tego rodzaju przestępstwa, do których użycie komputera oraz technik teleinformatycznych nie jest niezbędne, aczkolwiek w sposób znaczący ułatwia ich dokonanie. Będą to głównie:

- „oszustwa
- fałszerstwa oraz kradzież tożsamości,
- kradzieże informacji,
- inwigilacja,
- inne"[23].

W myśl przyjętej przez ONZ definicji cyberprzestępczości, przedstawiającej jej wąskie znaczenie, jest to „nielegalne działanie, dokonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub procesowanych przez te systemy danych". W ujęciu szerszym do cyberprzestępczości zaliczane są wszelkie nielegalne działania dotyczące urządzeń teleinformatycznych lub popełnione za ich pomocą, jak choćby „nielegalne posiadanie i rozpowszechnianie informacji przy wykorzystaniu fizycznych nośników lub Internetu"[24]. Z kolei definicja ujęta w komunikacie Komisji Europejskiej do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 2007 roku zatytułowanym *W kierunku ogólnej strategii zwalczania cyberprzestępczości* za cyberprzestępstwo uznaje działanie, które jest wymierzone przeciwko „poufności, integralności danych, sabotaż komputerowy, szpiegostwo komputerowe"[25], włączając również, na przykład, nielegalny podsłuch. Twórcy wspomnianego komunikatu klasyfikują cyberprzestępstwa jako:

- „przestępstwa przeciwko poufności, integralności i dostępności danych – do tych przestępstw zaliczamy głównie nielegalny dostęp do systemów poprzez *hacking*, podsłuch i oszukiwanie uprawnionych pracowników, szpiegostwa komputerowe, sabotaż oraz wymuszenia komputerowe (wirusy, ataki DoS, DDoS, spam),
- przestępstwa tradycyjne powiązane z komputerami, takie jak oszustwa (od klasycznych oszustw jak manipulacje fakturami lub kontami firmowymi, do manipulacji *online* – oszukańczych aukcji czy nielegalnego używania kart kredytowych). Przestępstwa obejmują

[22] Siwicki M., *Podział i definicja cyberprzestępstw*, Prok. i Pr. 2012, nr 7–8, s. 242
[23] *Ibidem, s. 243.*
[24] http://lexblog.pl/*definicja-cyberprzestepstwa/* Lexblog.pl [dostęp: 23.03.2018]
[25] Siwicki M., *op.cit*, s.243.

również komputerowe podróbki, molestowanie dzieci, aż do ataków na życie ludzkie, np. przez manipulowanie systemami energetycznymi, szpitalnymi lub kontroli ruchu powietrznego".

1.4.2. Konwencja budapeszteńska

Konwencja budapeszeńska[26] jest dokumentem strategicznym wypracowanym i przyjętym przez Radę Europy w roku 2001. Dokument ten (zwany również konwencją o cyberprzestępczości) szerzej będzie analizowany w rozdziale II, stąd w tym miejscu zostanie omówiony skrótowo. Warto rzec, że wnosi on bardzo istotne dla całego procesu zapobiegania szeroko rozumianej cyberprzestępczości zapisy normatywne definiujące czyny wywołujące zagrożenia cyberprzestrzeni. Art. 1 konwencji budapeszeńskiej stanowi, iż:

- „<<system informatyczny>> oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych;
- <<dane informatyczne>> oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny;
- <<dostawca usług>> oznacza (i) dowolny podmiot prywatny lub publiczny, który umożliwia użytkownikom jego usług komunikowanie się za pomocą systemu informatycznego, oraz (ii) dowolny inny podmiot, który przetwarza lub przechowuje dane informatyczne w imieniu takich usług komunikacyjnych lub użytkowników takich usług,
- <<dane dotyczące ruchu>> oznaczają dowolne dane informatyczne odnoszące się do komunikowania się za pomocą systemu informatycznego, wygenerowane przez system informatyczny, który utworzył część w łańcuchu komunikacyjnym, wskazujące swoje pochodzenie, przeznaczenie, ścieżkę, czas, datę, rozmiar, czas trwania lub rodzaj danej usługi"[27].

Konwencja budapeszteńska wprowadza także (po raz pierwszy w dokumentach

[26] *Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r*. (Dz.U. poz. 1514). Zob. na ten temat: D. Głowacka, *Konwencja o cyberprzestępczości – konieczność ratyfikacji, potrzeba rewizji* [online], http://www.europapraw.org/ files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf [dostęp: 13 II 2018]. Tekst konwencji: *Convention of Cybercrime* [online], Budapest, 23 XI 2001 r., European Treaty Series nr 185, http:// conventions.coe.int/Treaty/en/Treaties/Html/185.htm [dostęp: 13 II 2018].

[27] http://prawo.vagla.pl/node/1493

strategicznych dotyczących bezpieczeństwa cyberprzestrzeni) podział czynów uznawanych za cyberprzestępstwa i systematyzuje je w czterech kategoriach: przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów; przestępstwa komputerowe; przestępstwa ze względu na charakter zawartych informacji oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych[28]. Podział ten (w szczególności dwie pierwsze kategorie) autor chciałby omówić nieco szerzej, z uwagi na jego istotne znaczenie dla problematyki podjętej w niniejszej pracy.

W art. 2-5 do kategorii pierwszej konwencja zalicza:

- nielegalny dostęp – rozumiany jako umyślny i bezprawny dostęp do całości lub części systemu informatycznego. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione przez naruszenie zabezpieczeń, z zamiarem pozyskania danych informatycznych lub z innym nieuczciwym zamiarem albo w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym (art. 2);
- nielegalne przechwytywanie danych – rozumiane jako umyślne, bezprawne przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym (art. 3);
- naruszenie integralności danych – rozumiane jako umyślne, bezprawne niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych. Strona może zastrzec sobie prawo wprowadzenia wymogu, że zachowanie opisane w ustępie l musi skutkować poważną szkodą (art. 4);
- naruszenie integralności systemu – rozumiane jako umyślne, bezprawne, poważne zakłócanie funkcjonowania systemu informatycznego przez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych (art. 5);
- niewłaściwe wykorzystywanie urządzeń – rozumiane jako umyślne i bezprawne

[28] Aleksandrowicz T., *Strategie bezpieczeństwa w cyberprzestrzeni. Cyberwojny*, w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2014, s. 17.

działania polegające na produkcji, sprzedaży, pozyskiwaniu z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania:

- urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim do popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2–5;
- hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna (art. 6)[29].

W art. 7 i 8 konwencja systematyzuje należące do kategorii drugiej przestępstwa komputerowe: fałszerstwo komputerowe (art. 7) i oszustwo komputerowe (art. 8). „Tym pierwszym będzie: umyślne, bezprawne wprowadzanie i dokonywanie zmian, wykasowywanie lub usuwanie danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane w celach zgodnych z prawem jako autentyczne, bez względu na to, czy są one zrozumiałe i czy można je bezpośrednio odczytać. Strona może wprowadzić wymóg, że odpowiedzialność karna dotyczy działania w zamiarze oszustwa lub w podobnym nieuczciwym zamiarze. Natomiast za oszustwo komputerowe konwencja budapeszteńska uznaje umyślne, bezprawne spowodowanie utraty majątku przez inną osobę przez: wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych bądź każdą ingerencję w funkcjonowanie systemu komputerowego z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby”[30].

Kategoria trzecia obejmuje przestępstwa „kontentowe” (czyli dotyczące zawartości) i obejmuje, między innymi: dziecięcą pornografię, dostarczanie instrukcji przestępczych, oferty popełniania przestępstw. Do tej kategorii zaliczamy także molestowanie i lobbing poprzez sieć, rozpowszechnianie fałszywych informacji (np. czarny PR, schematy *pump-and-dump*) oraz internetowy hazard. I wreszcie, w kategorii czwartej, zamieszczono przestępstwa powiązane z naruszeniem prawa autorskiego i praw pokrewnych, takie jak nieautoryzowane kopiowanie i rozpowszechnianie programów komputerowych, nieautoryzowane użycie baz danych[31].

---

[29] *Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r*. (Dz.U. poz. 1514). Zob. na ten temat: D. Głowacka, *Konwencja o cyberprzestępczości – konieczność ratyfikacji, potrzeba rewizji* [online], http://www.europapraw.org/ files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf [dostęp: 13 II 2018]. Tekst konwencji: *Convention of Cybercrime* [online], Budapest, 23 XI 2001 r., European Treaty Series nr 185, http:// conventions.coe.int/Treaty/en/Treaties/Html/185.htm [dostęp: 13 II 2018].

[30] Aleksandrowicz T., *op. cit.,* s. 18

[31] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, *W kierunku ogólnej strategii zwalczania cyberprzestępczości*, KOM (2007), s. 267

Dyrektywa 2013/40/EU stanowiąca o atakach na systemy informatyczne[32], również analizowana w rozdziale II, stanowi istotny z punktu widzenia krajów członkowskich EU dokument programowy, z uwagi na fakt, iż obliguje je do tworzenie prawa krajowego umożliwiającego zwalczanie zagrożeń dla cyberprzestrzeni. Dyrektywa ta (będąca dokumentem prawotwórczym, nie zaś o charakterze deklaratywnym) zaleca penalizację takich czynów, jak:

- „niezgodnego z prawem dostępu do systemów informatycznych – rozumianego jako umyślne i bezprawne uzyskiwanie dostępu do całości lub jakiejkolwiek części systemu informatycznego, gdy zostało ono popełnione z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 3),
- niezgodnej z prawem ingerencji w systemy – rozumianego jako umyślne i bezprawne uzyskiwanie dostępu do całości lub jakiejkolwiek części systemu informatycznego, gdy to przestępstwo zostało popełnione z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 4),
- niezgodnej z prawem ingerencji w dane – rozumianej jako umyślne i bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 5),
- niezgodnego z prawem przechwytywania – rozumianego jako umyślne i bezprawne przechwytywanie za pomocą środków technicznych niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego, w tym emisji elektromagnetycznych z systemu informatycznego zawierającego takie dane komputerowe, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 6)”[33].

1.4.3. Przestępstwa przeciw bezpieczeństwu cyberprzestrzeni w polskim kodeksie karnym.

W polskim systemie prawnym o przestępstwach przeciwko bezpieczeństwu cyberprzestrzeni traktują zapisy *Ustawy z dnia 6 czerwca 1997 roku – Kodeks karny* (tekst jednolity: *Dz.U. z 2016 r. poz. 1137*). Stosowne regulacje zawarto w rozdziale XXXIII Ustawy, klasyfikując je jako „Przestępstwa przeciwko ochronie informacji” – konkretnie są to przepisy art. 267, 268, 268a, 269, 269a i 269b. Zapisy przytoczone zostaną w pełnym brzmieniu:

[32] *Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW* (Dz.Urz. UE L 218 z 14 VIII 2013 r. poz. 8).
[33] Synteza zapisów dyrektywy podana za: Aleksandrowicz T., *op. cit.,* s. 18-19

Art. 267

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1–4 następuje na wniosek pokrzywdzonego.

Art. 268

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268a

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Art. 269
§ 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269a
Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269b
§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy[34].

1.4.4. Techniki cyberprzestępcze – próba systematyki

W praktyce można wyróżnić do dwudziestu podstawowych narzędzi wykorzystywanych do przeprowadzania różnego rodzaju ataków na systemy informatyczne:

- wirusy, robaki i bakterie (oprogramowanie złośliwe – *malware*) – programy rozprzestrzeniające się w systemie informatycznym i zmieniające sposób jego działania lub reprodukujące się i zajmujące pamięć procesora, przestrzeń dyskową i inne zasoby, a w rezultacie – blokujące dostęp do danych,
- bomby logiczne – aktywizujące nowe funkcje elementów logicznych komputera i prowadzące do zniszczenia sprzętu i oprogramowania,
- konie trojańskie – programy umożliwiające podejmowanie w systemie komputerowym działań bez wiedzy i zgody jego prawowitego użytkownika, np. usuwanie plików, formatowanie dysków, kopiowanie danych itp.,
- próbkowanie – dostęp do komputera przez analizę jego charakterystyki,
- uwierzytelnianie – podszywanie się pod osobę uprawnioną do dostępu do systemu,
- ominięcie – ominięcie procesu zabezpieczającego system,
- czytanie – nieuprawniony dostęp do informacji,
- kopiowanie – nieuprawnione kopiowanie plików,
- kradzież – przejęcie zasobów systemu przez osobę nieuprawnioną bez pozostawiania kopii,
- modyfikacja – zmiana zawartości danych lub charakterystyki obiektu ataku,
- usunięcie – zniszczenie obiektu ataku,
- złośliwe podzespoły – umieszczanie w komputerach chipów zawierających programy umożliwiające nieuprawniony dostęp lub tworzące wady konstrukcyjne,
- tylne drzwi – pozostawienie przez twórców oprogramowania „furtki" nieznanej użytkownikowi; za pomocą tylnych drzwi można uzyskać nieuprawniony dostęp do systemu,

[34] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (tekst jednolity: Dz.U. z 2016 r. poz. 1137).*

- maskarada – udawanie przez atakującego jednego z użytkowników systemu przez na przykład modyfikację pakietów w trakcie połączenia,
- przechwycenie transmisji – uzyskanie dostępu do treści przesyłanych między komputerami,
- podsłuchiwanie – śledzenie ruchu w sieci,
- receptor van Ecka – oglądanie przez napastnika na oddzielnym monitorze repliki obrazów pojawiających się na monitorze użytkownika atakowanego komputera,
- DDoS – zablokowanie dostępu do strony internetowej przez przesyłanie pod jej adresem olbrzymiego pakietu danych z różnych źródeł, co powoduje zawieszenie się serwera,
- *e-mail bombing* – przesyłanie na skrzynkę pocztową atakowanego użytkownika wielkiej ilości danych, co powoduje jej przepełnienie,
- *electromagnetic pulse* – czyli emisja promieniowania elektromagnetycznego, które niszczy urządzenia elektroniczne i dane[35].

1.5. Terroryzm

1.5.1. Terroryzm – rys historyczny

Termin „terror" wywodzi się z języka łacińskiego i oznacza „stosowanie przemocy, gwałtu, okrucieństwa w celu zastraszenia kogoś"[36], choć jego źródłosłów pochodzi od gr. *tero* – drżeć, bać się[37]. Jeżeli chodzi natomiast o termin „terroryzm", to pomimo całkowitej zgodności co do uznania terroryzmu za jeden z najważniejszych problemów międzynarodowych, jak dotąd na forum międzynarodowym nie opracowano ani jednolitej definicji tego zagrożenia ani też prawnego określenia tego pojęcia. I choć w niniejszym opracowaniu nie przewidziano głębszej analizy zjawiska terroryzmu, ani też bliższego przedstawienia jego – niewątpliwie bardzo istotnej – roli w kształtowaniu dziejów ludzkości, wskazanie kilku najistotniejszych (z funkcjonalnego punktu widzenia) cech wydaje się jednak nie tyleż uzasadnione, co wręcz niezbędne.

---

[35] Wykaz technik i narzędzi cyberprzestępczych sporządzono na podstawie: E. Lichocki, *Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych RP*, Wydział Bezpieczeństwa Narodowego Akademii Obrony Narodowej, Warszawa 2009, s. 62–63 (rozprawa doktorska), patrz też: Aleksandrowicz T., *op. cit.,* s. 14-15.

[36] *Słownik języka polskiego*, PWN, Warszawa 2002

[37] *Ibidem.*

Choć terminem ’terroryzm’ społeczeństwo Europy posługuje się już prawie 250 lat, to znaczenie tego zjawiska zmieniało się znacząco wraz z upływem czasu i zmienia się w dalszym ciągu. W literaturze przedmiotu trudno odnaleźć jednoznacznego zdefiniowania, czym dokładnie jest terroryzm, wiadomo za to, niejako instynktownie, czym miałby on być i czemu służyć. Terroryzm – a w następstwie czasowym także i cyberterroryzm – sam w sobie nie różni się bowiem aż tak bardzo od innych form przemocy skierowanej przeciwko przypadkowym celom czy też od niekonwencjonalnych działań wojennych. Co zatem wiadomo? Iż jest to zjawisko jednoznacznie negatywne i bezwzględnie podlegające zwalczaniu. Warto jednak w tym miejscu nadmienić, gdy pojęcie terroryzmu po raz pierwszy wyłoniło się pod koniec XIX wieku w czasach Wielkiej Rewolucji Francuskiej i było wówczas kojarzone z początkami demokracji i nie było naznaczone owymi pejoratywnymi konotacjami, które wiążą się z nimi obecnie. Było raczej postrzegane jako świt nowej ery w stosunkach społecznych, narodziny demokracji, kres panowania monarchii i zasadniczo jako ustanowienie rządów ludu. Prowadzone przez terrorystów (czy też anarchistów, jak zwano ich w carskiej Rosji) działania były wówczas niemal wyłącznie kojarzone ze zwalczaniem ustrojów konkretnych krajów w przeciwieństwie do dzisiejszych czasów, gdy terroryzm jest postrzegany jako zjawisko międzypaństwowe lub jako akty przemocy podejmowane przez jednostki lub grupy ludzi. Owe pozytywne konotacje terroryzmu skończyły się jednak już w lipcu 1794 roku, gdy Maximilien de Robespierre, przywódca rewolucji francuskiej, przedstawił listę zdrajców, którzy według niego podważyli idee rewolucji. Tym samym terroryzm objawił się nagle czymś jako coś, co nie było pozytywne ani dobre, lecz ewidentnie negatywne, a przy tym stanowiło nadużycie i z pewnością wiązało się z przemocą, często wymierzoną w zwykłych ludzi. W ten oto sposób terroryzm począł jawić się zarówno jako koncepcja i środek rewolucji oraz jako sposób osiągnięcia fundamentalnej zmiany politycznej od połowy do końca XIX wieku. Jest też kojarzony z dwoma konkretnymi ruchami, z których każdy stanowił w istocie spuściznę po Wielkiej Rewolucji Francuskiej. Mowa tu zarówno o organizacjach rewolucyjnych o charakterze antymonarchistycznym, których celem była próba obalenia dynastii rządzących w Europie i ustanowienie na ich miejscu demokracji, jak i o ruchu anarchistycznym. Stan ten utrzymywał się przez około 30-40 lat i dotyczył głównie Cesarstwa Rosyjskiego będąc – jak się później okazało – skutecznym sposobem na destrukcję samodzierżawia jako skrajnie absolutystycznego systemu władzy. Od czasów Aleksandra III,

poprzez zabójstwo Piotra Stołypina aż do tragicznego końca Mikołaja II i zagłady całej dynastii Romanowów, terroryzm był stałym elementem systemu społeczno-politycznego Rosji.

W wieku XX, a w szczególności w jego pierwszej połowie, terroryzm staje się coraz bardziej związany już nie tylko z ruchami rewolucyjnymi czy anarchistycznymi, które dążą do fundamentalnych zmian politycznych, lecz również – co istotne – z ruchem separatystycznym i organizacjami irredentystycznymi. Innymi słowy, z osobami lub grupami starającymi się wykroić sobie historyczną, językową lub kulturową ojczyznę dla siebie. Wtedy właśnie u progu I wojny światowej zrodziła się zdolność terroryzmu, aby znacząco wpływać na zdarzenia o charakterze globalnym. Przykładem może być zabójstwo arcyksięcia Franciszka Ferdynanda, następcy tronu z rodu Habsburgów, w czerwcu 1914 roku przez Gawriło Principa, rewolucjonisty należącego dokładnie do jednego z tych irredentystycznych, nacjonalistycznych organizacji separatystycznych, które w ten sposób starały się wyrwać Bośnię z imperium Habsburgów i ustanowić ją niezależnym i suwerennym państwem. Terroryzm więc przekształcił się wówczas ze zjawiska kojarzonego z rządami rewolucji francuskiej w zjawisko stanowczo wywodzące się z ludu, czyli – jak powiedzieliby Rosjanie – ideę narodnikowską.

Ciekawe jest to, że w latach 30. XX wieku zjawisko to znowu przechyliło się w kierunku swych rządowych konotacji, a to z racji, gdy terroryzm bardzo mocno zaczął być kojarzony z nadużyciem władzy i represjami wobec ludności wymierzonymi przez nazistowskie Niemcy i stalinowską Rosję. Kolejny więc raz terroryzm objawia się jako ściśle związany z rządami, a tendencja ta, choć cykliczna, będzie odtąd stale widoczna.

W latach pięćdziesiątych, po II wojnie światowej, terroryzm na nowo zwróci się ku podmiotom niepaństwowym i zacznie być kojarzony z przeciwnikami kolonializmu, nacjonalistami, ludami krajów rozwijających się, dążącymi do zrzucenia kajdan imperializmu i uwolnienia się od europejskich rządów. Znowu zatem stanie się zjawiskiem bardzo nacjonalistycznym, ale także nadal irredentystycznym dążącym do odtworzenia lub przywrócenia ojczyzny. W latach rewolucji obyczajowej w krajach Zachodu, czyli 60-70 XX wielu, nadal w dużym stopniu terroryzm skupi się na pozapaństwowych podmiotach i przestanie być kojarzony z rządami, choć z drugiej strony zacznie mówić się o dwóch oddzielnych grupach terrorystów lub dwóch grupach rewolucjonistów. Jedną była radykalna lewica lub elementy marksistowskie, a drugą grupy separatystyczne, zwłaszcza w takich miejscach, jak Palestyna, Irlandia, Hiszpania i wielu innych.

Lata 80 ubiegłego wieku to powrót terroryzmu państwowego. Mimo że wówczas termin „imperium zła" jeszcze nie powstał, to terroryzm postrzegano jako zjawisko, którym sterowała Moskwa, a które w życie wdrażał Związek Radziecki ze swoimi towarzyszami z Układu Warszawskiego lub bloku wschodniego w ramach niewypowiedzianej wojny antyimperialistycznej przeciwko Stanom Zjednoczonym i Zachodowi. Stało się to pewnego rodzaju dominującą interpretacją, że wszystkie ugrupowania terrorystyczne były organizowane w ramach jednego powszechnego spisku wywodzącego się ze Związku Radzieckiego. Po upadku ZSSR i rozpadzie bloku wschodniego terroryzm postrzegany był międzypaństwowo jako rodzaj zastępczych działań wojennych, kierowanych przez państwo narodowe o ustalonej pozycji przeciwko potężniejszym mocarstwom lub ich wrogom. Zaczął być kojarzony, na przykład, z reżimem pułkownika Kadafiego w Libii czy Saddama Husseina w Iraku, i wydaje się to właśnie taka forma działań wojennych, w której państwa sprawują kontrolę nad terrorystami. Był to swoisty powrót do dawnej odmiany terroryzmu, której ważnym motywem stał się imperatyw religijny, a zatem przemoc była uzasadniona lub usankcjonowana na bazie zasad teologicznych. Taka postać terroryzmu stała się wówczas bardzo powszechna i pozostaje aktualna do dziś, a 11 września 2001 roku jedynie ugruntował ten pogląd.

Początek XXI wieku można nazwać czasem narodzin cyberterroryzmu. Mimo że oczywiście fundamentalne podstawy terroryzmu pozostały zawsze nadzwyczaj spójne i niezmienne przez dziesięciolecia, to właśnie przedrostek „cyber" jest świadectwem zupełnie nowej epoki. Epoki, w której to postęp technologiczny zdecydował o zmianie sposobów ataku i wzroście poziomu zagrożenia.

1.5.2. Przegląd wybranych definicji terroryzmu

Brak uzgodnionej definicji semantycznej tego zjawiska sprawia, iż również klasyfikacja prawna nie może być ani jednolita, ani jednoznaczna, co dowodzi fakt, że jak dotąd w literaturze przedmiotu występuje około 600 definicji terroryzmu. Warto z pewnością dokonać pewnego ich przeglądu, zaczynając od definicji US Federal Bureau of Investigation (FBI), która przyjmuje, że za terroryzm uznaje się „bezprawne użycie siły lub przemocy wobec osób lub mienia, w celu zastraszenia lub wywarcia przymusu na rząd, ludność cywilną albo część wyżej wymienionych, co zmierza do promocji celów politycznych lub społecznych"[38]. Z kolei US National

[38] Hoffman B., *Oblicza terroryzmu*, Warszawa 2001, s. 27.

Infrastructure Protection Centre uważa natomiast, że terroryzm to „[…] bezprawne użycie – lub groźba użycia – siły czy przemocy wobec osoby lub mienia, by wymuszać lub zastraszać rządy czy społeczeństwa, często dla osiągnięcia celów politycznych, religijnych lub ideologicznych”[39]. Definicję terroryzmu zaproponowała także Komisja Europejska, według której terroryzmem są „wszelkie celowe akty popełnione przez pojedyncze osoby lub organizacje przeciw jednemu, lub kilku państwom, ich instytucjom lub ludności, w celu zastraszania oraz poważnego osłabienia lub zniszczenia struktury politycznej, gospodarczej i społecznej kraju”[40].

Zgodnie z definicję Zgromadzenia Parlamentarnego Rady Europy aktem terrorystycznym jest „każdy czyn popełniony przez osobę lub grupę osób z udziałem przemocy lub groźby jej użycia przeciwko państwu, jego instytucjom, jego ludności w ogólności lub konkretnym jednostkom, motywowanym przez separatystyczne aspiracje, ekstremistyczne koncepcje ideologiczne, fanatyzm lub irracjonalne i subiektywne czynniki, zorientowany na stworzenie klimatu terroru wśród osób publicznych, określonych jednostek lub grup w społeczeństwie bądź w całym społeczeństwie”[41].

Brak ogólnie akceptowanej definicji terroryzmu jest dostrzegany także wśród polskich badaczy i znawców zagadnienia już od przeszło dwóch dekad. Jarosław Tomasiewicz proponował, aby terroryzmem nazywać systematycznym posługiwaniem się aktami terroru indywidualnego dla osiągnięcia celu politycznego[42]. Podobne stanowisko zajął Krzysztof Karolczak, który zjawisko terroryzmu uznaje za „politycznie umotywowane działanie, które przy użyciu dowolnych metod zastraszających, ma doprowadzić do oczekiwanych zachowań obiektu, wobec którego jest zastosowana”[43], jednak odmiennie już zjawisko terroryzmu ujmuje Marek Madeja, mówiąc, iż terroryzm jest „służącą realizacji określonego programu politycznego przemocą lub groźbą jej użycia ze strony podmiotów niepaństwowych, która ma wzbudzić strach w grupie szerszej niż bezpośrednio zaatakowani i w ten sposób nakłonić rządy państw do ustępstwa lub doprowadzić do zniszczenia dotychczasowego porządku publicznego”[44]. Przytoczone definicje, bardzo skrótowe i ogólne, nieco bardziej szczegółowo rozwijają Tomasz Białek i Bartosz Bolechów. T. Białek za terroryzm uznaje „wywieranie wpływu politycznego

[39] Ibidem, s. 27.
[40] Jaskiernia A., *Uwarunkowania skuteczności zwalczania terroryzmu w świetle prac Rady Europy,* [w:]. Chodura I., (red.), *Jednostka i społeczeństwo wobec zagrożenia terroryzmem,* „Biuletyn Informacji Rady Europy” 2002, nr 1, s. 81.
[41] *Ibidem.*
[42] Tomasiewicz J., *Terroryzm na tle przemocy politycznej*, Katowice 2000, s. 12.
[43] Jaroszyński K., *Koncepcja współczesnych działań antyterrorystycznych*, [w:] „Zeszyty Naukowe AON” 2003, s. 32.
[44] Madej M., *Międzynarodowy terroryzm polityczny*, Warszawa 2001, s. 7.

przez bezprawne stosowanie siły – przymusu lub przemocy, związane z łamaniem elementarnych norm społecznych i ustalonych w danym kręgu reguł walki politycznej, oparte na rozmyślnym zastraszeniu i manipulowaniu; osiąganie celów politycznych poprzez stwarzanie aktami przemocy atmosfery zagrożenia i utrudnianie funkcjonowania wrogiego układu społecznego oraz wymuszanie decyzji, a także działań przeciwnika przez drastyczną taktykę faktów dokonanych lub szantażu siłowego"[45]. Natomiast Bartosz Bolechów prezentuje pogląd, iż „terroryzm jest formą przemocy politycznej, polegającej na stosowaniu morderstw lub zniszczeń (albo grożeniem zastosowania takich środków) w celu wywołania szoku i ekstremalnego zastraszenia jednostek, grup społecznych lub rządów, czego efektem mają być wymuszenia pożądanych ustępstw politycznych, sprowokowanie nieprzemyślanych działań lub/i zademonstrowanie nagłośnienie własnych politycznych przekonań"[46].

Odmienne, i to znacząco w stosunku do większości badaczy, zdanie prezentuje Krzysztof Liedel, twierdząc, że terroryzm to „metoda działania, która posłużyć może realizacji dowolnego celu politycznego. […] Terroryzm nie jest samodzielnym, autonomicznym zjawiskiem, a jedynie metodą służącą realizacji różnorodnych celów"[47]. Z kolei Adam Pawłowski zauważył (warto zaznaczyć, iż mowa tu o definicji powstałej już pod koniec lat 70, XX wieku), że terroryzm to „planowana taktyka działania politycznego zaangażowanych osób, polegająca stosowaniu spektakularnych środków fizycznych przeciwko osobistym i rzeczowym prawom drugich osób, w celu zwrócenia na siebie i swoje idee uwagi publicznej bądź w zamiarze wywołania takiej grozy, aby osoby trzecie poczuły się zmuszone do zachowania się odpowiadającego terrorystom"[48]. Zgodnie natomiast z definicją zaproponowaną przez Tadeusza Hanuska (w tych samych latach co definicja A. Pawłowskiego), „terroryzm jest to planowana, zorganizowana i zazwyczaj uzasadniona ideologicznie działalność osób lub grup mająca na celu wymuszenie od władz państwowych, społeczeństwa lub poszczególnych osób określonych świadczeń, zachowań lub postaw, a realizowana w przestępczych formach obliczonych na wywołanie szerokiego i maksymalnie zastraszonego rozgłosu w opinii publicznej"[49].

[45] Białek T., *Terroryzm - manipulacja strachem*, Warszawa 2005 s. 151
[46] Bolechów B., *Terroryzm w świecie podwubiegunowym,* Toruń 2002, s. 35.
[47] Liedel K., *Dbałość o bezpieczeństwo narodowe Polski w kontekście zagrożenia terrorystycznego,* http://www.terroryzm.com/articles.php?id=220, [dostęp: 21.04.2018]
[48] Pawłowski A., *Terroryzm polityczny w Europie w XIX i XX wieku*, Zielona Góra 1980, s. 9.
[49] T. Hanusek, *W sprawie pojęcia współczesnego terroryzmu*, [w:] „Problemy Kryminalistyki" 1980 nr 143, s. 33.

Zdaniem autora bardzo istotna dla definiowania współczesnego terroryzmu jest interferencyjna koncepcja terroryzmu zaproponowana przez Sebastiana Wojciechowskiego w pracy *Terroryzm na początku XXI wieku. Pojęcie, istota i przyczyny zjawiska*[50]. W modelu interferencyjnym przewiduje się bowiem, że terroryzm jest systemem obejmującym różne elementy, na przykład, różne jego części (m.in. organizacje terrorystyczne), tak zwane otoczenie czy zachodzące między nimi relacje. Ta autorska koncepcja zakłada między innymi:

a) wielość i różnorodność interakcji zachodzących pomiędzy terroryzmem wewnętrznym i zewnętrznym […];
b) interdyscyplinarność terroryzmu oznaczającą, iż zjawisko to powinno być analizowane wieloaspektowo nie tylko przez pryzmat: polityki, historii, etniczności czy religii, lecz także na przykład z uwzględnieniem płaszczyzny socjologicznej, psychologicznej, ekonomicznej, kulturowej itp.;
c) dualizm przyczynowo skutkowy terroryzmu rozumiany jako wzajemne „uzupełnianie się" sfery przyczyn i skutków […];
d) dyfuzję terroryzmu […][51].

Syntetyczna analiza dotychczasowego stanu wiedzy na temat charakterystyki terroryzmu, pomimo zaobserwowanej różnorodności definicyjnej, pozwala wyodrębnić kilka jego cech dystynktywnych. Syntetyczna analiza dotychczasowego stanu wiedzy na temat charakterystyki terroryzmu pozwala wyodrębnić kilka jego cech dystynktywnych. Terroryzm jest zawsze:

- nacechowany politycznie zarówno poprzez cele, jak i motywacje;
- zaplanowany i realizowany tak, by oddziaływać psychologiczne;
- wykorzystywany przez organizacje o rozbudowanej, hierarchicznej strukturze, w tym państwa, ugrupowania irredentystyczne, grupy motywowane religijnie i ideologicznie;
- wykonywany z użyciem przemocy lub poprzez zagrożenie jej zastosowaniem.

Celem terroryzmu jest więc każdorazowo wzbudzenie strachu nie tylko wśród bezpośrednich ofiar ataku, ale też – a wręcz przede wszystkim – wśród obserwatorów[52]. Z uwagi na to współczesne formy terroryzmu są trwale związane z masowym przekazem

[50] Wojciechowski S., *Terroryzm na początku XXI wieku. Pojęcie, istota i przyczyny zjawiska*, Poznań 2013.
[51] *Ibidem,* s.12
[52] Por. Marian Filar: *Terroryzm – problemy definicyjne oraz regulacje prawne w polskim prawie karnym w świetle prawa międzynarodowego i porównawczego* [w:] terroryzm. Materiały z sesji naukowej, Toruń 2002, s. 17.

informacji – udział mediów to dla terrorystów gwarancja osiągnięcia założonych celów, pozwala on bowiem nie tylko rozpowszechnić przekaz będący motywacją ataku, ale też – jak napisał Marian Filar – „zdobyć dominację i kontrolę nad obserwatorami aktu terrorystycznego”[53]. Terroryzm – również za pośrednictwem mediów – zawsze zmierza do osiągnięcia:

- „celu pierwotnego (głównego), którym jest zmuszenie do pożądanych – z punktu widzenia terroryzmu – zachowań rządu, przedstawicieli władzy lub określonej populacji: grupy społecznej, klasy, partii albo jednostki;
- celu instrumentalnego (ubocznego, pośredniego) stanowiącego techniczny środek realizacji celu głównego (cel ten osiągany jest poprzez różne sposoby atakowania dóbr pozostających pod ochroną prawa)”[54].

Jak zauważył Jarosław Gryz, zjawisko kontestacji społecznej, która prowadzi do coraz większej radykalizacji postaw politycznych, a w jej efekcie do terroryzmu, staje się coraz powszechniejsze i jest to zjawisko o charakterze ponadnarodowym. „W sposób symboliczny wiek ten zainicjował 11 września 2001 roku, kiedy to dokonano masowych w swojej skali ataków terrorystycznych w Stanach Zjednoczonych. Cechą charakterystyczną tych zamachów było transglobalne przeniesienie konfliktów występujących w odmiennych kulturach oraz uwarunkowaniach społecznych. W rezultacie ukazany został nowy paradygmat powszechnego terroryzmu międzynarodowego, którego źródła, jak i formy mają niemal nieograniczoną postać. Jego cechą wspólną z poprzednim pozostaje przemoc traktowana jako narzędzie wywierania wpływu politycznego”[55].

1.5.3. Terroryzm państwowy – wsparcie państw dla organizacji terrorystycznych w oparciu o wybrane przykłady

Terroryzm jest powszechnie potępianym działaniem, które jest zwalczane zarówno w wymiarze krajowym, jak i międzynarodowym. Pomimo jego ogromnej szkodliwości i trudnych do przewidzenia skutków wciąż istnieje wiele państw, które w sposób ukryty wspierają terrorystów, zapewniając im tym samym możliwość funkcjonowania i przetrwania. Działania

[53] *Ibidem.*
[54] Liedel K., Piasecka P., *Ochrona Obywateli i instytucji publicznych przed atakami terroryzmu i przemocy,* Warszawa 2004, s. 5.
55 Gryz J., *Terroryzm międzynarodowy jako zjawisko społeczne w początkach XXI wieku*, “Bezpieczeństwo Narodowe” , Zeszyty Naukowe AON nr 1(102) 2016, s. 5.

terrorystyczne wymagają znacznych nakładów kapitału, który przeznaczany jest na szkolenia terrorystów, ich podróże, tworzenie kryjówek, działalność wywiadowczą, zakup broni i inne elementy towarzyszące ich egzystencji. Lista państw wspierających terroryzm tworzona jest przez amerykański Departament Stanu. Jej ostatnia aktualizacja miała miejsce w listopadzie 2017 roku. Za umieszczanie państw na wspomnianej liście odpowiada Sekretarz Stanu USA[56]. Bada on przypadki krajów, które wielokrotnie wspierały akty terroryzmu międzynarodowego, a swoim postępowaniem naruszyły takie regulacje prawne, jak:

- Art. 6(j) ustawy o zarządzaniu eksportem;
- Art. 40 ustawy o kontroli eksportu broni;
- Art. 620A ustawy o pomocy zagranicznej[57].

Spełnienie wszystkich wymienionych przesłanek sprawia, że państwo nie tylko zostaje wpisane na listę o publicznym charakterze, do której dostęp mają inne państwa, media, organizacje międzynarodowe, inwestorzy itp., ale także może zostać poddane sankcjom. Stany Zjednoczone stosują cztery podstawowe rodzaje sankcji wobec państw, które są zaangażowane we wsparcie terrorystów. Po pierwsze, Stany Zjednoczone ograniczają pomoc udzielaną takim podmiotom, co w wielu przypadkach jest niezwykle skutecznym i odczuwalnym bodźcem (zwłaszcza jeżeli mowa o ograniczeniu wsparcia finansowego lub też militarnego). Drugą z sankcji stanowi zakaz eksportu oraz sprzedaży broni. Działanie to ma uniemożliwić jej rozpowszechnianie oraz przekazywanie terrorystom. Należy jednak podkreślić, że terroryści posiadają różnorodne źródła, z których pozyskują broń. Wiele z elementów wyposażenia militarnego pochodzi z tak zwanego czarnego rynku, gdzie broń oraz amunicja są pozyskiwane i sprzedawane w sposób nielegalny. Wśród sankcji występują również kontrole wywozu produktów podwójnego zastosowania, a także różnego rodzaju ograniczenia itp.[58]. W roku 2018 na liście państw wspierających terroryzm znajdowały się cztery państwa. Ich wyszczególnienie wraz z datą wpisania na listę zostało zamieszczone w tabeli (tabela 1).

[56] *State Sponsors of Terroris*, https://www.state.gov/j/ct/list/c14151.htm, [dostęp: 16.11.2018 r.]
[57] *Ibidem*, [dostęp: 16.11.2018 r.]
[58] *Ibidem*, [dostęp: 16.11.2018 r.]

Tabela 1. **Państwa wspierające terroryzm wpisane na listę Departamentu Stanu USA**

Państwo	Data wpisania na listę
Korea Północna	20 listopad 2017
Iran	19 styczeń 1984
Sudan	12 sierpnia 1993
Syria	29 grudnia 1979

Źródło: opracowanie własne na podstawie: State Sponsors of Terroris, https://www.state.gov/j/ct/list/c14151.htm, [dostęp: 16.11.2018].

Jednym z państw, które zostało uznane za wspierające terroryzm, jest Korea Północna. Sekretarz Stanu uznał, że rząd tego państwa wielokrotnie wspierał akty międzynarodowego terroryzmu. Wnioskował o to, ponieważ Korea Północna przyczyniała się do zabójstw dokonywanych na obcym terytorium. Dodatkowo Korea Północna prowadzi rozległe badania nad rozwojem rakiet jądrowych oraz batalistycznych, a sam Kim Dzong Un jest zagrożeniem dla amerykańskich miast, terytoriów oraz sojuszników. Poprzednio Korea Północna została wpisana na listę podmiotów sponsorujących terroryzm w 1988 roku. Był to efekt uczestnictwa w ostrzelaniu samolotu pasażerskiego Korean Airlines w 1987 roku[59]. Państwo znajdowało się na liście aż do 2008 roku, wówczas to Sekretarz Stanu USA uznał, że Korea Północna spełnia wszelkie wymogi, które są niezbędne, aby wykreślić ją z listy. Po tym zdarzeniu Korea Północna nie zaprzestała swojej szkodliwej praktyki i w 2017 roku ponownie znalazła się na opisywanej liście. Wynikało to ze wsparcia dla aktów międzynarodowego terroryzmu, ale także z nieustannego naruszania rezolucji Rady Bezpieczeństwa ONZ. Przykładowo Korea Północna wciąż udzielała schronienia dla czterech japońskich członków Czerwonej Armii uczestniczących w porwaniu samolotu Japan Airlines w 1970 roku, a których wydania żąda Japonia. Należy więc powiedzieć, że nie tylko ułatwia organizację samych ataków terrorystycznych, ale w wyraźny sposób narusza postanowienia obowiązujących aktów prawa międzynarodowego[60].

Kolejnym państwem, którego działania przyczyniają się do rozpowszechniania działalności terrorystycznej na całym świecie, jest Iran. Pomimo tego, że państwo zostało oficjalnie uznane za podmiot wspierający terrorystów, nie zaprzestało swojej szkodliwej

[59] US. Department of State, *Country Reports on Terrorism 2017*, https://www.state.gov/j/ct/rls/crt/index.htm [dostęp: 16.11.2018 r.]
[60] US. Department of State, Country Reports on Terrorism 2017, https://www.state.gov/j/ct/rls/crt/index.htm[dostęp: 16.11.2018 r.].

działalności[61]. Według danych z 2017 roku, Iran kontynuuje udzielanie wsparcia dla takich organizacji terrorystycznych jak:

- libański Hezbollah;
- palestyńskie grupy terrorystyczne w Gazie;
- grupy terrorystyczne w Syrii;
- grupy terrorystyczne w Iraku;
- inne ugrupowania terrorystyczne, które funkcjonują na terenie Bliskiego Wschodu[62].

Iran wspiera działania terrorystyczne na różne sposoby. Jednym z przykładów jest wykorzystywanie Korpusu Islamskiej Siły Rewolucji (QGW-QF), aby zapewnić wsparcie organizacjom terrorystycznym, ochronę przed podobnymi tajnymi operacjami i przyczynić się do tworzenia klimatu niestabilności na Bliskim Wschodzie. Iran potwierdził zaangażowanie IRGC-QF w oba konflikty w Iraku i Syrii. Dodatkowo IRGC-QF to podstawowe narzędzie Iranu, które wykorzystywane jest w celu wsparcia terrorystów działających za granicami państwa. Ugrupowanie to można przyrównać do podmiotu niepaństwowego zaangażowanego w wojnę hybrydową.

W 2017 roku Iran wspierał różne irackie grupy terrorystyczne Shia, w tym Kata'ib Hezbollah. Umacniał również reżim Assada w Syrii. Iran postrzega bowiem Assada jako kluczowego sojusznika, a Syrię oraz Irak jako strategiczne szlaki dostarczania broni dla libańskiego Hezbollahu, głównego sojusznika Iranu w postaci grupy terrorystycznej. Od końca konfliktu izraelsko-libańskiego w 2006 roku Iran dostarczył libańskiemu Hezbollahowi tysiące rakiet, pocisków i broni ręcznej, bezpośrednio naruszając rezolucję Rady Bezpieczeństwa ONZ nr 1701[63]. Iran dostarczył także setki milionów dolarów na wsparcie tego ugrupowania terrorystycznego i wyszkolił tysiące swoich bojowników w obozach w Iranie. Libańskie bojówki Hezbollahu były szeroko wykorzystywane w Syrii, w trakcie walki o umocnienie reżimu Assada. W Bahrajnie Iran nadal zapewniał broń, wsparcie i szkolenia lokalnym grupom szyickim. W marcu 2017 roku Departament Stanu wyznaczył dwie osoby powiązane z brygadami al-Ashtar z siedzibą w Bahrajnie (AAB), które otrzymują finansowanie i wsparcie od rządu Iranu. Co więcej, Iran wciąż rozbudowuje ofensywny program cybernetyczny, którego celem jest wspieranie

[61] Ibidem, [dostęp: 16.11.2018 r.].
[62] Ibidem, [dostęp: 16.11.2018 r.].
[63] Rezolucja Rady Bezpieczeństwa nr 1701 zakładała zaprzestanie działań zbrojnych oraz wycofanie się wojsk irańskich z terenu Libii. Jednym z założeń było również całkowite rozbrojenie Hezbollahu.

ataków cyberterrorystycznych na rządy innych państw czy podmioty należące do sektora prywatnego. Zaangażowanie w terroryzm w Iranie objawia się również wsparciem członków Al-Kaidy, którzy znaleźli schronienie na terytorium państwa. Rząd Iranu odmawia ich wydania oraz publicznej identyfikacji. Dodatkowo państwo umożliwia członkom organizacji rozmieszczanie strategicznych obiektów na jego terytorium[64]. Według danych z września 2018 roku na wsparcie różnych ugrupowań terrorystycznych Iran przeznacza średnio od 3,6 do 16 miliardów dolarów rocznie. Środki te są lokowane w terroryzm oraz umacnianie reżimów sprzyjających Iranowi[65]. Charakterystyka wydatków z 2017 roku została przedstawiona w tabeli (tabela 2).

Tabela 2. Wydatki Iranu na wsparcie działalności terrorystycznej – średnia wartość roczna według danych z 2018 roku

Ugrupowanie/reżim	Wartość wsparcia
Hezbollah	100-200 mln dolarów;
Reżim Assada w Syri	3,5-15 mld dolarów
Organizacje terrorystyczne w Syrii oraz Iraku	12-26 mln dolarów;
Organizacje terrorystyczne w Jemenie	10-20 mln dolarów;
Hamas	Brak szczegółowych szacunku
RAZEM	3,6-16 mld dolarów

Źródło: opracowanie własne na podstawie: Outlaw Regime: A chronicle of Iran's descrutive activities, https://www.state.gov/documents/organization/286410.pdf, [dostęp: 16.11.2018],

Państwo, które aktywnie uczestniczy w ułatwianiu działania współczesnych terrorystów to również Sudan, który na liście Departamentu Stanu USA znajduje się od 1993 roku. Sekretarz Stanu oskarża to państwo, że poprzez swoje działania wspiera takie organizacje terrorystyczne jak:

- Palestyński Islamski Dżihad;
- Hamas;
- Abu Nidal
- Hezbollah[66].

Pomimo tego, że Sudan znajduje się na oficjalnej liście państw wspierających terroryzm współpracuje ze Stanami Zjednoczonymi w zakresie zwalczania terroryzmu. Bezpośrednio po

[64] Hoffman B., *Recent Trends and Future Prospects of Iranian Sponsored International Terrorism*, RAND, Santa Monica 2008, s. 151.
[65] *A chronicle of Iran's descrutive activities*, https://www.state.gov/documents/organization/286410.pdf, [dostęp: 16.11.2018], s. 22-26.
[66] Wejkszner A., *Terroryzm sponsorowany przez państwa. Casus bliskowschodnich państw-sponsorów*, „Przegląd Politologiczny", nr 2, Tom 15, 2010, s. 59.

wpisaniu państwa na listę oraz po nałożeniu znacznych sankcji oraz licznych upomnień rząd Sudanu kontynuował prowadzenie działań antyterrorystycznych wraz z partnerami regionalnymi. W tym samym czasie prowadził operacje, których cel stanowiło przeciwdziałanie zagrożeniom dla interesów USA i personelu placówek dyplomatycznych państwa w Sudanie. Państwo zaangażowało się nawet w realizację założeń programu radykalizacji postaw Sudanu, który składa się z pięciu odmiennych poziomów. Jego głównym postulatem była reintegracja oraz rehabilitacja zagranicznych bojowników terrorystycznych, którzy popierali ideologie terrorystyczne. Efektem tego było przeprowadzenie kilku akcji „pokazowych". Jedna z nich odbyła się w czerwcu 2010 roku, kiedy to czterech Sudańczyków zostało skazanych na karę śmierci. Wyrok został nałożony za zabicie dwóch pracowników ambasady Stanów Zjednoczonych w styczniu 2008 roku. Pomimo zastosowania wszystkich środków zapobiegawczych, dwóm z czterech zamachowców udało się zbiec. Jeden z nich wciąż przebywa na wolności (prawdopodobnie ukrywa się w Somalii), a drugi ponownie trafił do więzienia, gdzie odsiaduje karę dożywocia[67].

W lutym 2017 roku niezidentyfikowana grupa osób prawdopodobnie przedwcześnie zdetonowała bombę w mieszkaniu mieszczącym się w dzielnicy Arkawit w Chartumie, co spowodowało eksplozję. Czyn ten został zaklasyfikowany jako akt terroryzmu, dlatego też sudańscy urzędnicy zdecydowali się na podjęcie restrykcyjnych kroków. Według oficjalnych doniesień, za zamach odpowiadają cudzoziemcy, przy których znaleziono materiały wybuchowe, broń oraz zagraniczne paszporty. Warto podkreślić, że był to jedyny atak terrorystyczny do jakiego doszło w 2017 roku w Sudanie[68]. Pozytywne zmiany w podejściu Sudanu do walki z terroryzmem sprawiły, że w październiku 2017 roku Stany Zjednoczone zdecydowały się na zniesienie sankcji gospodarczych wobec Sudanu. Państwo w pozytywny sposób wywiązuje się z założeń pięciopoziomowego planu zaangażowania, który obejmuje proces oceny sudańskiej współpracy antyterrorystycznej ze Stanami Zjednoczonymi. Plan wzywa Sudan do usprawnienia działań antyterrorystycznych poprzez wzmocnioną współpracę międzyregionalną i międzynarodową. W ramach rządowej strategii antyterrorystycznej siły sudańskie patrolują sudańsko-libijską granicę, aby ograniczyć przepływ osób, które mogą być związane z terroryzmem, zajmować się przemytem broni bądź innymi, nielegalnymi aktywnościami. Sudan stara się aktywnie zwalczać zjawisko terroryzmu i dąży do tego, by Stany Zjednoczone wykreśliły

[67] *Ibidem*, s. 59.
[68] US. Department of State, *Country Reports on Terrorism 2017*, https://www.state.gov/j/ct/rls/crt/index.htm[dostęp: 16.11.2018].

go z listy krajów sponsorujących terrorystów. Należy jednak podkreślić, że rozległe rozmiary terytorium państwa, przestarzała technologia rządowa czy praktycznie nieistniejące ograniczenia wizowe wciąż stanowią ogromne wyzwanie dla bezpieczeństwa państwa i jego granic[69].

Ostatnim z państw, które znajduje się na liście podmiotów wspierających terroryzm, jest Syria. Na listę Departamentu Stanu USA została wpisana w 1979 roku. Od tego momentu Syria wciąż podejmowała polityczne oraz wojskowe wysiłki na rzecz wsparcia dla różnorodnych ugrupowań terrorystycznych. Reżim nadal zapewniał broń i wielowymiarowe wsparcie libańskiemu Hezbollahowi, a także zezwalał Iranowi na ponowne zbrojenie organizacji terrorystycznych. Państwa regularnie współpracowały pomiędzy sobą i udzielały wsparcia na arenie międzynarodowej. Relacje reżimu Assada z libańskim Hezbollahem i Iranem stały się jeszcze silniejsze w 2017 roku. Wynikało to przede wszystkim z rosnącej zależności trwałości reżimu od wsparcia zewnętrznego. Prezydent Baszar al-Assad pozostał zagorzałym obrońcą polityki Iranu, podczas gdy Iran wykazywał równie energiczne poparcie dla syryjskiego reżimu. Syryjskie przemówienia rządowe i komunikaty prasowe często zawierały oświadczenia wspierające grupy terrorystyczne, w szczególności libański Hezbollah. Można więc powiedzieć, że działania Syrii realizowane były w sposób świadomy, ponieważ państwo dostrzegało w nim liczne korzyści. Mowa tutaj przede wszystkim o poparciu politycznym i zbrojnym[70].

W ciągu ostatniego dziesięciolecia liberalny stosunek reżimu Assada do al-Kaidy i innych ugrupowań terrorystycznych przyczynił się do ich znacznego rozwoju. Syryjski rząd przez wiele lat dokonywał transferu terrorystów przez swoje terytorium do Iraku, aby mogli walczyć z siłami koalicyjnymi. Działania te są bardzo dobrze udokumentowane, jednak władze Syrii wciąż twierdzą, że są państwem, które padło ofiarą terroryzmu, a szczególnie terrorystów tworzących opozycję rządu. Należy jednak zaznaczyć, że to z Syrii swoje ataki terrorystyczne planowała jedna z najgroźniejszych współczesnych organizacji terrorystycznych – ISIS. Ponadto reżim syryjski zakupił ropę od ISIS za pośrednictwem różnych pośredników, co zwiększyło dochody grupy terrorystycznej. Dodatkowo Syria nie wypełnia swoich zobowiązań wynikających z Konwencji o broni chemicznej (CWC). Stany Zjednoczone oceniają, że Syria wielokrotnie stosowała broń chemiczną przeciwko ludności syryjskiej od czasu przystąpienia do Konwencji w 2013 roku, jest to zatem jawne naruszenie zobowiązań wynikających z CWC. W czasie obecnego konfliktu

[69] *Ibidem*, [dostęp: 16.11.2018].
[70] Wejkszner A., op. cit., s. 63.

pojawiły się liczne doniesienia na temat ponownego stosowaniu broni chemicznej przez reżim (wcześniejsze przypadki zostały odnotowane w 2014 oraz 2015 roku)[71].

Synteza zaprezentowanych informacji pozwala dostrzec, że państwa w różny sposób wspierają oraz mogą wspierać działalność ugrupowań terrorystycznych. Cytowany już Artur Wejkszner proponuje dwa sposoby klasyfikacji tej pomocy[72]. Pierwszy z nich odnosi się do siły udzielanego wsparcia, co szczegółowo zostało wyjaśnione w tabeli (tabela 3).

Tabela 3. **Klasyfikacja wsparcia terrorystów przez państwo w zależności od siły/ poziomu zaangażowania**

Poziom zaangażowania	Charakterystyka
Silne wsparcie	Są to państwa, których cele polityki zagranicznej są tożsame z celami terrorystów;
Średnie wsparcie	Są to państwa sympatyzujące z organizacjami terrorystycznymi, które chętnie wspierają ich działania i wyrażają dla nich aprobatę. Część z nich nie chce bezpośrednio podejmować działań, które zostaną zrealizowane przez terrorystów;
Małe wsparcie	W tym przypadku występuje zamiar wsparcia, jednak nie ma odpowiednich środków, aby wesprzeć terrorystów. Państwo nie utrudnia jednak działalności terrorystycznej;
Ambiwalentne wsparcie	Jest to tolerowanie terrorystów i wspieranie ich jedynie w określonych i wybranych sytuacjach, które są zgodne z poglądami aktualnie rządzących i wdrażaną polityką zagraniczną;
Pasywne wsparcie	W tym przypadku nie występuje jakiekolwiek wsparcie dla działań terrorystów, jednak państwo równocześnie nie podejmuje żadnych inicjatyw na rzecz zwalczania organizacji terrorystycznych, dzięki temu w pewnym stopniu pozostają oni bezkarni. Władze często udają, iż nie dostrzegają, że na ich terytorium funkcjonują bardzo groźni terroryści;

Źródło: opracowanie własne na podstawie: A. Wejkszner, *Terroryzm sponsorowany przez państwa. Casus bliskowschodnich państw-sponsorów*, „Przegląd Politologiczny", nr 2, Tom 15, 2010, s. 56-57.

Przedstawione dane wskazują na stosunek państw wobec terroryzmu. Jego zakres rozpoczyna się od aktywnego współdziałania z terrorystami po pasywne wsparcie sprowadzające się do braku jakiejkolwiek reakcji. Każda z wymienionych postaw jest szkodliwa dla

[71] US. Department of State, *Country Reports on Terrorism 2017*, https://www.state.gov/j/ct/rls/crt/index.htm[dostęp: 16.11.2018].
[72] Wejkszner A., *op. cit*., s. 57.

bezpieczeństwa państwa[73]. Analiza dostępnej literatury oraz obserwacja działań praktycznych państw wspierających terroryzm pozwala również dostrzec, że państwa ułatwiają działalność terrorystyczną za sprawą:

- wsparcia militarnego – sprowadzającego się do szkolenia terrorystów na terenie danego państwa lub poza nimi (wykorzystanie broni, taktyka, wywiad) bądź też współdziałania z nimi w trakcie różnorodnych akcji operacyjnych;
- wsparcia finansowego i logistycznego – państwa przekazują terrorystom środki pieniężne, które wydają na broń, szkolenia czy planowanie nowych akcji terrorystycznych. Wsparcie logistyczne wiąże się z organizacją podróży i przemieszczaniem terrorystów, dostarczaniem im paszportów czy zapewnianiem schronienia na terenie państwa;
- wsparcia dyplomatycznego – ta forma wsparcia to zazwyczaj subtelne działania na korzyść terrorystów. Przykładem takiego wsparcia jest chociażby krytykowanie rządowych inicjatyw antyterrorystycznych;
- wsparcia organizacyjnego – objawia się we współtworzeniu struktur organizacyjnych ugrupowań terrorystycznych oraz wspierania ich w rekrutacji nowych członków. Państwa wykorzystują swoje doświadczenie i wiedzę, aby pomóc terrorystom sprawnie funkcjonować i planować kolejne ataki terrorystyczne;
- wsparcia w postaci wyznaczania kierunków ideologicznych, gdzie państwo doradza organizacji, jakie wartości i cele powinna wyznawać. Wsparcie to może przybrać formę przedstawienia gotowego zbioru idei bądź też pośrednią. Drugie rozwiązanie wiąże się z budowaniem korzystnej atmosfery dla rozwoju organizacji terrorystycznych;
- wsparcie w formie azylu dla terrorystów – wiele państw decyduje się na zapewnienie bezpiecznego schronienia dla terrorystów. Daje im dostęp do baz szkoleniowych, miejsc kontaktowych, noclegu, centrali dowodzenia, posiadanych systemów itp. Państwa tego typu są określane mianem *safe heaven*, a ich działalność jest doceniana przez terrorystów, którzy wiedzą, gdzie powinni się udać w przypadku wystąpienia niekorzystnych zbiegów okoliczności[74].

Syntetyzując przedstawione informacje, można zauważyć, że wiele spośród współczesnych państw posiada swój udział we wspieraniu działalności terrorystycznej. W

[73] Ibidem, s. 78.
[74] *Ibidem*, s. 59-60.

większości przypadków wynikają one ze świadomych i bezpośrednich inicjatyw, dzięki którym państwo chce umacniać swoją pozycję bądź też realizować przyjęte założenia polityki zagranicznej. Można więc powiedzieć, że terroryści stają się jednym z narzędzi budowania potęgi międzynarodowej, co wynika z ich bezwzględności, chęci do współpracy ze strukturami państwowymi, które mogą pomóc im w uzyskaniu licznych korzyści lub też uchronić przed najwyższym wymiarem kary. Terroryści mogą więc wspierać działania z zakresu wojny hybrydowej, która coraz częściej pojawia się we współczesnych relacjach międzynarodowych i jest sposobem na osiągnięcie zamierzonych celów politycznych, ekonomicznych, ale także i społecznych.

1.5.4. Wojna hybrydowa jako szczególna forma terroryzmu państwowego

Współczesne państwa posługują się różnorodnymi metodami walki ze swoimi przeciwnikami, które dostosowane są do ich aktualnych potrzeb oraz możliwości. Ewolucja uwarunkowań zewnętrznych i wewnętrznych sprawiła, że tradycyjne podejście do wojny stopniowo odchodzi w niepamięć. Obecnie kraje, które zobowiązały się do przestrzegania licznych porozumień oraz traktatów pokojowych posługują się działaniami, które tylko z pozoru nie przypominają działań wojennych. Przykładem takiego podejścia jest stosowanie wojny hybrydowej, która doczekała się dużego zainteresowania ze strony badaczy i teoretyków stosunków ekonomicznych. Zagadnienie wojny hybrydowej zaczęło pojawiać się już w latach 90. XX wieku w Stanach Zjednoczonych w odniesieniu do działań wojennych realizowanych w Iraku oraz Afganistanie. Pojęcie to nabrało jednak nowego znaczenia dopiero w ostatnich czasach, kiedy Rosja postanowiła wykorzystać niestandardowe metody walki wobec Ukrainy, a także dążyła do znacznej dezinformacji w relacjach z NATO czy Unią Europejską[75].

Próba definicji wojny hybrydowej nakazuje odwołać się do jednego z pierwszych jej wyjaśnień, które zostało stworzone przez Williama J. Nemetha w 2002 roku. W swojej pracy pt. *Future war and Chechnya: A case for hybrid warfare* autor ten analizował działania zbrojne pomiędzy Czeczenią i Rosją, a zagadnienia hybrydowości używał „nie tylko w stosunku do działań prowadzonych przez czeczeńskich bojowników, lecz także do sposobu funkcjonowania tamtejszego społeczeństwa. Jedną z cech społeczeństwa hybrydowego jest połączenie

[75] Grabowska K., *Próba wyjaśnienia pojęcia i istoty wojen hybrydowych*, „Świat Idei i Polityki", Tom 14, s.

nowoczesnych teorii politycznych z tradycyjną organizacją społeczną i obyczajowością”[76]. Badania W.J. Nemetha pozwoliły mu wyodrębnić kilka zasadniczych cech przypisywanych wojnie hybrydowej. Wśród nich można wymienić:

- „organizację armii, która stanowi reprezentację dla aktualnego rozwoju społeczno-ekonomicznego całego państwa jak i pojedynczych wspólnot oraz obowiązujących w ich ramach norm i wartości;
- nowe podejście do postrzegania siły militarnej, ponieważ w przypadku wojny hybrydowej siłę stanowi masowość zastosowanych ataków partyzanckich oraz zaawansowanie technologiczne;
- umiejętne wplatanie nowoczesnych technologii do działań strategicznych oraz taktycznych, które są realizowane w trakcie wojny”[77].

Podejście prezentowane przez W.J. Nemetha pozwoliło spojrzeć na wojnę w zupełnie nowy, odmienny sposób. Zainteresowało się nim wielu badaczy, którzy w czasach późniejszych pragnęli zgłębić zagadnienie wojny hybrydowej i dostrzec jej istotę oraz sens. Na szczególną uwagę zasługują tutaj zwłaszcza definicje opracowane przez Francisa G. Hoffmana oraz Walerija Gierasimowa. Zdaniem F.G. Hoffmana, który był amerykańskim analitykiem skupiającym się na analizie stosunków międzynarodowych, a swoje doświadczenia wojskowe zdobywał poprzez pełnienie funkcji oficera w armii Stanów Zjednoczonych, konieczne było spojrzenie na wojnę hybrydową jako na zupełnie nowy paradygmat[78]. Analityk ten skupił się bowiem na syntezie i analizie informacji na temat:

- wojen czwartej generacji;
- wojen złożonych;
- wojen bez ograniczeń[79].

Wyniki osiągnięte przez niego oraz jego współpracowników pozwoliły uznać, że wojny hybrydowe „zawierają w sobie zestaw różnych metod działań wojennych, wliczając w to działania konwencjonalne, nieregularne taktyki i ugrupowania zbrojne, akty terrorystyczne, w tym masową przemoc, oraz działania przestępcze.”[80]. Ze względu na swoją specyfikę tego rodzaju konflikty

[76] Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego”, Wydanie specjalne, 2011, s. 40.
[77] *Ibidem*, s. 40-41.
[78] Banasik M., *How to understand the hybrid war*, „Securitologia”, nr 1, 2015, s. 24.
[79] *Ibidem*, s. 24.
[80] Skoneczny Ł., *op. cit*., s. 41.

mogą być nadzorowane oraz prowadzone zarówno przez państwa, jak i inne podmioty pozapaństwowe, a w szczególnych przypadkach nawet przez większe zgrupowania czy oddziały. Zwycięstwo w wojnie hybrydowej jest uzależnione od zastosowania zaawansowanych technologii, które dają przewagę nad przeciwnikiem i umożliwiają przewidywanie jego ruchów oraz sprawne reagowanie. Dodatkowe znaczenie posiadają tutaj działania wymierzone w dezorganizację państwa i wywołanie chaosu. Dostrzec więc można, że wojna hybrydowa nosi w sobie znamiona ataku cyberterrorystycznego na infrastrukturę krytyczną państwa, gdzie w większości przypadków działania te skutkują znaczną dezinformacją oraz dezorganizacją jej funkcjonowania[81]. Dorobek F.G. Hoffmana pozwolił na stworzenie listy uniwersalnych cech wojny hybrydowej, które autor zaprezentował na przykładzie konfliktu na linii Hezbollah-armia izraelska (konflikt ten jest często określany mianem II wojny libańskiej). Charakterystyki te są następujące:

- podmioty pozapaństwowe są w stanie działać zgodnie z zachodnim modelem działań zbrojnych;
- bardzo dobre przeszkolenie podmiotów niepaństwowych, które sprawnie poruszają się w przestrzenie miejskiej i są w stanie świetnie się ukrywać oraz tworzyć liczne zasadzki;
- żołnierze są bardzo trudni do identyfikacji, ponieważ przenikają tłumy i niczym tak naprawdę się nie wyróżniają;
- realizacja działań informatyczno-wywiadowczych o charakterze strategicznym lub operacyjnym poprzez podmiot niepaństwowy;
- wyposażenie w nowoczesny sprzęt wojskowy żołnierzy, którzy walczą po stronie podmiotu niepaństwowego[82].

Wyszczególnione cechy wojny hybrydowej dowodzą, że staje się ona niebezpiecznym narzędziem realizacji różnorodnych celów współczesnych państw. Przemawia za tym jej charakter i trudność w rozgraniczeniu stanu wojny i pokoju oraz w posługiwaniu się najnowszymi rozwiązaniami technologicznymi oraz nowoczesnym sprzętem wojskowym przez podmioty niepaństwowe[83]. Wojna hybrydowa stała się przedmiotem zainteresowania rosyjskich badaczy, którzy dążyli do poznania jej specyfiki oraz oceny przydatności w perspektywie działań

[81] *Ibidem,* s. 43.
[82] Banasiak M., Parafianowicz R., *Teoria i praktyka działań hybrydowych*, „Zeszyty Naukowe Akademii Obrony Narodowej", nr 2(99), 2015, s. 10.
[83] *Ibidem,* s. 10.

podejmowanych przez Rosję. Na uwagę zasługują opracowania generała armii Walerija Wasilijewicza Gierasimowa, który przez długi czas pełnił i wciąż pełni funkcję Szefa Sztabu Generalnego Sił Zbrojnych Rosji. Jego spojrzenie rzuca zupełnie nowe światło na konflikty hybrydowe, ponieważ koncepcja stworzona przez W. Gierasimowa została wykorzystana w praktyce podczas konfliktu na linii Rosja-Ukraina. W wydanym opracowaniu pt. *Znaczenie nauki w przewidywaniu* W. Gierasimow w bezpośredni sposób nie używa określenia wojna hybrydowa, jednak jego treść jednoznacznie wskazuje na to, jaki rodzaj działań charakteryzuje. W. Gierasimow uważa, że w czasach współczesnych dochodzi do zatarcia granic pomiędzy wojną a pokojem, ponieważ państwa nieustannie walczą o swoje interesy i dążą do tego, aby to ich racje zostały uznane, posługując się przy tym niematerialnymi środkami działania[84]. Wśród nich za kluczowe instrumenty oddziaływania uważa się:

- narzędzia ekonomiczne;
- narzędzia humanitarne;
- narzędzia polityczne;
- manipulowanie opiniami oraz nastrojami osób, które zamieszkują na terenie objętym konfliktem[85].

W ujęciu W. Gierasimowa przedstawione działania powinny być wspierane odpowiednio dobranymi i zaplanowanymi operacjami militarnymi. Mowa tutaj przede wszystkim o zastosowaniu wojny informacyjnej, a także o realizacji działań jednostek operacyjnych. Dopiero w późniejszej, końcowej fazie konfliktu zaleca się wprowadzenie oddziałów zbrojnych odpowiadających za nadzorowanie misji humanitarnych bądź zbrojnych na terenie objętym konfliktem. Jak podkreśla W. Gierasimow, nowoczesna technologia usprawnia komunikację na linii dowództwo-oddziały zbrojne. Dzięki temu są one w stanie szybciej reagować oraz informować o bieżącej sytuacji. Dodatkowo nowoczesna technologia daje szansę na osłabienie sił przeciwnika. Jako jeden z przykładów można przytoczyć zdarzenia z Ameryki Południowej, gdzie członkowie społeczeństwa byli motywowani do walki za pośrednictwem mediów społecznościowych. Co więcej, ten nowoczesny środek komunikacji posłużył również jako narzędzie oddziaływania na władze państwowe[86].

[84] Deshpande V., *Hybrid Warfare: The changing character of conflict,* Pentagon Press, Waszyngton 2018, s. 26.
[85] *Ibidem*, s. 26.
[86] Skoneczny Ł.*, op. cit*., s. 41.

Koncepcje wojny hybrydowej W.J. Hoffmana oraz W. Gierasimowa pozwalają dostrzec duże zmiany w zakresie prowadzenia współczesnych konfliktów zbrojnych. Ich autorzy podkreślają bowiem, że obecnie konieczne jest zastosowanie niestandardowych, pozamilitarnych środków oddziaływania na wroga. Nie bez znaczenia jest również dążenie do łączenia strategicznych, operacyjnych oraz taktycznych obszarów działania czy decentralizacja dowództwa. Wszystkie te elementy są wspierane nowoczesną technologią, która wpływa na możliwości prowadzenia konfliktu hybrydowego. Dodatkowo państwa decydują się na stosowanie działań asymetrycznych i angażowanie małych, jednak bardzo dobrze przeszkolonych i wyposażonych oddziałów partyzanckich[87].

Analiza części pozostałych źródeł literatury przedmiotu zwraca uwagę na inne charakterystyki związane z wojną hybrydową. Przykładowo Aleksandra Gorzkowicz zauważa i podkreśla, że jest ona prowadzona na dwóch płaszczyznach. Mowa tutaj o płaszczyźnie terytorialnej oraz wirtualnej. Płaszczyzna terytorialna odnosi się do państwa lub też grup, na przykład, wspólnot etnicznych zamieszkujących dane terytorium. Z kolei płaszczyzna wirtualna stanowi znacznie szerszą kategorię, gdyż jest ponadterytorialna oraz transgraniczna. Daje również szerokie spektrum działania[88]. Autor ten wskazuje, że wojna hybrydowa wyróżnia się dwiema podstawowymi cechami, a mianowicie psychologicznym charakterem oraz stosowaniem przestrzeni cybernetycznej do realizacji celów wojennych, na przykład zniszczenia sieci teleinformatycznych, propagandy czy rozpowszechniania gróźb. Ataki te są szybkie i trudne do przewidzenia, a ich skutki powodują natężenie paniki wśród ludności cywilnej. Zdaniem badaczki zatem, problemy związane z regulowaniem działań wojen hybrydowych będą się nasilać w nadchodzący czasie, czego doskonałym przykładem jest konflikt Rosja-Ukraina. Wynika to przede wszystkim z braku odpowiednich uregulowań prawnych, a mowa przede wszystkim o braku uniwersalnej definicji wojny hybrydowej w prawie międzynarodowym czy jakichkolwiek regulacjach pozwalających na jej klasyfikowanie bądź też zwalczanie[89].

[87] I*bidem*, s. 44.
[88] *Ibidem*, s. 44
[89] Gorzkowicz A., *Wojna hybrydowa na Ukrainie jako przykład współczesnych konfliktów zbrojnych*, „Roczniki Studenckie Akademii Wojsk Lądowych", nr 1(1), 2017, s. 148-149.

1.6. Cyberterroryzm

1.6.1. Wybrane definicje cyberterroryzmu obecne w literaturze przedmiotu

Cyberterroryzm to zjawisko nadal stosunkowo nowe, a jego chronologia obejmuje ostatnie ćwierćwiecze. Co prawda za twórcę pojęcia 'cyberterroryzm' uznaje się Barry'ego Collina, pracownika Institute for Security and Intelligence z Kalifornii, który już w latach 80. XX wieku użył go dla określenia połączenia cyberprzestrzeni i terroryzmu[90]. Niemniej jednak w niniejszym opracowaniu analizie poddane będą te formy cyberterroryzmu, które dopiero w ostatnim dwudziestoleciu niejako od nowa definiują to pojęcie. Współczesny cyberterroryzm zakłada wykorzystanie nowoczesnych technologii komputerowych i teleinformatycznych, te zaś (w obecnej formule, choć oczywiście ulegającej dynamicznej fluktuacji), istnieją od niewielu lat, zwłaszcza w rozumieniu systemu światowego. Ponadto w niniejszej pracy analizowane będzie zjawisko cyberterroryzmu, wymierzonego głównie w infrastrukturę krytyczną, zwłaszcza energetyczną, czyli w system, który w obecnym kształcie również istnieje od bardzo niedawna.

Tomasz Szubrycht wyróżnia trzy grupy semantyczne dotyczące sposobu podziału definiowania zjawiska cyberterroryzmu. Jego zdaniem, postrzeganie tego zjawiska można podzielić na trzy grupy:

„pojęcia prezentowane w mediach;

definicje obowiązujące w gronie specjalistów;

definicje stworzone na użytek innych dziedzin działalności człowieka w dziedzinie informatyk".[91].

Według wspomnianego już B. Collina, „cyberterroryzm to świadome wykorzystanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia terrorystycznej akcji"[92]. Ogólnie przyjmuje się, że w pojęciu cyberterroryzmu mieści się „wykorzystywanie systemów teleinformatycznych do dezinformacji oraz walki psychologicznej itp. W tym przypadku celem ataku jest najczęściej informacja przetwarzana, a nie system jako taki"[93]. Cyberterroryzm rozumiemy tu jako „działania blokujące, niszczące lub zniekształcające w stosunku do informacji przetwarzanej, przechowywanej i przekazywanej w systemach teleinformatycznych oraz niszczące, ewentualnie obezwładniające te systemy"[94].

---

[90] Denning D., *Wojna informacyjna i bezpieczeństwo informacji,* Warszawa 2002, s. 79

[91] Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, w: „Zeszyty Naukowe Akademii Marynarki Wojennej", XLVI nr 1 (160), 2005, s.175 i dalsze.

[92] White K. C., *Cyber-Terrorism: Modem Mayhem*, Carlisle 1998, s. 10

[93] Kośla R., *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski,* [w:] Jędrzejewski M., *Analiza systemowa zjawiska infoterroryzmu,* Warszawa 2002, s. 482

[94] *Ibidem, s. 481*

Dorothy Denning za cyberterroryzm uważa już „samą groźbę ataku na komputery, sieci lub systemy informacyjne w celu zastraszenia lub wymuszenia na rządzie lub ludziach daleko idących politycznych i społecznych celów”[95]. Jej zdaniem jednak, za atak cyberterrorystyczny można uznać „tylko taki akt, który powoduje bezpośrednie szkody człowiekowi i jego mieniu lub przynajmniej jest na tyle znaczący, że budzi strach”[96]. Okazuje się zatem, że owo rozróżnienie nie jest ani tak łatwe ani tak oczywiste, a zastosowane kryteria czynią je dość arbitralnym. D. Denning jako przykład takich „aktów” klasyfikowanych jako cyberterrorystyczne podaje „śmierć człowieka, obrażenia ciała, wybuch, zderzenie samolotów lub spowodowanie strat finansowych”, zatem akty niewywołujące takich skutków, według niej, nie są już atakami cyberterrorystycznymi. Niestety, D. Dennig nie daje odpowiedzi, jak klasyfikować na przykład dokonane za pomocą technik informatycznych wstrzymanie dostaw energii elektrycznej – na tyle krótkotrwałe, że nie muszą wywołać niczyjej śmierci ani też strat materialnych. W tym przypadku o definiowaniu takiego rodzaju aktu jako cyberterrorystycznego powinno decydować domniemanie zamiaru i skutek ataku, nie zaś to, czy ostatecznie wyrządził on straty finansowe czy doprowadził do śmierci ludzi.

Według definicji zaproponowanej przez US National Infrastructure Protection Centre, w roku 2001 cyberterroryzmem będzie każdy „[...] „akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie i / lub przerwanie świadczenia usług dla wywołania strachu, poprzez wprowadzanie zamieszania lub niepewności w danej populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonego przez terrorystów programu”[97]. Z kolei w opinii US Federal Bureau of Investigation (FBI) cyberterroryzm „[...] jest to obmyślony, politycznie umotywowany akt przemocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który mając charakter niemilitarny, przeprowadzony jest przez ponadnarodowe lub narodowe grupy terrorystyczne”[98]. Należałoby zatem przyjąć, że wskazanie „niemilitarnego” charakteru takiego aktu zakłada, iż owe „militarne” będą klasyfikowane jako element konfliktu cybernetycznego czy informatycznego, nie zaś w kategorii aktu cyberterrorystycznego. Autor

[95] Denning D., *op. cit*, s. 79.
[96] *Ibidem*, s. 80
[97] http://www.nopc.gov./publication/highlight/2001/highlight-01-06. htm, [dostęp: 17 III 2017]
[98] *Ibidem*.

niniejszej rozprawy przypuszcza, że z uwagi na dynamikę zmian w charakterze współczesnych konfliktów definicja ta uległa modyfikacji na rzecz dopuszczenia aktu cyberterrorystycznego jako elementu hybrydowego konfliktu militarnego.

Tym samym warto przywołać definicję zaproponowaną przez Jamesa Lewisa (dokładnie z tego samego, bo 2002 roku, w którym swoją definicję opracowała D. Dening), według której cyberterroryzm to „wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych /takich jak energetyka transport, instytucje rządowe, itp./, bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań”[99].

Mark M. Pollit, wcześniej pracownik FBI, a obecnie wykładowca Syracuse University, twierdzi, iż „cyberterroryzm to przemyślany, politycznie umotywowany atak, skierowany przeciw informacjom, systemom komputerowym, programom i danym, który prowadzi do oddziaływania na nie militarne cele, przeprowadzony przez grupy narodowościowe lub przez tajnych agentów”[100]. Jak słusznie zauważył Ernest Lichocki, definicja Pollita „[…] nie ogranicza zakresu środków użytych do przeprowadzenia ataku cyberterrorystycznego, czyli atak może nastąpić zarówno przy użyciu środków oddziaływania fizycznego, jak i teleinformatycznego”[101].

Wiesław Smolski zaproponował klasyfikację cyberterroryzmu w oparciu o kryterium podmiotowe i przedmiotowe. Jak pisze, „stosując pierwsze z nich, mówimy o cyberterrorystach i ich ofiarach, czyli o podmiotach działań i podmiotach ataku. W kontekście stosunków międzynarodowych podmioty ataku stanowią uczestnicy państwowi i niepaństwowi. Wśród podmiotów działań możemy wyróżnić grupy zorganizowane i cyberterrorystów indywidualnych. Wśród grup zorganizowanych istnieją zarówno klasyczne organizacje terrorystyczne […] które oprócz środków konwencjonalnych wykorzystują w swoich działaniach zarówno cyberprzestrzeń, jak i grupy terrorystyczne, składające się z hakerów komputerowych działających w zasadzie wyłącznie w cyberprzestrzeni. Jeśli chodzi o cyberterrorystów indywidualnych, to istnieje około kilku tysięcy osób, które można określić mianem profesjonalnych hakerów. Są to ludzie posiadający ściśle określone kwalifikacje, którzy dokładnie wiedzą, co robią. Są to osoby, które za odpowiednią opłatą mogą zrobić wszystko,

[99] Lewis, J. A., *Assessing the risk of cyber terrorism, cyber war and other cyber threats*, Center for Strategic and International Studies 2002 r., [URL http://www.csis.org/tech/0211_lewis.pdf].
[100] Pollit Mark M., *Cyberterrorism*, Facts or Fancy, http://www.cs.georgetown.edu/~denning/infosec/pollitt.html] [dostęp: 22.11.2015] Obecnie publikacja niedostępna.
[101] Lichocki E, *Cyberterroryzm państwowy i niepaństwowy, początki, formy, skutki*, s. 6. Opracowanie pochodzi ze zbiorów Collegium Civitas/Akademia Obrony Narodowej.

mogą więc wykonywać zadania o charakterze politycznym, zlecone przez organizacje terrorystyczne […][102].

Zdaniem badacza, kryterium przedmiotowe dotyczy skutków ataków cyberterrorystycznych. „Posiadają one aspekt militarny, gospodarczy i polityczny. […] Przykładem skutków militarnych jest działalność hakerów komputerowych wynajętych przez władze chińskie, którzy wykradli tajne informacje z laboratorium badań nad bronią nuklearną w Los Alamos w Nowym Meksyku. Fakt ten miał miejsce pod koniec lat 90. ubiegłego stulecia a był utrzymywany w tajemnicy do 2000 roku"[103].

Zdaniem autora niniejszej pracy, zdecydowanie najtrafniejszą, najbardziej szczegółową i precyzyjną, a jednocześnie szeroko poznawczą definicję, zaproponował w roku 2012 Daniel Mildner. Jednocześnie należy uznać, że jest to definicja najbardziej aktualna i kompletna, bowiem dla jej wypracowania poddano analizie frekwencyjnej 46 dotychczas przyjętych definicji – 26 anglojęzycznych, 17 polskojęzycznych i 3 rosyjskojęzycznych. Niezaprzeczalnie istotny pozostaje fakt, iż największa liczba 30 analizowanych przez D. Mildnera definicji miała charakter instytucjonalny, co -– dla neoinstytucjonalnej perspektywy badawczej przyjętej w niniejszej pracy – nie pozostaje bez znaczenia. W jego opinii cyberterroryzm „jest to jedna z odmian terroryzmu, wyróżniona ze względu na podejmowane w celu jej wykonania środki. Stanowi działanie niezgodne z prawem lub przez prawo nieregulowane, a podejmowane przez jakikolwiek podmiot: jednostkę lub grupę. Działanie to polega na stosowaniu groźby przemocy (przemocy psychicznej) lub przemocy fizycznej. Jest podejmowane w cyberprzestrzeni (pośrednie i bezpośrednie) oraz poza nią, ale na cyberprzestrzeń oddziałujące". Cyberterroryzm to działanie skierowane przeciwko komputerom i sieciom komputerowym, zarówno ich warstwie fizycznej, jak i cyfrowej, a w szczególności komputerom i sieciom, składającym się na infrastrukturę krytyczna. Bezpośrednim celem tych działań jest całkowite lub częściowe zniszczenie lub zakłócenie działania fizycznej lub cyfrowej warstwy sieci. Działania te mają spowodować poczucie zagrożenia, straty materialne lub ludzkie. Widownia tych działań są dowolne instytucje, które mogą przyjąć 'komunikat' cyberterrorystów lub tez przekazać go innym instytucjom (np. społeczeństwu i składającym się nań grupom, opinii publicznej, instytucjom państwa, organizacjom, w tym międzynarodowym, mediom). Efekt to wywarcie wpływu na

[102] Smolski W., *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, Białystok, s. 482.
[103] *Ibidem*, s. 483.

ośrodki decyzyjne, czyli osoby lub instytucje mogące bezpośrednio (na przykład rządy państw) lub pośrednio (na przykład społeczeństwa, poszczególne grupy społeczne) zrealizować postulaty podejmujących atak cyberterrorystyczny. Żądania cyberterrorystów mogą odnosić się do dowolnie wskazanego celu mającego charakter polityczny. Może mieć on zarówno charakter instrumentalny (osiągniecie określonych, wskazanych korzyści), jak i ekspresywny (gdy działanie ma charakter symboliczny)"[104].

Przedstawione powyżej wybrane próby zdefiniowania pojęcia cyberterroryzmu – mimo iż posiadają szereg kryteriów wspólnych (zwłaszcza co do charakteru ataku, a także zastosowanych środków) – to jednak określenie ich jako „tożsamych" jest niemożliwe. Choć definicje podstawowe wydaje się stosunkowo pokrewne i zbliżone semantycznie u wszystkich autorów, to podawane przez nich znaczenia rozszerzające, pełniące funkcję dopełniającą i uzupełniającą, czynią je dalece różnorodnymi. Przyjęcie jednoznacznej, kompletnej i uzgodnionej definicji cyberterroryzmu nie wydaje się nadal możliwe, czego uzasadnieniem wydaje się niewątpliwie wyjątkowa złożoność i dynamika zmian w charakterystyce tego zjawiska. Zasadne jest więc zaproponowanie poniższej krótkiej definicji zjawiska cyberterroryzmu, która – będąc niewątpliwie jedynie syntezą definicji cytowanych uprzednio – jest na potrzeby niniejszej pracy niezbędna.

1.6.2. Cyberterroryzm – próba definicji własnej

Cyberterroryzmem należy określić motywowany politycznie, ideologicznie, gospodarczo lub militarnie atak (albo samą groźbę takiego ataku), prowadzony z użyciem technik i narzędzi teleinformatycznych na systemy i sieci teleinformatyczne oraz/lub zgromadzone dane, w celu uszkodzenia, zniszczenia lub sparaliżowania systemu infrastruktury krytycznej państwa oraz/lub w celu zastraszenia i wymuszenia określonych działań czy koncesji politycznych, militarnych lub gospodarczych. Atak cyberterrorystyczny może być autonomiczny, ale może również być częścią składową kompleksowego działania o charakterze polityczno-militarnym (konflikt hybrydowy).

Definicja powyższa w sposób oczywisty ma charakter roboczy, stanie się jednak podstawą dla dalszego wnioskowania w zakresie oceny możliwości wypracowania skutecznej polityki zapobiegania cyberterroryzmowi w kontekście ochrony infrastruktury krytycznej.

[104] Mildner D., *op. cit., s. 109.*

1.6.3. Obszary zagrożeń cyberterrorystycznych

Zagrożenie tym zjawiskiem dotknąć dziś może praktycznie wszystkich jednostek organizacyjnych państwa, wszystkich podsektorów infrastruktury krytycznej. I to nie tylko jednego, konkretnego państwa narodowego, ale i całej grupy państw czy organizacji międzynarodowych. Oddziaływanie aktu terrorystycznego, dokonanego poprzez cyberatak, jest zawsze wielowymiarowe, przyczynia się do destrukcji i dezorganizacji życia całej społeczności lub sporej jej części. Zwłaszcza ataki na systemy energetyczne, ale też transportowe, łącznościowe czy sieci bankowe są wyjątkowo skutecznym narzędziem wpływu na rządy i opinię społeczną. W przypadku podziału na obszar zagrożeń cyberterrorystycznych mamy do czynienia głównie z atakami na:

- systemy wojskowe, które przechowują informacje o położeniu satelitów, rozmieszczeniu wojsk oraz broni, prowadzących badania nad nowymi rodzajami broni, systemami łączności itp. Głównymi sprawcami są z reguły agenci obcych wywiadów, zaś zleceniodawcami przede wszystkim inne państwa;
- systemy przedsiębiorstw, które przechowują informacje ważne z punktu widzenia działalności firmy, np. o wykorzystywanych technologiach itp. Głównymi sprawcami byli i nadal są najczęściej pracownicy (lub byli pracownicy), którzy współpracują z konkurencją, obcymi wywiadami, czy też działają po prostu z chęci zysku, bez motywacji pozaekonomicznej;
- systemy wchodzące w skład tak zwanej, infrastruktury krytycznej państwa, czyli systemy: bankowo-finansowe, energetyczne, telekomunikacyjne, dostarczania wody, transportu, służb do działań w sytuacjach wyjątkowych, które przechowują informacje ważne dla bezpieczeństwa państwa. Sprawcami tych ataków mogą być zarówno pracownicy firm związanych z wyżej wymienionymi systemami oraz terroryści.[105] Infrastruktura krytyczna ze względu na swoje znaczenie i rolę w bezpieczeństwie państwa jest częstym przedmiotem działania terrorystów. Starają się oni podejmować wszelkie działania, które zakłócą jej sprawne funkcjonowanie, a tym samym doprowadzą do dezorganizacji w danym państwie. Coraz większym zagrożeniem staje się cyberterroryzm, co należy wiązać z postępem technologicznym i informatyzacją życia ludzkiego. Obecnie trudno bowiem mówić o elementach infrastruktury

[105] *Ibidem*, s. 483.

krytycznej, która nie korzysta ze wsparcia technologicznego. Stąd też należy powiedzieć, że podatność na zagrożenia cyberterroryzmem stale wzrasta i będzie wzrastać. W celu zrozumienia owej zależności konieczne jest przedstawienie powiązań, jakie występują pomiędzy elementami infrastruktury krytycznej, rozwiązaniami z zakresu technologii informacyjnych, z których korzystają, potencjalnymi zagrożeniami terrorystycznymi oraz ich ewentualnymi skutkami[106]. Uwaga poświęcona zostanie takim systemom, jak:

- system zaopatrzenia w surowce energetyczne, energię oraz paliwa;
- system łączności oraz sieci teleinformatyczne;
- systemy bankowe oraz finansowe;
- systemy zaopatrzenia w żywność oraz wodę;
- systemy zapewniające sprawność funkcjonowania administracji publicznej;
- systemy tworzenia, przechowywania oraz składowania substancji szkodliwych, na przykład chemicznych, łatwopalnych, toksycznych itp.;
- systemy ratownicze oraz ochrony zdrowia;
- systemy transportowe[107].

1.6.4. Czynniki skuteczności ataków cyberterrorystycznych

Pierwszy to anonimowość (a więc bezpieczeństwo własne) sprawców ataku, tym samym bardzo duża trudność wykrycia przygotowywanego ataku przez służby odpowiedzialne za obronę cyberprzestrzeni – czyli tym samym możliwość dokonywania całkowicie nagłych oraz nieprzewidywalnych, a przez to bardzo skutecznych akcji. Ofiary cyberataków są nieświadome zagrożeń, a przez to zupełnie nieprzygotowane do ich odparcia. I zupełnie nieistotne jest przy tym, czy ofiarą jest państwo, organizacja, czy po prostu duża firma – element zaskoczenia pozostaje bowiem taki sam. Brak wiedzy o tym, kto, skąd i dlaczego dokonuje ataku, daje terrorystom możliwość manipulowania informacją, utrudnia ofiarom nie tylko odparcie samego ataku, ale też wprowadzenia działań profilaktycznych, czyli tworzenie skutecznych, systemowych czy międzynarodowych struktur przeciwdziałania.

[106] Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki informacyjne", nr 1-2, 2014, s. 28.
[107] *Ibidem*, s. 28.

Drugim wydaje się bezpieczeństwo osobiste (fizyczne i prawne) terrorystów oraz niski koszt realizacji aktu agresji – w porównaniu z kosztami ataków terrorystycznych, nazwijmy je „analogowymi" wymagających użycia drogiej broni czy technologii, zaangażowania wielu ludzi i rozbudowanej logistyki, skuteczny cyberatak można przeprowadzić z użyciem zwyczajnego komputera biurowego podłączonego do sieci Internet w dowolnym miejscu na świecie. W kontekście zjawiska cyberterroryzmu międzypaństwowego aspekt kosztów odgrywa jeszcze większą rolę, jeśli porównać go z ogromnymi nakładami niezbędnymi do prowadzenia regularnych działań zbrojnych. Hakerzy zaś dokonujący ataku, mogącego doprowadzić do śmierci wielu ludzi, sami pozostają bezpieczni, nie będąc w żaden sposób zagrożonymi bezpośrednimi skutkami swojego działania – ataku w cyberprzestrzeni można dokonać z dowolnego miejsca na ziemi, często odległego o tysiące kilometrów od zaatakowanego obiektu czy systemu.

I ostatni, trzeci, czynnik, to brak możliwości odwetu czy zastosowania sankcji wobec sprawców – w jaki sposób zaatakowany kraj może skutecznie zwalczać sprawców, nie znając często ich miejsca pobytu czy nawet przynależności państwowej? Walka z wirtualnym przeciwnikiem sprowadza się w gruncie rzeczy do próby zabezpieczenia przed kolejnym atakiem, ma więc charakter jedynie defensywny. Trudno wyobrazić sobie walkę z cyberterrorystami atakującymi przez Internet energetyczną infrastrukturę przesyłową czy wytwórczą za pomocą jakichkolwiek konwencjonalnych środków militarnych.

Rozdział II

Polityki ochrony cyberprzestrzeni w Unii Europejskiej

2.1. Zapobieganie terroryzmowi jako element procesu integracji europejskiej w latach 1951-1999

Początki realizacji idei integracji europejskiej w formie unii gospodarczo-politycznej datuje się na lata 50. XX wieku, a za pierwszy dokument odzwierciedlający tendencje zjednoczeniowe państw Europy uznaje się Traktat Paryski z 18 kwietnia 1951 roku. Stanowił o powstaniu Europejskiej Wspólnoty Węgla i Stali[108] jako wspólnego rynku dla przemysłu węglowego i stalowego. Z kolei 25 marca 1957 roku Belgia, Francja, Holandia, Luksemburg, RFN i Włochy podpisały dwa traktaty – o ustanowieniu Europejskiej Wspólnoty Energii Atomowej (Euratom) oraz Europejskiej Wspólnoty Gospodarczej (EWG)[109]. Oba te dokumenty są przykładami integracji sektorowej, z których każdy odnosi się do wybranych dziedzin gospodarki, podporządkowując ich interesom wszystkie inne zagadnienia.

Warto tym samym zwrócić uwagę, że w początkach procesu integracji europejskiej najważniejszymi kwestiami pozostawały stosunki gospodarcze i ekonomiczne. Przed kilka dekad Wspólnota Europejska miała przede wszystkim charakter unii handlowej, a więc współpraca między państwami członkowskimi zorganizowana była jedynie wokół tych zagadnień. Pozostałe kwestie polityczne, w tym aspekty polityki bezpieczeństwa wewnętrznego, nie znajdowały się wówczas w centrum zainteresowania przedstawicieli państw, toteż nie podejmowano w tym kierunku żadnych wspólnych działań. Autorzy traktatu o wprowadzeniu Europejskiej Wspólnoty Gospodarczej podkreślali między innymi „zamiar wprowadzenia podstaw trwałej jedności pomiędzy narodami europejskimi, zapewnienia, że postęp gospodarczy i społeczny zlikwiduje bariery dzielące Europę, oraz podjęcia działań, które doprowadzą do stałego podnoszenia warunków życia oraz pracy obywateli państw członkowskich. Służyć temu miało utworzenie wspólnego rynku i stopniowe ujednolicanie polityki gospodarczej państw członkowskich”[110]. Zgodnie z art. 7a Traktatu EWG (obecnie art. 14 Traktatu WE) rynek wewnętrzny zdefiniowany jest jako „obszar bez granic wewnętrznych, na którym zgodnie z postanowieniami Traktatu zapewniony zostaje swobodny przepływ towarów, osób, usług i kapitału”[111]. Pomimo daleko w

[108] Gelberg L., *Prawo międzynarodowe i historia dyplomacji,* t. III, Warszawa 1960, s. 401–440
[109] Na podstawie art. 8 Traktatu o Unii Europejskiej (Dz.U. 2004 r. Nr 90 poz. 864/30), od dnia1 listopada 1993 r. EWG nosi nazwę „Wspólnoty Europejskiej”. Tym nazewnictwem autor będzie się posługiwał w dalszej części niniejszej pracy.
[110] Madej M., *O koncepcji i praktyce harmonizacji prawa w krajach EWG*, „Państwo i Prawo” 1972, nr 8-9, s. 153 i n.
[111] Lenaerts K., Van Nuffel P., *Podstawy prawa europejskiego*, Warszawa 1998, s. 31

istocie idących założeń traktat nie przewidywał jednak podejmowania jakichkolwiek działań na rzecz przeciwdziałania i zwalczania potencjalnych zagrożeń dla wspólnego rynku wewnętrznego, do których niewątpliwie zaliczyć należało terroryzm. Nie podjęto nawet próby określenia przyszłych, intencjonalnych ram instytucjonalnych dla współpracy w przeciwdziałaniu i zwalczaniu tego rodzaju przestępczości.

Dopiero gwałtowne rozszerzanie się zagrożenia terroryzmem jako problemu międzynarodowego wywołało zmianę w charakterze współpracy krajów członkowskich w ramach UE. Do tego stopnia, że walka z terroryzmem i zapobieganie jego skutków została zaliczona do jednego z głównych zadań procesu integracji europejskiej. „Natężenie zamachów terrorystycznych, także w skali globalnej, jakie miały miejsce pod koniec lat 70. ubiegłego stulecia jednoznacznie rozwiały wątpliwości, że państwa członkowskie są w stanie indywidualnie stawiać czoła tego typu wyzwaniom. Uznano wówczas, że formuła europejskiej integracji może stanowić podstawę do intensyfikacji działań w kontekście zwalczania terroryzmu[112]. Imperatyw na rzecz skoncentrowania sił w przeciwdziałaniu terroryzmowi zaowocował powstaniem form bezpośredniej współpracy w ramach procesów integracyjnych. Należy jednak podkreślić, że pierwsze dokumenty Wspólnot Europejskich stworzone w celu przeciwdziałania i zwalczanie przestępczości, w tym terroryzmu, miały jednak charakter polityczny, bez próby wypracowania przepisów prawnych. W grudniu 1975 roku w Rzymie powołano – w gruncie rzeczy nieformalną – grupę współpracy między ministrami sprawiedliwości i spraw wewnętrznych państw członkowskich Wspólnot Europejskich w zakresie przeciwdziałania i zwalczania zjawiska terroryzmu, radykalizmu, ekstremizmu i przemocy, czyli tak zwaną grupę TREVI (skrót pochodzi od słów: *Terrorisme*, *Radicalisme*, *Extrémisme*, *Violence Internationale*).

2.1.1. Inicjatywa TREVI

Działalność grupy Trevi była oparta na konsultacjach między rządami krajów WE, a inicjatorów, decyzje i postanowienia przyjmowano w drodze konsensu. Trevi funkcjonowała w oparciu o trzy poziomy: ministrowie spraw wewnętrznych i sprawiedliwości (*Ministers*), wyżsi urzędnicy (*Trevi Senior Officials*), Trojka i grupy robocze (*Trevi troika*). Inicjatywa ta opierała się na okresowych spotkaniach, których celem było omawianie problematyki zagrożeń dla

[112] Gancarz G., Podstawy współpracy z zakresie zwalczania terroryzmu w prawie Unii Europejskiej, Warszawa 2008, s. 2.

bezpieczeństwa państw, w tym także terroryzm. „Z czasem wykształciła ona własne struktury robocze, podgrupy, z których jedna bezpośrednio zajmowała się tematyką terroryzmu (tzw. TREVI I). Jednym z najważniejszych zadań stało się wspólne i regularne analizowanie zewnętrznych i wewnętrznych zagrożeń terroryzmem, wypracowanie jednolitej strategii działań w zwalczaniu grup terrorystycznych oraz umożliwienie państwom-członkom UE współpracy w przeciwstawianiu się zagrożeniom”[113].

Grupa TREVI nie była w żaden sposób powiązana z instytucjami europejskimi, a tym bardziej z Komisją oraz Parlamentem Europejskim, za czym zresztą szczególnie optowała Wielka Brytania. Z uwagi jednak na poziom reprezentacji poszczególnych państw rozpoczęły się działania nieformalne między Wspólnotami i Grupą TREVI. TREVI 1 rozpoczęła działalność 31 maja 1977 roku i była najaktywniejszą z grup roboczych oraz – co istotne – posiadała uprawnienia operacyjne. „Do jej zadań należała realizacja następujących zobowiązań: wymiana doświadczeń odnośnie walki z terroryzmem, wymiana informacji pomiędzy państwami członkowskimi o podjętych decyzjach dotyczących aktów terroru, powołanie jednostek odpowiedzialnych za współpracę w zwalczaniu terroryzmu międzynarodowego. Celem grupy było analizowanie ewentualnych zagrożeń terrorystycznych, zarówno na obszarze Wspólnot, jak i poza ich granicami. Grupa miała też wypracować wspólną strategię zwalczania tego zjawiska oraz doprowadzić do ułatwienia współpracy pomiędzy państwami członkowskimi w celu przeciwstawienia się wszelkim aktom terroru”[114].

Prace Grupy TREVI zakończyły się wraz z wejściem w życie traktatu z Maastricht. Co warte jednak podkreślenia, jej wieloletni dorobek, zwłaszcza w sferze koncepcji wypracowujących zasady współpracy w zakresie zwalczania terroryzmu, stał się podstawą dla dalszych prac programowych i legislacyjnych w ramach wspólnoty.

2.1.2. Układ z Schengen

Układ z Schengen z 1985 roku można określić jako kolejny z kamieni milowych przybliżających struktury wspólnotowe do współczesnego kształtu dokumentów strategicznych dotyczących zabezpieczenia przed terroryzmem oraz – niejako wynikowo – cyberterroryzmem.

[113] W 1989 r. została zastąpiona przez mechanizm przewodnictwa, sk³adaj¹cy siê z obecnego przewodnicz¹cego, dwóch poprzednich i dwóch przysz³ych; J. D. Occhipinti, *The Politics of EU Police Cooperation. Toward a European FBI?*, London 2003, s. 32. Przypis podany za : Wojnicz L., *Nieformalne struktury państw Unii Europejskiej w walce z międzynarodowym terroryzmem. Bilans współpracy i wyzwania,* Szczecin 2007, s. 46.

[114] Wawrzyk P., *Polityka Unii Europejskiej w obszarze spraw wewnętrznych i wymiaru sprawiedliwości*, Warszawa 2007, s. 32.

Należy jednakże pamiętać, że współpraca w ramach Schengen ograniczona była tylko do pięciu państw członkowskich, co nie pozostawało bez wpływu na skuteczność jej działania. Z jednej strony ograniczenie do kilku państw-sygnatariuszy znacząco hamowało zasięg działania układu, z drugiej jednak – w tak kameralnym zespole łatwiej i szybciej można było podjąć decyzje. „W ramach działań podjętych przez państwa członkowskie nacisk położono głównie na wzmocnienia kontroli na granicach zewnętrznych. Konsekwencjami tych działań były zwiększone możliwości przeciwdziałania takim zagrożeniom, jak: nielegalna migracja, przestępczość zorganizowana oraz terroryzm. Rozwiązania wypracowane w ramach Układu z Schengen posłużyły w przyszłości do zacieśnienia operacyjnej współpracy transgranicznej, co miało niewątpliwy wpływ na zapobieganie i zwalczanie terroryzmu”[115].

2.1.3. Traktat z Maastricht

Wspomniano wyżej, że zarówno Grupa TREVI, jak i układ z Schengen nie zostały formalnie ujęte w ramy współpracy z instytucjami europejskimi, takimi jak Komisja i Parlament Europejski. Więcej, nie były też w żaden sposób uzupełniane przez przepisy prawne krajów-sygnatariuszy, tym samym działały one niejako poza strukturami instytucjonalnymi Wspólnot Europejskich, co uległo zmianie dopiero w roku 1992, po zawarciu traktatu z Maastricht i utworzeniu Unii Europejskiej. Traktat o Unii Europejskiej doprowadził do inkorporacji dotychczasowych ustaleń nieformalnych grup do III filaru UE – stosowne przepisy zawarto w art. 29 TUE. Na jego mocy przedmiotem „wspólnego zainteresowania” państw członkowskich stała się: współpraca Policji w celach prewencyjnych i w walce z terroryzmem, nielegalnym handlem narkotykami oraz innymi poważnymi formami przestępczości międzynarodowej. Po raz pierwszy prawo traktatowe uczyniło z terroryzmu przedmiot współpracy państw członkowskich w ramach nowoutworzonej Unii Europejskiej. Podjęto m.in. działania zmierzające do wzmocnienia współpracy celnej oraz obejmujące całą Unię ujednolicenie systemu wymiany informacji w ramach Europejskiego Urzędu Policji. […] Problematyka terroryzmu została ujęta przede wszystkim w ramach współpracy policyjnej i sądowej w sprawach karnych. Artykuł 29 TUE stanowi, iż budowa obszaru wolności, bezpieczeństwa i sprawiedliwości powinna się odbywać przez zapobieganie przestępczości zorganizowanej lub innym formom przestępczości, w

[115] Jasiński F., Narojek M., Rakowski P., *Wewnętrzne i zewnętrzne aspekty współpracy antyterrorystycznej w Unii Europejskiej w kontekście Polski, jako państwa członkowskiego*, Centrum Europejskie – Natolin, Warszawa 2006, s. 10-11.

szczególności poprzez walkę z terroryzmem, handlem ludźmi i przestępstwami przeciwko dzieciom, handlem środkami odurzającymi, substancjami psychotropowymi i bronią oraz korupcją i nadużyciami finansowymi[116]. W traktacie z Maastricht przyjęto też wspólne propozycje związane z planem stworzenia i utrzymywania rejestru wyspecjalizowanych antyterrorystycznych kompetencji, umiejętności i wiedzy eksperckiej w celu ułatwienia współpracy antyterrorystycznej między państwami UE. „Każde państwo członkowskie sprawujące przewodnictwo w Unii miało być odpowiedzialne za kompletowanie, prowadzenie i upowszechnianie wspomnianego rejestru. Warto przypomnieć, że powyższe rozwiązania wynikają z podstaw ogólniejszych zawartych np. w art. J.4, w którymi stwierdza się, iż: „Wspólna polityka zagraniczna wspólna polityka bezpieczeństwa obejmuje wszystkie te kwestie, które są związane z bezpieczeństwem Unii"[117].

Warte uwagi są zwłaszcza zapisy art. 2 ust. 1 Konwencji o Europolu[118]. Ustalono w nim, że jednym z najważniejszych celów tej organizacji jest „doskonalenie i wzmocnienie efektywności działania oraz wsparcie instytucji odpowiedzialnych w państwach UE za zapobieganie i walkę z terroryzmem"[119]. Ponadto na Europol nałożono obowiązek zajmowania się „przestępstwami, jakie zostały lub mogą zostać popełnione w trakcie działań terrorystycznych wobec życia, zdrowia, wolności osobistej lub majątku"[120].

W 1996 roku powołano Europejski Komitet do spraw Przestępczości, który zaproponował Komisji utworzenie w swoich ramach komitetu ekspertów do spraw cyberprzestępczości. Miało to związek z przyjęciem przez PE tak zwanego Raportu Kaspersena, który sugerował wypracowanie wspólnego dla państw UE dokumentu strategicznego dotyczącego zagrożeń bezpieczeństwa cyberprzestrzeni[121]. W konsekwencji 4 lutego 1997 roku powołano Komitet Ekspertów do spraw Przestępczości w Cyberprzestrzeni *(Committee of Experts on Crime in Cyber-space*).

[116] Gancarz G., *op. cit., s. 4.*
[117] Krajski S., *Traktat z Maastricht. Wstęp i komentarz.* Warszawa 1998. s. 25
[118] *Artykuł K.3 Traktatu o Unii Europejskiej w sprawie ustanowienia Europejskiego Urzędu Policji (Konwencja o Europolu)*, Bruksela, 26 lipca 1995 r. Dz. U. z 2005, Nr 29, poz. 243.
[119] *Ibidem*
[120] *Ibidem*
[121] Więcej na temat raportu H.W.K. Kaspersena w publikacji: Targalski R., *Konwencja o cyberprzestępczości*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009, s. 208.

2.1.4. Traktat z Amsterdamu i Szczyt Rady Europejskiej w Tampere

Traktat amsterdamski zawarto 2 października 1997 roku i według powszechnej wśród badaczy opinii, nie zreformował on w zasadniczy sposób zadań Unii Europejskiej w zakresie zapobiegania terroryzmowi i cyberprzestępczości. Niemniej jednak warto zauważyć, że został on podpisany przez piętnaście państw członkowskich, jak i deklaratywnie rozszerzył także i pogłębił proces tworzenia „obszaru pozbawionego wewnętrznych granic". Jedną z najważniejszych zmian w traktacie amsterdamskim było zatem zintegrowanie dotychczasowych efektów współpracy w ramach Schengen ze strukturami Unii Europejskiej. Choć postanowienia z Amsterdamu miały wejść w życie dopiero w roku 1999, to już 15 grudnia 1997 roku Parlament Europejski i Rada UE wydały dyrektywę w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym[122]. Co prawda w roku 2002 została ona zastąpiona już nowym aktem prawnym uwzględniającym dominujące trendy zarówno digitalizacji, jak i zwiększanie mobilności użytkowników sieci teleinformatycznych oraz zwiększenie się ilości dostępnych usług opartych o przetwarzanie danych o użytkownikach za pomocą komunikacji elektronicznej[123], niemniej jednak należy uznać za niewątpliwie istotne zasygnalizowanie w tym dokumencie wiedzy o obecnym w cyberprzestrzeni nowym typie zagrożeń terrorystycznych. „W ramach III filaru określono ponadto odpowiednie ramy instytucjonalne, tj. Komitet Koordynujący, trzy Grupy Sterujące oraz wiele hierarchicznie uporządkowanych grup roboczych, składających się z ekspertów krajów członkowskich. Grupa Sterująca II, po utworzeniu Europolu, przejęła kompetencje TREVI. Podczas szczytu w Amsterdamie przyjęto ponadto Plan UE działania na rzecz zwalczania przestępczości zorganizowanej"[124].

Wzmocnieniem zmian wprowadzonych przez Traktat z Amsterdamu oraz potwierdzeniem kierunku współpracy państw członkowskich UE były konkluzje przyjęte podczas szczytu Rady Europejskiej w Tampere w październiku 1999 roku. „Problem skutecznej prewencji, współpracy właściwych organów oraz walki z terroryzmem został wprawdzie ogólnie zawarty w ramach głównego celu UE, jakim jest budowa obszaru wolności, bezpieczeństwa i sprawiedliwości w ramach granic Unii. Wskazano m.in. na konieczność zapewnienia lepszej koordynacji działań, znaczenie walki z finansowaniem terroryzmu, wzmocnienie współpracy z

[122] *Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym.*
[123] *Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej.*
[124] Mierzejewski D.J., *Bezpieczeństwo Europejskie w warunkach przemian globalizacyjnych*, Toruń 2011, s. 168-169.

Europolem, przeciwdziałanie terroryzmowi internetowemu oraz koncentrację prac Grupy Roboczej ds. Terroryzmu na kwestii opisywania aktów terrorystycznych w krajach unijnych”[125]. Odwołania do terroryzmu i cyberterroryzmu międzynarodowego zostały także ogólnie wspomniane w postanowieniach dotyczących Wspólnej Polityki Zagranicznej i Bezpieczeństwa. Uznano między innymi za konieczne „zapewnienie szeroko rozumianego bezpieczeństwa zarówno w kontekście zagrożeń międzynarodowych, jak i współpracy międzynarodowej w tym zakresie”[126].

Za bezpośredni efekt prac szczytu w Tampere dla polityki cyberbezpieczeństwa UE należy uznać rezolucję nr 3, przyjętą w Londynie na XXIII Konferencji Europejskiego Komitetu ds. Przestępczości, w dniach 8-9 czerwca 2000 roku. Zdecydowanie podkreślono w niej konieczność stworzenia efektywnego systemu współpracy międzynarodowej w zakresie walki z cyberprzestępczością.

2.2. Unia Europejska a zwalczanie terroryzmu i cyberterroryzmu w latach 2001-2015

2.2.1. Reakcje UE na zamach z 11 września 2001 roku

Na nadzwyczajnym posiedzeniu Rady Europejskiej 21 września 2001 roku, zwołanym w reakcji na zamachy z 11 września przyjęto postulat, iż walka z terroryzmem staje się jednym z najważniejszych celów UE, zaś deklarację tę ujęto w formę „Planu działania w zakresie zwalczania terroryzmu”[127]. „Rada postulowała o konieczności wzmocnienia współpracy policyjnej i sądowej w tym zakresie oraz wsparcia działań zapewniających większe bezpieczeństwo transportowi lotniczemu, także za pomocą instrumentów Wspólnej Polityki Zagranicznej i Bezpieczeństwa. Podkreślono również, że wojskowa interwencja Stanów Zjednoczonych przeciw państwom, które wsparły terrorystów dokonujących zamachów, jest – na mocy Rezolucji Narodów Zjednoczonych 1368 – prawnie dopuszczalna”[128]. Podczas szczytu w Laeken, w grudniu 2001 roku, wypracowano porozumienie w zakresie stworzenia podstaw prawnych do funkcjonowania europejskiego nakazu aresztowania oraz powoływania wspólnych grup dochodzeniowych. Wprowadzono też europejską listę osób i organizacji związanych z działalnością terrorystyczną, w stosunku do których uprawnione stały się działania prewencyjne.

[125] Jasiński F., Narojek M., Rakowski P., *op. cit.*, s. 19.
[126] *Ibidem.*
[127] *Dokument Rady SN 140/01*
[128] Gancarz G., *op. cit.,* s. 5.

2.2.2. Konwencja Rady Europy o cyberprzestępczości (*The Council of Europe Convention on Cybercrime*) [129]

Przyjęta w Budapeszcie 23 listopada 2001 roku ma charakter umowy o charakterze międzynarodowym i stanowi przełomowy dokument w zakresie zapewnienia ochrony cyberprzestrzeni przed atakami cyberprzestępczymi i cyberterrorystycznymi. „Utworzony w lutym 1997 roku Komitet Ekspertów ds. Przestępczości w Cyberprzestrzeni (*Commitee of Experts on Crime in Cyberspace, PC-CY*) wynegocjował i opracował w ciągu następnych czterech lat projekt konwencji. W pracach nad jej ostatecznym tekstem, obok państw członkowskich Rady Europy, uczestniczyły Japonia, Kanada, Republika Południowej Afryki oraz Stany Zjednoczone. Szczególnie USA, ze względu na największe doświadczenie w regulowanym temacie, miały istotny wpływ na ostateczny kształt dokumentu.

Końcowa, dwudziesta siódma z kolei, wersja Konwencji została zatwierdzona przez CDPC w czerwcu 2001 roku, a niecałe pół roku później przyjęta przez Komitet Ministrów”[130]. Główny cel Konwencji zawarto w jej preambule, a jest nim „ochrona społeczeństwa przed cyberprzestępczością”, poprzez uznanie „działań skierowanych przeciwko poufności, integralności i dostępności systemów informatycznych, sieci i danych informatycznych, jak również nieprawidłowego wykorzystania tych systemów, sieci i danych [...] za przestępstwo, a także przyjęcie środków, które będą przydatne w skutecznym zwalczaniu takich przestępstw, poprzez ułatwienie ich wykrywania, prowadzenia dochodzenia i ścigania zarówno na szczeblu krajowym, jak i międzynarodowym oraz poprzez przyjęcie rozwiązań sprzyjających szybkiej i rzetelnej współpracy międzynarodowej”[131]. „Aby działania takie były skuteczne, niezbędne było przyjęcie odpowiednich przepisów prawnych, które miały opierać się na międzynarodowej współpracy. Współpraca taka powinna odbywać się nie tylko pomiędzy poszczególnymi państwami, ale również pomiędzy prywatnymi przedsiębiorstwami i organizacjami”[132].

Pomimo jasno sprecyzowanego celu, którym jest skuteczne zapobieganie cyberprzestępczości, w Konwencji podkreślono stanowczo podkreślono wagę zachowania balansu pomiędzy instrumentami prawnymi chroniącymi przed cyberprzestępczością, a ochroną podstawowych praw człowieka. Jak podaje Jędrzej Skrzypczak „w szczególności wyrażono

[129] *Konwencja Rady Europy o Cyberprzestępczości z 23 listopada 2001 r. dziennikustaw.gov.pl/du/2015/728*.
[130] Dziwisz D., *Stany Zjednoczone a międzynarodowe bezpieczeństwo cybernetyczne*, Kraków 2015, s. 167
[131] *Ibidem*.
[132] Ciekanowski Z., Rejman K., Wyrębek M., *Cyberterroryzm jako współczesna broń masowego rażenia*, MMR, vol. XXIII, (1/2018), pp. 37-49, Biała Podlaska 2018, s. 43-44.

przekonanie, że należy chronić wartości i dobra strzeżone na mocy Konwencji Rady Europy z 1950 roku o ochronie praw człowieka i podstawowych wolności[133] oraz Międzynarodowym Paktem Narodów Zjednoczonych z 1966 roku o prawach obywatelskich i politycznych[134]. W szczególności chodzi o prawo każdej jednostki do posiadania własnych wolnych opinii, jak również prawo do wolności wypowiedzi, łącznie z wolnością poszukiwania, uzyskiwania i dzielenia się wszelkiego rodzaju informacjami i ideami, bez względu na granice oraz prawo do poszanowania prywatności." [135]

Konwencja składa się z trzech rozdziałów, z których pierwszy – będący przeglądem najważniejszych definicji – nie wymaga omówienia w tej pracy. Rozdział drugi jest zestawieniem propozycji środków prawnych, których celem jest zapobieganie cyberprzestępczości i cyberterroryzmowi. Przedstawiono w nim katalog przestępstw w cyberprzestrzeni, które powinny znaleźć się w narodowych kodeksach karnych krajów członkowskich, wśród nich:

- „przestępstwa przeciwko poufności, dostępności i integralności systemów i danych informatycznych, czyli nielegalny dostęp i przechwytywanie danych, jak również naruszenie ich integralności i integralności systemu;
- przestępstwa komputerowe, do których zalicza się: fałszerstwa i oszustwa komputerowe;
- przestępstwa związane z charakterem informacji, to między innymi działania związane z pornografią dziecięcą;
- przestępstwa związane z naruszeniem praw autorskich i pokrewnych"[136].

W myśl zapisów Konwencji każdy z krajów członkowskich UE powinien do swojego prawa wprowadzić takie regulacje prawne, które mogą umożliwić gromadzenie i rejestrowanie danych przez odpowiednie instytucje państwowe oraz nakazać dostawcom usług teleinformatycznych ich rejestrację i gromadzenie. Dodatkowo do krajowego prawa państw-sygnatariuszy należy wprowadzić takie środki prawne, które pozwolą odpowiednim organom na przechwytywanie w czasie rzeczywistym danych, szczególnie tych, których treści uważane są za niebezpieczne lub niezgodne z prawem[137].

---

[133] *Konwencja o ochronie praw człowieka i podstawowych wolności,* Rzym, 4 listopada 1950 r., (Dz. U. 1993, Nr 61, poz. 264, z późn. zm.).
[134] *Międzynarodowy Pakt Praw Obywatelskich i Politycznych,* Nowy Jork ,19 grudnia 1966 r. (Dz. U. 1977, Nr 38, poz. 167).
[135] Skrzypczak J., *Bezpieczeństwo teleinformatyczne w świetle Europejskiej Konwencji o Cyberprzestępczości*, [w:] „Przegląd Strategiczny" nr 1, Poznań 2011, s. 52.
[136] *Konwencja Rady Europy o Cyberprzestępczości* z 23 listopada 2001 *r., art. 16–17.*
[137] Warto dodać, iż uzupełnienie Konwencji stanowi dokument, który uzyskał moc prawną dopiero w marcu 2006 roku. Jest to *Protokół w sprawie kryminalizacji aktów o naturze rasistowskiej lub ksenofobicznej popełnianych z wykorzystaniem systemów komputerowych,* w którym zdefiniowano materiały o charakterze rasistowskim i ksenofobicznym w cyberprzestrzeni, i wzywa się państwa-strony do ich kryminalizacji. W pierwotnej wersji projektu ta problematyka miała zostać włączona do treści Konwencji, jednakże w opinii Departamentu Sprawiedliwości USA

Współpracę międzynarodowa w ramach Konwencji Rady Europy o cyberprzestępczości należy oceniać w sposób wyważony. Została ona ratyfikowana tylko przez trzydzieści dziewięć państw, co z uwagi na jej – według intencje autorów – globalny charakter stanowi dużą przeszkodę w zakresie jej funkcjonowania[138]. Polska należy do tych krajów europejskich, które (wespół z Czechami i Szwecją) jedynie Konwencję podpisały, jednak nie przeprowadziły jej ratyfikacji. Wynikać to może z faktu, iż Polska, będąca członkiem UE dopiero do maja 2004 roku, jak i wiele innych państw poszerzonej EU, nie uczestniczyła w opracowaniu jej treści. Nieprzynależność członkowska nie powinna jednak stanowić istotnej przeszkody w ewentualnej chęci włączenia większej liczby krajów do prac nad dokumentem – tym bardziej jeśli mowa o państwach starających się o przyjęcie do Unii w stosunkowo niedługim czasie. Podobnie Rosja oraz Chiny nie są sygnatariuszami Konwencji, i tymczasem to te właśnie państwa przodują, jeśli chodzi o liczbę ataków cybernetycznych, na inne kraje. Powody, dla których Chiny oficjalnie nie przystąpiły do ratyfikacji, nie są znane opinii publicznej, natomiast Rosja podniosła kwestię zapisu w artykule 32 punkt b, który mówi, iż: „Strona, bez zezwolenia drugiej Strony, może uzyskać dostęp lub otrzymać za pomocą systemu informatycznego znajdującego się na własnym terytorium dane informatyczne przechowywane na terytorium innego państwa, jeżeli Strona uzyska prawnie skuteczną i dobrowolną zgodę osoby upoważnionej do ujawnienia Stronie tych danych za pomocą tego systemu informatycznego”[139]. „[Zapis ten] uderza w suwerenność i bezpieczeństwo państw członkowskich oraz prawa obywateli tych państw”[140] – w ten właśnie sposób Władimir Putin uzasadnił odmowę ratyfikacji Konwencji. Abstrahując od kwestii, że zastrzeżenie to wydaje się w pewnym stopniu zasadne, można jedynie domniemywać, że rządowi Rosji nie zależy na udziale w międzynarodowym porozumieniu dotyczącym cyberbezpieczeństwa. Kraj ten zajmuje wszak pierwsze miejsce na liście państw-cyberagresorów, a z jego terenu wychodzi największa liczba ataków cyberterrorystycznych. *Casus* Rosji i Chin obnaża niejako słabość całego przedsięwzięcia, a wiąże się on ze stosunkowo niewielką liczbą państw-ratyfikatorów; „kraje uczestniczące w procesie przygotowania Konwencji nie są

„stałoby to w sprzeczności z wolnością wyrażania się zagwarantowaną w Pierwszej Poprawce do Konstytucji” 473. USA ostatecznie nie podpisały tego dokumentu i jest on ratyfikowany jedynie przez dwadzieścia państw.

[138] Duża zmiana w tej kwestii nastąpiła dopiero w roku 2012 – Konwencję ratyfikowało wówczas sześć kolejnych państw: Australia, Austria, Belgia, Gruzja, Japonia i Malta, a w 2013 dołączyła do nich Dominikana. W lutym 2013 roku pięćdziesiąt siedem państw było stronami, sygnatariuszami albo zostało zaproszonych do przystąpienia do Konwencji. Informacja podana [za:] *Cooperation Against Cybercrime: Progress Made in 2012 A Brief Review of Council of Europe Activities*, Rada Europyhttp://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Docs2013/cyber%20AS%20re-view2012_flyer_v6.pdf, [dostęp: 12.02.2019]

[139] *Konwencja Rady Europy o Cyberprzestępczości z 23 listopada 2001 r. dziennikustaw.gov.pl/du/2015/728, s.65,* [dostęp: 12.02.2019]

[140] *Putin defies Convention on Cybercrime*, http://eng.cnews.ru/news/top/indexEn.shtml?2008/03/27/293913, [dostęp: 12.02.2019]

największym zagrożeniem cybernetycznym, gdzie hakerzy działają swobodnie i bez żadnych ograniczeń. Zazwyczaj ataki dokonywane są z serwerów umieszczonych na terytorium państw, które nie są i prawdopodobnie nie będą stronami Konwencji"[141]. Wypada tym samym zgodzić się z wnioskiem Agnieszki Bógdał-Brzezińskiej i Marcina Gawryckiego, iż „Konwencja Rady Europy o cyberprzestępczości może stanowić modelowe rozwiązanie legislacyjne w państwach wysoko rozwiniętych, ale nie powinna służyć za przykład dla krajów rozwijających się"[142].

Sam przebieg prac nad założeniami Konwencji także wzbudził wiele kontrowersji, zwłaszcza wśród organizacji pozarządowych, które choć formalnie zostały zaproszone przez Radę Europy do udziału w dialogu i konsultacjach, to w praktyce prawie wszystkie ich wnioski i propozycje zostały zignorowane. Proces opracowywania nie był zdaniem wielu obserwatorów dostępny i otwarty, nie można go uznać za przejrzysty – a właśnie obie wartości: transparentność i dialog deklarowała RE, przystępując do prac. Również ochrona praw podstawowych, w tym prawa do prywatności, zdaniem wielu znawców tematu[143], nie jest w Konwencji nie tyle nieprzestrzegana, co raczej nieuwzględniona w żadnym z zapisów. W związku z tym dokument ten postrzegany jest jako kompromis pomiędzy ochroną praw człowieka a walką z cyberprzestępczością, stanowiąc niesatysfakcjonujący nikogo kompromis. „[…] *American Civil Liberties Union* (ACLU) obawia się, że Konwencja może być nadużywana przez władze USA do inwigilacji i działań zakazanych aktualnym prawem amerykańskim".

Z kolei waszyngtońskie „*Center for Democracy and Technology* (CDT) jeszcze przed przyjęciem Konwencji sprzeciwiło się wielu jej zapisom, w tym przede wszystkim wymogom odnośnie dostawców Internetu przechowywania zapisów aktywności ich klientów. W petycji do sekretarza generalnego Rady Europy Waltera Schwimmera w ostrym tonie skomentowano, że podobne rozwiązania jak te z artykułów 17, 18, 24, 25 Konwencji wykorzystywano w przeszłości, aby identyfikować dysydentów i prześladować mniejszości […]"[144]. Zapisom Konwencji stawiano także zarzut arbitralnego rozszerzenia katalogu czynów uznanych za przestępstwo, co sprawia, iż działania w cyberprzestrzeni, do tej pory uznawane za legalne, stają się sprzeczne z prawem – dotyczy to zwłaszcza artykułu 10, tj. kwestii związanych z prawem autorskim oraz

[141] Dziwisz D., *op. cit.*, s. 174
[142] Bógdał-Brzezińska A., Gawrycki M. F., *Cyberterroryzm i problemy bezpieczeństwa...*, *op. cit.*, s. 243
[143] Por: M.A. Vatis, *The Council of Europe Convention on Cybercrime*, [w:] *Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy*, National Research Council, Waszyngton, DC, 2010, s. 218. [oraz:] Dziwisz D., *op. cit.*, s. 174, [oraz:] Głowacka D, *Konwencja o cyberprzestępczości...*, *op. cit. s. 201*.
[144] Dziwisz D., *op. cit.*, s. 176

ochroną praw człowieka – artykuł 14[145]. Kwestią sporną pozostawała też skuteczność procedur jurysdykcji. Przyjęto bowiem zasadę odpowiedzialności określanej terytorialnie, nie uwzględniając oczywistej eksterytorialności – czy może raczej „wszechterytorialności" – Internetu.

Jednakże nawet uwzględniając przywołane zastrzeżenia, Konwencję Rady Europy o cyberprzestępczości należy uznać zarówno za prekursorskie, jak i raczej skuteczne narzędzie do ochrony bezpieczeństwa cyberprzestrzeni oraz do walki z cyberterroryzmem. Konwencja jest bowiem cały czas udoskonalana i aktualizowana, a jej zapisy poddawane rewizji i uzupełniane o wyniki doświadczeń kilkunastu już lat funkcjonowania. Przykładem może być przyjęcie *Strategii Regulacyjnej RE dotyczącej Internetu na lata 2012–2015*[146]*,* w której poddano analizie kwestie ujednolicania prawa na poziomie globalnym i propagowanie Konwencji jako standardu odniesienia dla rozwoju coraz skuteczniejszej współpracy w zwalczaniu cyberprzestępczości[147].

2.2.3. Europejska Strategia Bezpieczeństwa *(European Security Strategy)*

W lipcu 2003 roku Parlament Europejski przyjął dokument strategiczny precyzujący zakres zainteresowania Agend UE kwestiami bezpieczeństwa międzynarodowego, czyli Europejską Strategię Bezpieczeństwa – Bezpieczna Europa w Lepszym Świecie[148]. „We wprowadzeniu do tego dokumentu zauważono, że podstawą europejskiej integracji i bezpieczeństwa jest sojusz Europy ze Stanami Zjednoczonymi Ameryki i stabilizująca dla pokoju w Europie rola Paktu Północnego Atlantyku. Stwierdzono, że wspólnota jako związek 25 krajów, które zamieszkuje ponad 450 milionów ludzi, powinna mieć decydujący głos w sprawach bezpieczeństwa Starego Kontynentu i suwerennie wpływać na bezpieczeństwo globalne"[149].

Strategia sformułowała i przyjęła trzy cele strategiczne, których osiągnięcie określono jako niezbędne dla zbudowania trwałego i stabilnego poziomu bezpieczeństwa krajów wspólnoty:

---

[145] *Konwencja Rady Europy o Cyberprzestępczości z 23 listopada 2001 r. dziennikustaw.gov.pl/du/2015/728, s.22-25*, [dostęp: 14.02.2019]

[146] *Internet Governance – Council of Europe Strategy 2012–2015*, Rada Europy, https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282011%29175&Language=lanEnglish&Ver=final&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383, [dostęp: 14.02.2019]

[147] Powołano w tym celu Cybercrime Convention Committee, dokonał oceny implementacji wybranych postanowień Konwencji w systemach prawnych krajów członkowskich. W pierwszej kolejności ocenie poddano realizację tzw. „niezwłocznych zabezpieczeń" (*expedited preservations*) z artykułu 16 (*Niezwłoczne zabezpieczanie przechowywanych danych informatycznych*), artykułu 17 (*Niezwłoczne zabezpieczanie i częściowe ujawnianie danych dotyczących ruchu*), artykułu 29 (*Wzajemna pomoc w niezwłocznym zabezpieczaniu przechowywanych danych informatycznych*) oraz artykułu 30 Konwencji (*Wzajemna pomoc w niezwłocznym ujawnianiu przechowywanych danych*. Informacja podana za: Dziwisz D., *op. cit.*, s. 178

[148] *Bezpieczna Europa w Lepszym Świecie – Europejska Strategia Bezpieczeństwa z dnia 12 grudnia 2003 r.*, http://www.bbn.gov.pl/ftp/dok/01/strategia_bezpieczenstwa_ue_2003.pdf

[149] Mierzejewski D.J., *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych, Toruń 2011, s. 192.*

- Cel 1 – „ciągłe monitorowanie, przewidywanie i natychmiastowe przeciwdziałanie zagrożeniom bezpieczeństwa, głównie terroryzmowi, rozprzestrzenianiu broni masowego rażenia i konfliktom regionalnym […]. Do realizacji tego celu powinno być zaangażowane całe instrumentarium, jakie posiadają państwa i wspólnota, zarówno wojskowe, jak i cywilne".
- Cel 2 – „wspieranie demokracji w krajach europejskich i na świecie jako gwaranta bezpieczeństwa wewnętrznego i międzynarodowego […)".
- Cel 3 – „rozwój integracji na płaszczyźnie politycznej, gospodarczej, kulturowej i militarnej, stabilizujący i zwiększający bezpieczeństwo europejskie"[150].

Parlament Europejski wraz z Radą Unii Europejskiej powołały też pierwszy wspólnotowy wyspecjalizowany organ powołany do ochrony cyberprzestrzeni i zwalczania zagrożeń cybernetycznych – Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (*European Network and Information Security Agency* – ENISA). Zadania ENISY nie miały charakteru operacyjnego czy śledczego, raczej ograniczały się do realizacji prac analitycznych, naukowo-badawczych oraz – w późniejszym okresie – szkoleniowych. Ponadto, jak zauważa Marta Stępień, „w tym czasie, pomimo powołania wyspecjalizowanej Agencji państwa członkowskie nie dostrzegały jeszcze wzrostu liczby wyzwań i zagrożeń w tej dziedzinie, a plany stworzenia wspólnej strategii ochrony cyberprzestrzeni były odległe"[151].

Na marginesie warto dodać – wyprzedzając nieco chronologię narracji – że powołana wiele lat później, we wrześniu 2017 roku, Europejska Agencja ds. Bezpieczeństwa Cybernetycznego była w praktyce rozwinięciem i wyposażeniem w szersze prerogatywy Agencji ENISA. Powstanie Europejskiej Agencji ds. Bezpieczeństwa Cybernetycznego miało przyczynić się do usprawnienia gotowości UE do reagowania na ataki przez organizowanie corocznych ogólnoeuropejskich ćwiczeń antycyberterrorystycznych oraz zapewnienie lepszej wymiany danych wywiadowczych o zagrożeniach i wiedzy na ten temat dzięki stworzeniu ośrodków wymiany informacji i analiz. Jej zadaniem było też centralne wsparcie krajów wspólnoty w proces wdrażania dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych, która nakłada na władze krajowe obowiązki sprawozdawcze w przypadku poważnych incydentów.

[150] *Ibidem,* s. 193-194.
[151] Stępień M., *Ochrona cyberprzestrzeni Rzeczypospolitej Polskiej a współpraca państw członkowskich Unii Europejskiej*, Siedlce 2017.

W komunikacie o powołaniu ENISA napisano: „Agencja bezpieczeństwa cybernetycznego powinna również pomóc ustanowić i wdrożyć ogólnounijne ramy certyfikacji, których wprowadzenie Komisja proponuje, aby zapewnić cyberbezpieczeństwo produktów i usług. Nowe europejskie certyfikaty cyberbezpieczeństwa zapewnią niezawodność miliardów urządzeń służących funkcjonowaniu istniejącej infrastruktury krytycznej, takiej jak sieci transportowe i energetyczne, jak również nowych urządzeń przeznaczonych dla konsumentów, takich jak samochody podłączone do sieci. Certyfikaty bezpieczeństwa cybernetycznego będą uznawane we wszystkich państwach członkowskich, a co za tym idzie – zmniejszą obciążenia administracyjne i koszty dla przedsiębiorstw […]”[152].

O Agencji tej mowa jest tu nieprzypadkowo w czasie przeszłym, ponieważ w grudniu 2018 roku Parlament Europejski, Rada i Komisja Europejska osiągnęły porozumienie dotyczące nowego aktu w sprawie cyberbezpieczeństwa, który wzmacnia mandat Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji – czyli ENISA. Propozycje uwzględnione w nowym Porozumieniu obejmują: „stały mandat agencji UE ds. cyberbezpieczeństwa (ENISA) w celu zastąpienia jej ograniczonego mandatu, który upłynąłby w 2020 r., oraz przydzielenie tej agencji większej ilości środków, aby umożliwić jej realizację celów, oraz solidniejszą podstawę dla działalności ENISA w perspektywie nowych ram certyfikacji cyberbezpieczeństwa, aby pomóc państwom członkowskim w skutecznym reagowaniu na cyberataki dzięki większej roli agencji we współpracy i koordynacji na szczeblu Unii”[153]. W dokumencie tym jednak próżno szukać wzmianki o Europejskiej Agencji ds. Bezpieczeństwa Cybernetycznego, choć jej zadania praktycznie pokrywają się obecnie z zakresem odpowiedzialności Agencji ENISA.

2.2.4. Decyzja Ramowa w sprawie ataków na systemy informatyczne *(Council Framework Decision of 24 February 2005 on attacks against information systems)*

W latach 2004-2005 zaobserwować można znaczne przyspieszenie prac nad wspólnotowymi dokumentami dotyczącymi zapobiegania i zwalczania cyberterroryzmu oraz ogólnie rozumianego bezpieczeństwa w cyberprzestrzeni. Szybciej zaczęły postępować też prace przygotowawcze w parlamentach narodowych krajów członkowskich dotyczące dostosowania legislacji do zapisów prawa UE.

[152] *europa.eu/rapid/press-release_IP-17-3193_pl.pdf* – [dostęp: 2.2.2019]
[153] *europa.eu/rapid/press-release_IP-18-6759_pl.pdf* – [dostęp: 2.2.2019]

Jak zauważają Anna Kańciak[154] i Zbigniew Chmielowski, w ramach struktur Unii Europejskiej można wyodrębnić dwa kluczowe obszary polityki bezpieczeństwa cyberprzestrzeni i zapobiegania cyberterroryzmowi. „Do pierwszego z nich należą regulacje ukierunkowane na zwalczanie cyberataków (w tym również cyberprzestępczości i cyberterroryzmu), do drugiego – mające na celu ochronę infrastruktury krytycznej (*Critical Infrastructure Protection*, CIP), krytycznej infrastruktury informatycznej (*Critical Information Infrastructure Protection*, CIIP) oraz bezpieczeństwa sieci i informacji (*Network and Information Security*, NIS)"[155]. Stosownie do tego podziału kompetencji „[…] wszelkie działania w zakresie pierwszego obszaru podlegają przepisom Tytułu V (Przestrzeń wolności, bezpieczeństwa i sprawiedliwości) Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Dlatego też, zgodnie z przedmiotowym i kompetencyjnym podziałem struktur unijnych, problematyka ta jest podejmowana przez Dyrekcję Generalną do Spraw Wewnętrznych i Migracji (*Directorate General for Migration and Home Affairs*). Z kolei drugi obszar znajduje się w kompetencji Dyrekcji Generalnej ds. Sieci komunikacyjnych, treści i technologii (*Directorate General for Communications Networks, Content and Technology*) i jest uregulowany w Tytule VIII (Polityka gospodarcza i pieniężna) TFUE.[156]

W obszarze pierwszym na forum Rady Europy (2005) przyjęto Decyzję Ramową Rady 2005/222/WSiSW w sprawie ataków na systemy informatyczne, której celem było „usprawnienie współpracy między organami sądowymi i innymi właściwymi organami, włącznie z policją i innymi wyspecjalizowanymi organami ścigania Państw Członkowskich, poprzez zbliżanie zasad prawa karnego w Państwach Członkowskich w dziedzinie ataków na systemy informatyczne"[157]. Decyzja Ramowa po raz pierwszy określiła też jako niezbędną konieczność wprowadzenia sankcji karnych za ataki na systemy informatyczne[158]. Decyzja Ramowa Rady 2005/222/WSiSW została zastąpiona Dyrektywą Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 roku,[159] dotyczącą ataków na systemy informatyczne i uchylającą poprzednią decyzję ramową Rady.

---

[154] Kańciak A., *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8, s. 112.
[155] Chmielowski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w EU i państwa członkowskich*, „Studia z Polityki Publicznej", nr 2(10)2016, s. 116
[156] *Ibidem*, s. 117.
[157] *Decyzja Ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne,* Pobrano z: http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri= CELEX:32005F0222&from=PL
[158] *Ibidem*
[159] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW, Dz. Urz. UE L 218 z 14.08.2013 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32013L0040 [dostęp: 14.02.2019]

Z kolei w obszarze drugim, tj, związanym z ochroną infrastruktury krytycznej, Komisja Europejska opracowała Zieloną księgę w sprawie europejskiego programu ochrony infrastruktury krytycznej. W załączniku nr 1 do niej po raz pierwszy sformułowano obowiązujące w UE definicje tego systemu (właściwie dwóch systemów – infrastruktury krytycznej oraz krytycznej infrastruktury informatycznej). Wyprzedzając nieco chronologię, należy dodać, iż ochronę systemu infrastruktury krytycznej objęto także odrębną regulacją Unii Europejskiej – Dyrektywą Rady 2008/114/WE z dnia 8 grudnia 2008 roku w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[160] będącą obecnie podstawowym elementem Europejskiego Programu Ochrony Infrastruktury Krytycznej (EPOIK).

2.2.5. Strategia Unii Europejskiej w dziedzinie walki z terroryzmem *(European Union strategy in the field of counter-terrorism)*

Dokument powyższy, przyjęty przez Radę Unii Europejskiej 30 listopada 2005 roku, został przygotowany we współpracy z Koordynatorem ds. Walki z Terroryzmem. Strategia stawia główny nacisk na „zwalczanie terroryzmu w skali światowej, przestrzegając praw człowieka, by Europa była miejscem bezpieczniejszym i obszarem wolności, bezpieczeństwa i sprawiedliwości dla swoich obywateli”[161]. Dokument ten omówiony zostanie nieco szerzej, jest on bowiem, zdaniem autora, tak pierwszym, jak i podstawowym aktem strategicznym określającym ramy i kierunki współpracy przy tworzeniu wspólnotowego, zbiorowego potencjału zabezpieczenia państw członkowskich przed zagrożeniami terroryzmu i cyberterroryzmu.

Podstawowym założeniem Strategii UE jest przekonanie, że bezpośrednia odpowiedzialność za skuteczność działań ochronnych przeciwko zagrożeniom terroryzmu i cyberterroryzmu spoczywa na państwach członkowskich, nie zaś na Unii jako organizacji państw. Nie oznacza to jednak, iż UE nie ma odgrywać żadnej roli w tym procesie, ma ona jednak przybierać następujące formy:

- „Wzmacnianie potencjału krajowego, tj. stosowanie zasad dobrej praktyki, wymiana wiedzy i doświadczeń w celu poprawy krajowego potencjału zapobiegania, ochrony,

[160] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, Dz. Urz. UE L 345 z 23.12.2008 http://rcb.gov.pl/wp-content/uploads/ dyrektywa_ rady_infr_eu.pdf, [dostęp: 14.02.2019]
[161] Pełny tekst strategii dostępny pod adresem http://register.consilium.europa.eu/pdf/pl/05/st14/st14469-re04.pl05.pdf

ścigania i reagowania na terroryzm, w tym poprzez usprawnienie gromadzenia i analizy informacji oraz danych wywiadowczych.

- Ułatwianie współpracy europejskiej, tj. współpraca w dziedzinie bezpiecznej wymiany informacji między państwami członkowskimi a instytucjami. Tworzenie i ocena mechanizmów ułatwiających współpracę, w tym między policją i sądownictwem, w razie potrzeby środkami legislacyjnymi.
- Budowa zbiorowego potencjału, tj. zapewnienie na szczeblu UE zdolności do rozumienia zagrożenia terroryzmem i zapewnienia wspólnych reakcji politycznych, optymalne wykorzystanie możliwości organów europejskich, jak Europol, Eurojust, Frontex, centrum MIC i SitCen.
- Wspieranie partnerstwa międzynarodowego, tj. współpraca z podmiotami spoza UE – zwłaszcza z ONZ, innymi organizacjami międzynarodowymi i kluczowymi państwami trzecimi nad pogłębieniem międzynarodowego konsensusu, budową potencjału i umocnieniem współpracy na rzecz walki z terroryzmem"[162].

Jak wynika z powyższego, strategia określa cztery filary działań w zakresie ochrony przed zagrożeniami terroryzmu i cyberterroryzmu, których wspólnym mianownikiem pozostaje miejsce UE jako wspólnoty w światowym systemie bezpieczeństwa. Filary te – zapobieganie, ochrona, ściganie i reagowanie – UE traktuje jako zobowiązanie do wniesienia proporcjonalnego, wewnętrznie komplementarnego wkładu w globalne bezpieczeństwo.

a) W ramach filaru pierwszego, czyli zapobiegania, strategia przedstawia plan działań przeciwdziałających radykalizacji postaw i rekrutacji kandydatów na terrorystów. Strategia ta koncentruje się na przeciwdziałaniu radykalizacji postaw i rekrutacji do grup terrorystycznych, jak Al-Kaida i grupy przez nią inspirowane, zważywszy, że ten rodzaj terroryzmu stanowi obecnie główne zagrożenie dla Unii jako całości[163]. Kluczowe priorytety, jakie zostały określone przez Unię Europejską w ramach filaru „zapobieganie", obejmują:
    - „wypracowywanie wspólnych sposobów podejścia do wykrywania zachowań problemowych, obejmujących w szczególności niewłaściwe wykorzystanie Internetu;
    - rozwiązywanie problemu podżegania i rekrutacji w kluczowych środowiskach, w szczególności w więzieniach oraz miejscach kształcenia i kultu religijnego, zwłaszcza

[162] Zakres działań UE, ujęty w *Strategii*…, podano za: Gancarz G., *op. cit.,* s. 7-8.
[163] *Strategia UE w dziedzinie walki z terroryzmem,* punk*t 6,* http://register.consilium.europa.eu/pdf/pl/05/st14/st14469-re04.pl05.pdf

poprzez wprowadzanie w życie przepisów uznających takie zachowania za przestępstwo;

- formułowanie strategii obecności w mediach i komunikacji pozwalającej lepiej objaśniać polityki UE;
- propagowanie dobrych rządów, demokracji, edukacji i pomyślnego rozwoju gospodarczego poprzez programy pomocy Wspólnoty i państw członkowskich;
- rozwijanie dialogu między kulturami w obrębie Unii i poza nią;
- tworzenie wolnego od emocji języka pozwalającego dyskutować o powyższych kwestiach;
- dalsze badania, wymianę doświadczeń i wyników analiz w celu głębszego zrozumienia tych kwestii i przygotowywania reakcji politycznych"[164].

b) W ramach filaru drugiego, czyli ochrony, celem założeń strategii jest ochrona obywateli oraz infrastruktury krytycznej państw przez zmniejszenie podatności na ataki terrorystyczne i cyberterrorystyczne. Cel ten ma zostać osiągnięty dzięki poprawie bezpieczeństwa granic, transportu i systemów infrastruktury krytycznej, w tym systemu teleinformatycznego. Filar ten, oprócz zapewniania ochrony przed atakami, ma również za zadanie wpłynąć na ograniczenie ich skutków. Główne postulaty zawarte w postanowieniach filaru drugiego zawierają:

- „poprawę bezpieczeństwa unijnych paszportów przez wprowadzenie danych biometrycznych;
- stworzenie systemu informacji wizowej (VIS) i systemu informacji Schengen drugiej generacji (SISII);
- przeprowadzenie za pośrednictwem agencji Frontex oceny rzeczywistego zagrożenia granic zewnętrznych UE;
- wprowadzenie w życie uzgodnionych wspólnych standardów bezpieczeństwa lotnictwa cywilnego, ochrony portów i bezpieczeństwa morskiego;
- uzgodnienie europejskiego programu ochrony infrastruktury strategicznej;
- jak najlepsze wykorzystanie efektów prac badawczych na szczeblu UE i Wspólnoty"[165].

[164] Gancarz G., *op. cit.,* s. 11
[165] *Strategia UE w dziedzinie walki z terroryzmem,* punk*t 6,* http://register.consilium.europa.eu/pdf/pl/05/st14/st14469-re04.pl05.pdf [oraz:] Gancarz G., *op. cit.,* s. 12.

Warto dodać, że w związku z filarem drugim, w grudniu 2006 roku, na wniosek Rady Europejskiej Komisja zaproponowała i wydała w formie dyrektyw wiele inicjatyw na rzecz zdolności do ochrony infrastruktury krytycznej. Między innymi przedłożono dyrektywę, w której ustanawia się i określa procedury służące identyfikowaniu i wyznaczaniu europejskiej infrastruktury krytycznej. Przygotowano też podstawy dla realizacji „Europejskiego systemu szybkiego ostrzegania" docelowo umożliwiającego reagowanie na sytuacje nadzwyczajne (obecnie jest to „System ostrzegania i informowania o zagrożeniach wobec infrastruktury krytycznej")[166].

c) W ramach filaru trzeciego, czyli ścigania, Strategia za najważniejsze uznaje działania mające doprowadzić do udaremniania realizacji aktów terrorystycznych oraz cyberterrorystycznych. „Podstawowe cele w tym zakresie to utrudnienie terrorystom planowania, niszczenie ich sieci i utrudnianie działań rekrutacyjnych, odcinanie terrorystów od źródeł finansowania i środków ataku oraz stawianie ich przed wymiarem sprawiedliwości, przy stałym poszanowaniu praw człowieka i prawa międzynarodowego. […] Unia będzie wspierać wysiłki państw członkowskich na rzecz udaremniania działań terrorystów poprzez stwarzanie zachęt do wymiany informacji i danych wywiadowczych między tymi Państwami, dostarczanie wspólnych analiz zagrożeń i umacniania współpracy operacyjnej w dziedzinie ochrony porządku publicznego"[167]. Główne postulaty zawarte w postanowieniach filaru trzeciego zawierają:

- „umocnienie zdolności krajowych do walki z terroryzmem, w świetle zaleceń dokonanych w procesie wzajemnej oceny krajowych systemów walki z terroryzmem;
- pełne wykorzystanie Europolu i Eurojustu dla ułatwienia współpracy policyjnej i sądowej oraz dalsze włączenie ocen zagrożeń przeprowadzanych przez Wspólne Centrum Sytuacyjne do procesu formułowania polityki walki z terroryzmem;
- dalszy rozwój wzajemnego uznawania orzeczeń sądowych, w tym poprzez wprowadzenie europejskiego nakazu dowodowego;
- zapewnienie pełnego wprowadzenia w życie i oceny istniejącego prawodawstwa, a także ratyfikacja stosownych międzynarodowych traktatów i konwencji;

[166] Rypulak-Mirowska K., *Zwalczanie terroryzmu – Wybrane zagadnienia polityki bezpieczeństwa wewnętrznego Unii Europejskiej – szanse i zagrożenia dla Polski*, Biuro Bezpieczeństwa Narodowego, Warszawa 2008, s. 53-54.
[167] *Strategia UE w dziedzinie walki z terroryzmem,* pkt 22 i 23*,* http://register.consilium.europa.eu/pdf/pl/05/st14/st14469-re04.pl05.pdf [oraz:] Gancarz G., *op. cit.,* s. 10

- rozwijanie zasady dostępności informacji związanej z ochroną porządku publicznego;
- kwestia dostępu terrorystów do broni i materiałów wybuchowych, od materiałów wybuchowych domowej roboty po materiały chemiczne, biologiczne, radiologiczne i nuklearne;
- ograniczanie źródeł finansowania terroryzmu, w tym poprzez wprowadzanie w życie uzgodnionych przepisów prawa, działania zapobiegające nadużywania sektora nonprofit i dokonywanie ocen ogólnych wyników działań UE w tej dziedzinie;
- udzielanie pomocy technicznej zwiększającej zdolność działania priorytetowych państw trzecich"[168].

d) Filar czwarty, czyli reagowanie, zawiera priorytety związane z przygotowaniem się Unii oraz państw członkowskich do sprawnej reakcji na skutki zamachu terrorystycznego, do ich minimalizacji oraz koordynacji działań podejmowanych po ataku. Najważniejsze z tych priorytetów to:
   - „przyjęcie na szczeblu UE ustaleń dotyczących koordynacji działań w sytuacjach kryzysowych i wspomagających je procedur operacyjnych;
   - przegląd prawodawstwa dotyczącego wspólnotowego mechanizmu ochrony ludności;
   - przeprowadzanie oceny ryzyka jako źródło informacji pozwalające rozwijać zdolność do reagowania na atak;
   - poprawa koordynacji działań z organizacjami międzynarodowymi w dziedzinie zarządzania reakcjami na ataki terrorystyczne i inne sytuacje kryzysowe;
   - wymiana zasad dobrej praktyki, wypracowywanie sposobów podejścia dotyczących udzielania pomocy ofiarom terroryzmu i ich rodzinom"[169].

[168] *Ibidem*.
[169] *Strategia UE w dziedzinie walki z terroryzmem,* pkt 22 i 23 , http://register.consilium.europa.eu/pdf/pl/05/st14/st14469-re04.pl05.pdf [oraz:] Gancarz G., *op. cit.,* s. 11, [oraz:] *Komunikat Komisji z 20 października 2004 r. do Rady i Parlamentu Europejskiego w sprawie zapobiegania, przygotowania oraz odpowiedzi na ataki terrorystyczne* COM (2004) 698 - końcowy, [oraz:] *decyzja Rady z 5 marca 2007 r. ustanawiająca Instrument Finansowy Ochrony Ludności,* Dz.Urz. UE 2007 L 71/9.

2.2.6. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów w kierunku ogólnej strategii zwalczania cyberprzestępczości (*Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards an overall strategy to combat cybercrime*) [170]

Dokument powyższy, przyjęty 22 maja 2007 roku, jest bardzo istotny z punktu widzenia wyodrębnienia z szeregu działań określanych szeroko jako 'zapobieganie zagrożeniom wspólnego bezpieczeństwa', zagadnień związanych bezpośrednio z walką z cyberprzestępczością i cyberterroryzmem. Podkreślono w nim fundamentalne znaczenie teleinformatycznej struktury krytycznej dla bezpieczeństwa krajów UE – to pierwsze w dokumentach strategicznych tak wyraźne określenie tego systemu jako jednego z najważniejszych. Komunikat wskazuje również konieczność wypracowania przez unijne instytucje jednolitej strategii do walki z cyberprzestępczością. Określa on główne zadania operacyjne z zakresu zwalczania przestępczości w cyberprzestrzeni na szczeblu unijnym, ale także sygnalizuje potrzebę ujednolicenia definicji przestępstw i krajowych przepisów prawa karnego w tej dziedzinie, choć jednocześnie „ze względu na dużą różnorodność rodzajów przestępstw objętych pojęciem cyberprzestępczości [stwierdzał, że] nie jest jeszcze właściwe ogólne ujednolicenie definicji"[171].

W latach kolejnych Unia Europejska wypracowała szereg dokumentów strategicznych będących jednocześnie rozwinięciem ustaleń z komunikatu z 22 maja 2007 roku. Z jednej strony poczynania te jawią się jako reakcja na kryzys finansowy z 2008 roku, sprzyjający destabilizacji światowego systemu bankowego, a drugiej stanowią wynik prac podjętych przez agencje unijne w celu ujednolicenia zapisów dotyczących zapobiegania zagrożeniom infrastruktury krytycznej w cyberprzestrzeni. W marcu 2009 roku przyjęto Komunikat KE w sprawie ochrony infrastruktury krytycznej, w roku 2010 – Komunikat KE pt. *Agenda Cyfrowa dla Europy* (*A Digital Agenda for Europe) oraz program Safer Internet Plus*).

[170] *Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, W kierunku ogólnej strategii zwalczania cyberprzestępczości z dnia 22 maja 2007 r.,* Pobrano z: http://eur-lex.europa.eu/legalcontent/PL/TXT/PDF/?uri=CELEX:52007DC0267&from=PL

[171] Stępień M., *op. cit.* s. 26-27.

2.2.7. Strategia Cyberbezpieczeństwa dla UE: „Otwarta, bezpieczna i chroniona cyberprzestrzeń" (*Cybersecurity Strategy of the European Union: "An Open, Safe and Secure Cyberspace"*)[172]

Dokument powyższy powstał w lutym 2013 roku i również można określić go mianem przełomowego w zakresie ochrony cyberprzestrzeni w państwach UE. Z dzisiejszej dodatkowo perspektywy można by ocenić, że przyjęto go zbyt późno w stosunku do rzeczywistych potrzeb i zagrożeń, co nie zmienia jednak faktu, iż pozostaje on wciąż aktualny, jak i stanowi podstawę do dalszych prac legislacyjnych i programowych. „Otwarta, bezpieczna i chroniona cyberprzestrzeń" obejmuje zabezpieczanie w cyberprzestrzeni: rynku wewnętrznego, systemu sprawiedliwości i spraw wewnętrznych oraz polityki zagranicznej, między innymi poprzez rozwijanie oraz finansowanie krajowych centrów i instytucji z zakresu przeciwdziałania cyberprzestępczości i cyberterroryzmowi. Wyróżniono tu pięć strategicznych priorytetów z zakresu cyberbezpieczeństwa:

- osiągnięcie odporności na cyberzagrożenia;
- radykalne ograniczenie cyberprzestępczości;
- opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie cyberbezpieczeństwa w powiązaniu ze Wspólną Polityką Bezpieczeństwa i Obrony;
- rozbudowa zasobów przemysłowych i technologicznych;
- ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE[173].

Ponadto strategii towarzyszy propozycja dyrektywy Parlamentu Europejskiego i Rady w sprawie bezpieczeństwa systemów informacyjnych UE „odwołująca się do konieczności zharmonizowania zasad. obowiązujących we wszystkich państwach członkowskich oraz zapewnienia efektywnej wymiany informacji pomiędzy sektorem prywatnym i publicznym"[174].

Zapisy przyjętej strategii pozwoliły również doprowadzić do powołania Europejskiego Centrum ds. Walki z Cyberprzestępczością. Ta centralizująca i koordynująca instytucja, która rozpoczęła działalność 11 stycznia 2013 roku, zapewnia głównie wymianę informacji pomiędzy

---

[172] *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* European Commission, Brussels, 7.2.2013, Pobrano z: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.
[173] *Ibidem,* s. 4-5.
[174] *Proposal for a Directive of the European Parliament and of the Council, concerning measures to ensure a high common level of network and information security across the Union,* Brussels, 7.2.2013, Pobrano z: http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri= CELEX:52013PC0048& from= EN, [za:] Stępień M., *op. cit.,* s. 28.

organami policyjnymi państw członkowskich oraz wspomaga działania wymierzone w przestępczość zorganizowaną, organizuje również szkolenia i ćwiczenia w zakresie ochrony cyberprzestrzeni i infrastruktury krytycznej zarówno dla agencji rządowych, jak i dla sektora prywatnego.

2.2.8. Dyrektywa Parlamentu Europejskiego w sprawie ataków na systemy informatyczne (*Directive of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision*) [175]

Dyrektywa Parlamentu Europejskiego z 12 sierpnia 2013 roku ma na celu korelacje przepisów prawa państw członkowskich w zakresie zapobiegania, zwalczania i penalizacji przestępstw związanych z systemami teleinformatycznymi. Dyrektywa wskazuje w pierwszym rzędzie na konieczność wypracowania wspólnych definicji oraz korelacji typologii tych przestępstw. Kolejnym postulatem jest doprowadzenie do skutecznej, ścisłej i prawidłowej współpracy pomiędzy organami ścigania w poszczególnych państwach, jak również pomiędzy nimi, a instytucjami Europejskimi (Eurojust, Europol, ENISA i Europejskim Centrum do spraw Walki z Cyberprzestępczością)[176]. Zgodnie z Dyrektywą do cyberprzestępstw zalicza się:

- nielegalny dostęp do systemu,
- nielegalną integrację w system,
- nielegalną integrację w dane,
- nielegalne przechwytywanie danych,
- nielegalne narzędzia do popełniania cyberprzestępstw.

„Dyrektywa wprowadziła również zaostrzenie kar za przestępstwa związane z przestępczą działalnością cybernetyczną. Najniższy wyrok za ciężkie przestępstwa tego typu to dwa lata, natomiast pięć lat grozi za popełnienie przestępstw związanych z ingerencją w system lub dane w ramach organizacji przestępczej, powodujące znaczne szkody lub w przypadku ataku na dane lub systemy należące do infrastruktury krytycznej”[177]. Do odpowiedzialności pociągnięte mogą być nie tylko osoby fizyczne, ale też i prawne. „Kary nałożone na nie powinny być

[175] *Dyrektywa Parlamentu Europejskiego i Rady z dnia12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW*, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32013L0040
[176] Adamski A., *Dyrektywa Parlamentu Europejskiego i Rady z dnia12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady. 2005/222/WSiSW – próba oceny*, za: http://www.secure.edu.pl/pdf/2013/D2_1630_A_Adamski.pdf [dostęp: 02.01.2019]
[177] Ciekanowski Z., Rejman K., Wyrębek M., *op. cit.,* s. 45.

odstraszające i proporcjonalne, zalicza się do nich: grzywnę, zakaz prowadzenia działalności gospodarczej (stały lub czasowy), nadzór sądowy, likwidacja, zamknięcie działalności (stałe lub czasowe) oraz pozbawienie praw do korzystania z pomocy i świadczeń publicznych”[178].

2.2.9. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Polityka wobec Internetu i zarządzanie Internetem: Rola Europy w kształtowaniu przyszłości zarządzania Internetem*[179]

Choć dokument ten nie dotyczy bezpośrednio zagadnienia cyberterroryzmu i zagrożeń infrastruktury krytycznej, to jednak porusza kwestie związane z wielopłaszczyznowym i wielopodmiotowym zarządzaniem (*governance*) cyberprzestrzenią oraz stwierdza, iż dla zapewnienia jej bezpieczeństwa najbardziej optymalny jest model wielopłaszczyznowego i wielopodmiotowego zarządzania, w którym pozycji dominującej nie ma żaden z podmiotów. Ten punkt widzenia wpisuje się tym samym w stanowisko Stanów Zjednoczonych uznających schemat partnerstwo publiczno-partnerstwo prywatne za właściwy kierunek polityki zapobiegania cyberterroryzmowi. Komisja Europejska uważa również, że procesowi temu „powinny podlegać także kwestie techniczne dotyczące zarówno protokołów internetowych, jak i innych technologii informacyjnych. Jak podkreśla się w komunikacie, szczegóły techniczne dotyczące protokołów internetowych i specyfikacje innych technologii informacyjnych mogą wywoływać znaczące skutki w zakresie polityki publicznej. Mogą one oddziaływać na prawa człowieka, takie jak prawo użytkowników do ochrony danych oraz do bezpieczeństwa, dostęp do zróżnicowanych zasobów wiedzy i informacji oraz wolność słowa w Internecie”[180]. Komunikat wnosi też nowe spojrzenie na kwestię neutralności sieciowej i jej znaczenia dla bezpiecznej, ale też otwartej cyberprzestrzeni, postrzegając ‘neutralność sieciową’ jako zależną od konkurencji rynkowej oraz uwzględniającą prawa podstawowe obywateli Unii Europejskiej – prawo do prywatności, ochronę danych osobowych, wolność wypowiedzi i swobodę prowadzenia działalności gospodarczej. Pogląd ten jest również zgodny ze stanowiskiem USA uznającym prymat konkurencji jako mechanizm regulacyjny jako najlepsze rozwiązanie dla bezpieczeństwa Internetu (więcej na ten temat w podrozdziale 3.3).

---

[178] *Dyrektywa Parlamentu Europejskiego i Rady z dnia12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, art. 11.*

[179] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Polityka wobec Internetu i zarządzanie Internetem: Rola Europy w kształtowaniu przyszłości zarządzania Internetem* (COM (2014) 72, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2014:0072:FIN:PL:PDF, [dostęp: 14.02.2019]

[180] Chmielowski Z., *op. cit.*, s. 110.

2.2.10. Europejska agenda bezpieczeństwa na lata 2015-2020

Agenda ta powstała w roku 2013, w celu dalszego rozwoju współpracy państw członkowskich w zakresie zwalczania zagrożeń związanych z bezpieczeństwem oraz zwiększenia wspólnego, ponadnarodowego zaangażowania w walkę przeciwko terroryzmowi, cyberprzestępczości i cyberterroryzmowi. Określono w niej konkretne narzędzia i środki mające na celu bardziej skuteczne przeciwdziałanie tym trzem zagrożeniom. Przestawiając ją na forum PE, Wiceprzewodniczący KE Frans Timmermans powiedział: „[…] terroryzm, cyberprzestępczość i cyberterroryzm są złożonymi i wciąż zmieniającymi się wyzwaniami w zakresie bezpieczeństwa o wymiarze transgranicznym. […] Za pomocą tej wspólnej unijnej agendy chcemy zachęcić organy krajowe do bardziej skutecznej współpracy, w duchu wzajemnego zaufania. Terroryści podejmują bowiem atak na cenione przez nas wartości demokratyczne".

Najważniejsze działania wymienione w *agendzie* obejmowały:

- „przeciwdziałanie radykalizacji postaw,
- aktualizację decyzji ramowej w sprawie zwalczania terroryzmu,
- wyeliminowanie finansowania przestępców,
- poszerzenie dialogu z sektorem informatycznym,
- wzmocnienie narzędzi zwalczania cyberprzestępczości,
- zwiększenie zasobów Europolu"[181].

W celu wzmocnienia zdolności w zakresie bezpieczeństwa cybernetycznego w Agendzie zaproponowano między innymi:

- utworzenie Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie cyberbezpieczeństwa - współpracujące z państwami członkowskimi w opracowywaniu i wdrażaniu narzędzi i technologii koniecznych i gwarantuje, że obrona będzie tak nowoczesna, jak broń, którą posługują się cyberprzestępcy.
- Opracowanie planu szybkiego reagowania państw członkowskich umożliwiającego natychmiastową, skuteczną i skoordynowaną reakcję w przypadkach wystąpienia ataków cybernetycznych na dużą skalę. Plan przewiduje też regularne testy w ramach ćwiczeń w zakresie zarządzania w sytuacji kryzysu cybernetycznego lub innej sytuacji kryzysowej.

[181] *http://europa.eu/rapid/press-release_IP-15-4865_pl.htm,* [dostęp: 02.02.2019]

- Wzmocnienie zdolności w zakresie obrony cybernetycznej – Agenda zachęca państwa członkowskie do włączenia cyberobrony w ramy stałej współpracy strukturalnej (PESCO) i Europejskiego Funduszu Obrony, aby wspierać w ten sposób projekty strukturalne w zakresie cyberobrony. Agenda przewiduje też współprace ze strukturami militarnymi Paktu Północnoatlantyckiego – UE i NATO będą razem wspierać współpracę na rzecz badań naukowych i innowacji w dziedzinie obrony cybernetycznej, także przez udział w równoległych i skoordynowanych ćwiczeniach.
- Dalsze pogłębienie współpracy międzynarodowej – tym samym UE wzmacnia zdolność reagowania na cyberataki, wprowadzając ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne. Istotną zmianą jest też deklaracja „wysiłków na rzecz budowania nowych zdolności, służących wspieraniu państw trzecich w walce z zagrożeniami cybernetycznymi”[182].

2.2.11. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, *Otwarta i bezpieczna Europa: realizacja założeń*[183]

Dokument ten poświęcono między innymi zwiększeniu zdolności operacyjnej zwalczania cyberprzestępczości poprzez utworzenia działającego w ramach Europolu Europejskiego Centrum ds. Walki z Cyberprzestępczością. Komunikat postuluje także utworzenie narodowych centrów ds. walki z cyberprzestępczością we wszystkich państwach członkowskich UE oraz wdrażania w uzgodnionych na forum Unii zaostrzonych przepisów karnych, a także wnosi o ustalenie jurysdykcji. W tym celu za niezbędne ocenia się ratyfikowanie Konwencji Rady Europy o cyberprzestępczości przez jak największą liczbę państw.

[182] *Ibidem*.
[183] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, *Otwarta i bezpieczna Europa: realizacja założeń* (COM (2014) 154, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX :52014DC0154 [dostęp: 14.02.2019]

Rozdział III

Polityka ochrony cyberprzestrzeni w Stanach Zjednoczonych Ameryki

3.1. Cyberprzestrzeń USA jako teatr działań wojennych

„Dobrze przeprowadzony atak cybernetyczny może pokonać Stany Zjednoczone w niecałe 15 minut”[184] – twierdzi Robert A. Clarke, autor przyjętej – choć nie bezkrytycznie – definicji cyberwojny. John A. Warden[185], na przykład, już w 1995 roku uznał sieci teleinformatyczne za piąty wymiar walki zbrojnej. Obecnie znawcy przedmiotu rozszerzają pojęcie cyberprzestrzeni jako piątego teatru działań wojennych do znacznie rozleglejszego obszaru wpływu na zdolność obronną przeciwnika. „Co za tym idzie, za ‘cyberwojnę’ czy też wojnę w cyberprzestrzeni można uznać nie tylko wykorzystanie sieci w ramach konfliktu zbrojnego, ale także w celach szpiegowskich lub terrorystycznych”[186]. Cyberprzestrzeń w kategoriach militarnych staje się zatem przestrzenią operacyjną i to w obu ujęciach definicyjnych tego terminu[187], co pozwala osiągnąć zamierzone cele wojenne nie tylko w ramach konfliktu w środowisku cyfrowym, ale też na innych przestrzeniach operacyjnych zarezerwowanych dotąd dla „tradycyjnych” teatrów działań wojennych.

Stany Zjednoczone należą do krajów o najbardziej rozwiniętej infrastrukturze teleinformatycznej, co z jednej strony pozwala im na sprawne i skuteczne zarządzanie systemami infrastruktury krytycznej, z drugiej natomiast znacząco zwiększa podatność na zagrożenia dla jej bezpieczeństwa. „We wrześniu 2007 r. amerykańscy eksperci ujawnili informacje, które wskazywały, iż w samych tylko Stanach Zjednoczonych chińscy hakerzy, dokonujący regularnych ataków na instytucje USA, kontrolują około 750 tysięcy komputerów w ramach własnej sieci botnet. Były doradca Pentagonu, Paul Strassman, określił tego typu sieć komputerów jako najtańszą broń ofensywną, jaką każdy kraj sobie może zapewnić.”[188].

Przykładem wykorzystania cyberataku w charakterze broni wymierzonej w siły zbrojne przeciwnika może być poważne włamanie do amerykańskich sieci wojskowych na Bliskim Wschodzie. Za pomocą pamięci USB do sieci wojskowych zostało przeniesione złośliwe

[184] Clarke R.A., Knake R.A., *Cyber War. The Next Threat to National Security and What to Do About It*, HarperCollins e-books, New York, NY, 2011
[185] Warden J.A*., op. cit., s. 40–55*
[186] *Lakomy M., Cyberwojna jako rzeczywistość XXI wieku,* [w:] „Stosunki Międzynarodowe” nr 3–4 (t.44), Warszawa 2011
[187] Przez dwa ujęcia pojęcia „operacyjności” autor rozumie zarówno określenie zakresu prowadzenia wojny w cyberprzestrzeni, jak i zdefiniowanie tego termin jako „przydatności” czy „użyteczności” – ujęcia te w żaden sposób się nie wykluczają i pozostają komplementarne semantycznie.
[188] Lynn III W.J., *Defending a New Domain*, „Foreign Affairs”, 2010 r.; [oraz:] N. Schachtman, *Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated)*, Wired.com, 2010 r., http://www.wired.com/dangerroom/2010 - [dostęp: 30.01.2019]

oprogramowanie, które błyskawicznie rozprzestrzeniło się między innymi na komputery Pentagonu. Umożliwiło to hakerom przede wszystkim transfer tajnych danych wojskowych poza zabezpieczone serwery. „Atak przez długi czas pozostał niewykryty i stanowił największe w historii włamanie do sieci militarnych USA. O jego powadze świadczy fakt, że w ramach operacji Buckshot Yankee amerykańskim informatykom usunięcie *malware* ze wszystkich serwerów US Army zajęło aż 14 miesięcy. Według słów przedstawicieli amerykańskiego wywiadu po dwóch latach dochodzenia uznano, że prawdopodobnie za włamaniem stały służby wywiadowcze Rosji, której hakerzy już wcześniej stosowali podobny kod"[189].

Sprawne funkcjonowanie każdego rozwiniętego państwa, w tym także jego armii, w coraz większym stopniu uzależnione jest od sieci teleinformatycznej. Praktycznie każda dziedzina gospodarki, infrastruktury oparta jest na oprogramowaniu komputerowym. Stany Zjednoczone, pozycjonowane do niedawna jako jedyne supermocarstwo cybernetyczne (aktualnie prymat przejmują Chiny), stały się w przeciągu ostatnich lat nie tylko prekursorem wojny cybernetycznej, ale też największym celem dla cyberterrorystów. Jak twierdzi cytowany już Robert A. Clarke, skuteczny atak z cyberprzestrzeni może w bardzo krótkim czasie spowodować zniszczenie infrastruktury krytycznej USA, a tym sam sparaliżować nie tylko gospodarkę, ale i siły zbrojne. I choć jego ostrzeżenia traktowane są przez część specjalistów jako nazbyt apokaliptyczne, a prezentowane zagrożenia za zbyt wyolbrzymione,[190] to jednak pozostają one odzwierciedleniem rosnącej obawy przed wojną w cyberprzestrzeni i atakami cyberterrorystycznymi. I choć możliwości działań ofensywnych USA w cyberprzestrzeni są ogromne, to wskaźnik skuteczności defensywy pozostaje niski. Innymi słowy, zaatakowanie Stanów Zjednoczonych za pomocą sieci teleinformatycznych pozostaje względnie łatwym zadaniem, dostępnym dla każdego państwa czy organizacji dysponujących odpowiednio przygotowanymi hakerami, a z uwagi na bardzo wysoki poziom udziału technologii teleinformatycznych w infrastrukturze krytycznej USA, atak ten prawie na pewno wywoła duże zniszczenia. Z drugiej strony, jeśli strona atakująca będzie państwem o niskim zaawansowaniu technologicznym swoich systemów infrastrukturalnych czy militarnych, może nie obawiać się ewentualnego odwetu cybernetycznego. Państwa o charakterze dyktatury

[189] Lynn III W.J., *Defending a New Domain*, „Foreign Affairs", 2010 r.; [oraz:] N. Schachtman, *Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated)*, Wired.com, 2010 r., http://www.wired.com/dangerroom/2010 - [dostęp: 30.01.2019]
[190] Patrz między innymi: Schneier B., *Book Review: Cyber War*, 21.12.2010, http://www.schneier.com/blog/archives/2010/12/book_review_ cyb.html, [oraz:] R. Singel, *White House Cyber Czar: "There Is No Cyberwar"*, 4.03.2010, http://www.wired.com/threatlevel/2010/03/ schmidt-cyberwar.

mogą wręcz odciąć kraj od Internetu, czego nie dokona żadne z państw demokratycznych, gdzie serwery i łącza stanowią w ogromnej większości własność prywatnych firm.

3.2. Ramowe doktryny obrony cybernetycznej USA

Kolejne administracje USA „ery cybernetycznej", czyli już od I kadencji George'a W. Busha, za priorytet w założeniach walki z atakami cyberterrorystycznymi, zarówno o charakterze międzypaństwowym, jak i dokonywanymi przez organizacje terrorystyczne, uznają strategie ofensywne. Wybór takiej doktryny może nie być do końca zrozumiały, z uwagi na wspomniany wcześniej wskaźnik możliwości obrony, który zwraca uwagę na to, że to właśnie USA są łatwym celem ataku cybernetycznego. Tymczasem wielu spośród ich potencjalnych przeciwników – czy to z uwagi na bezpaństwowy charakter (w przypadku organizacji terrorystycznej) czy też z uwagi na znacznie słabiej rozwinięty system teleinformatycznego zarządzania infrastrukturą krytyczną i siłami zbrojnymi (w przypadku krajów takich jak Iran czy Korea Północna) – po prostu nie odczuje skutków takiego ataku. Straty poniesione przez USA w cyberwojnie zawsze będą większe niż korzyści. Eksperci zgadzają się co do tego, że państwo atakujące USA w cyberwojnie może wyrządzić ogromne szkody w infrastrukturze krytycznej, a jednocześnie przetrwać działania odwetowe, jeśli te odbędą się w cyberprzestrzeni – z uwagi na potencjał militarny USA odwet za pomocą konwencjonalnych środków militarnych miałby oczywiście zupełnie inny skutek. W cyberprzestrzeni odwet symetryczny nie jest możliwy. Zdaniem R.A. Clarka na liście priorytetów USA na pierwszym miejscu powinna znaleźć się obrona, a potem dopiero działania ofensywne[191]. Podobnie twierdzi cytowany przez Dominikę Dziwisz Martin C. Libicki z RAND Corporation, który uważa, iż „nawet amerykański Departament Obrony, w którego misję wpisana jest ofensywa cybernetyczna, nie tylko chciałby, ale nawet musi przeznaczyć więcej środków na możliwości obrony niż na przygotowanie ataku. Zdolności odwetowe i powstrzymywania są tylko częścią wydatków"[192].

Czas po zamachach 11 września 2001 roku to okres wzmożonych działań administracji George'a W. Busha mających na celu zarówno opracowanie doktryny zabezpieczenia się przed atakiem terrorystycznym, jak i podjęcia kroków ofensywnych zarówno jako drogi odwetu, jak i działań odstraszających potencjalnych napastników. Z uwagi na fakt, iż zamachy przeprowadzone

[191] Clarke R.A., Knake R.A., *op. cit.,* s. 160.
[192] Libicki M.C., *Cyberspace Is Not a Warfighting Domain*, s. 122, [za:] Dziwisz D., *op. cit*., s. 132.

przez Al-Kaidę nie sposób zakwalifikować jako cyberterrorystyczne[193], działania USA dotyczące zabezpieczenia przed zagrożeniami ze strony terrorystów miały charakter raczej konwencjonalny – na kwestię ochrony przed cyberterroryzmem nie położono bowiem szczególnego nacisku. Warto zauważyć, że w amerykańskim systemie prawnym nie ma, jak dotąd, oficjalnej definicji cyberprzestępczości oraz cyberterroryzmu, zaś federalne organy ścigania zazwyczaj posługują się zawężającymi definicjami dostosowanymi dla swoich celów i procedur: „Własne definicje cyberprzestępczości i cyberterroryzmu mają, między innymi, Federalne Biuro Śledcze (FBI), Centrum Zgłaszania Oszustw Internetowych (*Internet Fraud Complaint Center*, IC3), Tajna Służba Stanów Zjednoczonych (*U.S. Secret Service*). Chociaż działalność FBI zazwyczaj kojarzona jest wyłącznie z kontrwywiadem, to od początku lat dziewięćdziesiątych coraz większa część zadań Biura sprowadza się do zwalczania przestępczości komputerowej i cyberterroryzmu"[194]. Jednolita definicja nie wydaje się jednak niezbędna, skoro wszystkie wyżej wymienione agencje wypełniają swoje zadania w zakresie zwalczania cyberterroryzmu Można by więc zaryzykować twierdzenie, że uzgodniona definicja ograniczałaby wręcz te działania. Ponadto część badaczy uważa, że niemożliwa jest precyzyjna identyfikacja różnic między cyberterroryzmem a wojną cybernetyczną, przyznając tym samym, uznają, że nie ma potrzeby definiowania cyberterroryzmu, „ponieważ dla potrzeb nauki i w praktyce wystarczające jest zdefiniowanie wojny informacyjnej […][195]. Autor tego opracowania sądzi jednak, iż pojęcia cyberwojny i cyberterroryzmu obejmują różne zakresy semantyczne, jednak pomimo dużej liczby cech wspólnych są to *de facto* dwie oddzielne kategorie.

Amerykańska doktryna konfliktu cybernetycznego zakłada, iż stroną atakującą w cyberwojnie będą odpowiednio: Rosja, Chiny, Izrael, a dopiero w czwartej kolejności wskazuje na USA[196].

Warto zwrócić uwagę, że Izrael, będący strategicznym sojusznikiem USA, wymieniany jest w niej jako strona ofensywna, ale to jedynie przy założeniu, że atak izraelski nie będzie wymierzony w Stany Zjednoczone. Rosja to w sposób historycznie uwarunkowany, wywodzący się jeszcze z czasów zimnej wojny i koncepcji świata dwubiegunowego, potencjalny przeciwnik USA, zatem umieszczenie jej na pierwszym miejscu agresorów w cyberwojnie wydaje się ze wszech miar

[193] Cytowany już Martin Libicki twierdzi jednak, że silne dowody przemawiają za tym, że ataki z 11 września 2001 roku były koordynowane i dowodzone za pomocą Internetu. Terroryści, planując ataki, wymieniali się planami, korzystając z tego samego konta e-mail, logowali się na stronie poczty internetowej i tutaj zostawiali wskazówki działań i inne informacje. eInformacja podana [za:] Dziwisz D., *op. cit.*, s. 132
[194] Dziwisz D., *op. cit.*, s. 74.
[195] Stark R., *Future Warfare: Information Superiority through Info War*, http://www.smsu.edu/. [Za:] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa...*, *op. cit.*, s. 69.
[196] Kuehl D.A., *From Cyberspace to Cyberpower: Defining the Problem*, [w:] F.D. Kramer, S.H. Starr, LK. Wentz (red.), *Cyberpower and National Security*, Waszyngton 2009, s. 38

uzasadnione. Drugie miejsce Chin również wydaje się słuszną dedukcją, choć należy założyć, że z uwagi na skokowo rosnący potencjał informatyczny ChRL już niedługo to właśnie one staną się głównym przeciwnikiem USA (a także Rosji) w potencjalnym cyberkonflikcie. Kraje zaliczone niegdyś przez George'a W. Busha do „osi zła", takie jak Iran czy Korea Północna, znajdują się na dalszych miejscach. Tymczasem dla tych właśnie państw cyberatak jest najbardziej odpowiednią dla ich potencjału bronią przeciwko infrastrukturze krytycznej USA, same zaś, z powodów omówionych wcześniej, nie muszą się specjalnie obawiać odwetu w cyberprzestrzeni.

3.3. Ramowe założenia Ochrony Infrastruktury Krytycznej w USA

W *USA Patriot Act* – a warto przypomnieć, że ta kontrowersyjna ustawa powstawała jako reakcja na zamachy terrorystyczne z 11 września 2001 roku – infrastruktura krytyczna została zdefiniowana jako „systemy i zasoby, zarówno fizyczne, jak i wirtualne, ważne dla Stanów Zjednoczonych w takim stopniu, że ich awaria albo zniszczenie miałyby destrukcyjny wpływ na bezpieczeństwo narodowe, ekonomiczne, bezpieczeństwo narodowego systemu zdrowia albo na jakąkolwiek kombinację tych zagrożeń"[197]. Zgodnie z definicją przyjętą przez NATO, na wniosek USA 'infrastruktura krytyczna' to „budowle, usługi oraz systemy informacyjne, będące na tyle istotne dla państw, że ich niewydolność lub zniszczenie miałyby wyniszczający wpływ na bezpieczeństwo narodowe, gospodarkę, zdrowie publiczne oraz porządek publiczny i efektywne funkcjonowanie rządu"[198]. W ten sposób zdefiniowane pojęcie infrastruktury krytycznej obejmuje zarówno systemy instalacji fizycznych, jak i systemy teleinformatyczne. Jak we wszystkich państwach rozwiniętych, większość systemów była od siebie fizycznie niezależna, jednak z uwagi na rozwój technik informatycznych, w celu zwiększenia efektywności działania i uproszczenia zarządzania, systemy te zostały w znacznym stopniu połączone. W USA wykorzystanie SCADA i innych rozwiązań sieciowych osiągnęło szczególnie wysoki poziom, co uczyniło amerykańską infrastrukturę krytyczną o wiele bardziej podatną na atak cybernetyczny. Można założyć, że to właśnie w tym kraju infrastruktura krytyczna właśnie z uwagi na stopień zaawansowania informatycznego jest najbardziej narażona na zagrożenia – nie tylko cyberterrorystyczne, ale także skutki zdarzeń losowych – oraz te związane z błędami operatorów systemów (w rozdziale I niniejszego opracowania wskazano szczegółowy wykaz tych zagrożeń).

[197] *Ibidem*.
[198] Soloch P., *NATO a ochrona infrastruktury krytycznej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2007, http://www.bbn.gov.pl/portal/pl/2/915/O_przyszlosci_NATO.html?search=474159029, [dostęp: 20.01.2019]

Jak podaje Dominika Dziwisz, „Amerykańska Prezydencka Komisja Ochrony Infrastruktury Krytycznej, powołana w lipcu 1996 roku (*President's Commission on Critical Infrastructure Protection*, PCCIP) zidentyfikowała osiem obszarów infrastruktury krytycznej: telekomunikację, bankowość i finanse, wytwarzanie i przesył energii elektrycznej, dystrybucję i magazynowanie ropy naftowej i gazu, dostawy wody, transport, służby ratownicze i usługi rządowe. […] wyodrębniła [także] pięć sektorów, dla których obrony konieczna była współpraca trzech stron: rządu, właścicieli elementów infrastruktury krytycznej i operatorów. Należą do nich: wytwarzanie i dystrybucja energii (w tym energii elektrycznej), dystrybucja i magazynowanie ropy naftowej i gazu, finanse i bankowość, systemy fizycznej dystrybucji (w tym powietrznej, morskiej i lądowej) oraz najważniejsze usługi społeczne (w tym dostawy wody, usługi rządu, służby ratownicze)"[199].

Strategia obrony cyberprzestrzeni w zakresie ochrony infrastruktury krytycznej powstała w czasach administracji George'a W. Busha, ale obowiązywała jeszcze przez dwie kadencję Baracka Obamy, jak również aktualna jest dziś w administracji Donalda Trumpa. Jak pisze D. Dziwisz, „kładzie [ona] nacisk na zdolność atakowania w cyberprzestrzeni, a mniej uwagi przywiązuje do możliwości obrony. Rozwiązania w zakresie defensywy cybernetycznej ograniczają się do zabezpieczania systemów rządowych i wojskowych. Bezpieczeństwo przedsiębiorstw sektora prywatnego, właścicieli większości elementów infrastruktury krytycznej, pozostaje przeważnie problemem sektora prywatnego"[200]. Jeśli chodzi o ochronę systemów wojskowych i rządowych, to pod koniec 2009 roku w USA powstała *Cyber Command* (USCYBERCOM), czyli agencja militarna, dla której jedynym obszarem działania jest cyberprzestrzeń. Jej zadaniem jest obrona określonych sieci Departamentu Obrony (na dziś to około 8 milionów urządzeń działających w blisko 15. tysiącach sieci), ale też atak na sieci i infrastrukturę krytyczną nieprzyjaciela. Zgodnie z jej wytycznymi, obrona własnych systemów sieciowych realizowana będzie poprzez działania ofensywne, co oznacza blokowanie, ale i niszczenie sieci przeciwnika.

Federalne sieci cywilne chronione są natomiast przez Krajową Sekcję Cyberbezpieczeństwa Departamentu Bezpieczeństwa Krajowego (*National Cyber Security Division*, NCSD) powołaną do realizacji dwóch zadań. Pierwszym z nich jest zapewnienie sprawnie działającego systemu obrony cyberprzestrzeni (*National Cyberspace Response System*, NCRS), drugim natomiast to

[199] Dziwisz D., *Stany Zjednoczone a międzynarodowe bezpieczeństwo cybernetyczne*, Kraków 2015, s. 61-62.
[200] Dziwisz D., *op. cit.*, s. 132

ochrona infrastruktury krytycznej USA. NCDS koordynuje i nadzoruje działania związane z bezpieczeństwem komputerów osobistych, analizą zagrożeń dla „cywilnej" cyberprzestrzeni, zajmuje się także zarządzaniem i koordynacją działań agencji federalnych zgrupowanych w Krajowej Grupie ds. Przeciwdziałania Atakom w Cyberprzestrzeni (*National Cyber Response Co-ordination Group*, NCRCG).

Jak dotąd nie stworzono żadnej agencji czy organizacji na szczeblu federalnym, która zajmowałaby się ochroną bezpieczeństwa cybernetycznego sektora prywatnego. Tymczasem bardzo duża część urządzeń i systemów infrastruktury krytycznej USA należy w istocie do przedsiębiorstw prywatnych. Luka ta odnosi się zwłaszcza do sektora teleinformatycznego oraz energetycznego, które praktycznie w całości znajdują się w rękach prywatnych koncernów i firm, pozostawiając tym samym odpowiedzialność za zabezpieczenie tychże struktur całkowicie po stronie sektora niepaństwowego. Z jednej zatem strony uznano zabezpieczenie infrastruktury krytycznej za priorytet strategii obrony narodowej, z drugiej natomiast nie zapewniono kompleksowego i skutecznego wsparcia nawet dla najistotniejszych jej systemów. Trudno bowiem za takie zapisy uznać dokument pt. *Triady Strategii Obrony* (*Defensive Triad Strategy*), w którym zawarto propozycję legislacji na szczeblu federalnym mającą tworzyć obowiązujące w sektorze prywatnym standardy bezpieczeństwa. Martin Libicki w rozmowie z Dominiką Dziwisz wyraża pogląd, iż rząd USA powinien chronić tylko wybrane elementy systemu infrastruktury krytycznej, zwłaszcza wspomniane powyżej energetyczny i teleinformatyczny, nie bez racji uważając je za najważniejsze dla funkcjonowania państwa. „Jeśli chodzi o sektor energetyczny – wprowadziłbym bezwzględny wymóg całkowitego odcięcia systemów kontroli w elektrowniach od Internetu. To, oczywiście, nie pozostanie bez wpływu na koszty energii elektrycznej, czyli uderzy po kieszeniach obywateli. Ale jest to jedyny sposób, aby wyeliminować ryzyko ataku cybernetycznego. Są jednak elementy infrastruktury krytycznej, które nie mogą działać bez podłączenia do sieci, na przykład telekomunikacja, bo to nie tylko telefony, ale (też) Internet albo bankowość […]"[201]. Podejście takie, prezentowane nie tylko przez M. Libickiego, ale też wielu innych specjalistów w dziedzinie cyberbezpieczeństwa, jak choćby Jason Healey[202], zakłada jednak, iż choć rzeczywiście większa ochrona rządu dla sektora prywatnego zarządzającego infrastrukturą krytyczną USA jest niezbędna, to same firmy pozostaną nieaktywne w tym zakresie. Jak zauważa właśnie J. Healey, „największym

[201] Dziwisz D., *op. cit.*, s. 134
[202] Por. m.in: J. Healey, *Preparing for Cyber 9/12*, „Atlantic Council Issue Brief", Waszyngton, 2012 [oraz:] J. Healey, *The US Cyber Policy Reboot*, „Atlantic Council Issue Brief", Waszyngton, 2012.

problemem [dla Administracji] jest zakładanie z góry, że dla każdego z tych obszarów możliwe są tylko rozwiązania na poziomie rządowym. Tutaj myśli się, że w cyberprzestępczości, cyberszpiegostwie i cyberwojnie rola sektora prywatnego ogranicza się do bycia ofiarą. Innymi słowy, rola obywateli i firm prywatnych w zapobieganiu cyberzagrożeniom sprowadza się wyłącznie do zgłaszania popełnionych przestępstw. Jeśli w Waszyngtonie mówi się o cyberproblemie i partnerstwie publiczno-prywatnym, to tak naprawdę myśli się o tym, co rząd powinien zrobić, żeby ochronić sektor prywatny. Istnieje duży rozdźwięk między działaniami, jakich oczekiwalibyśmy od przedsiębiorstw w celu zabezpieczenia się przed atakami, a tym, co przerzuca na nich rząd. A zatem to nie jest tylko ogólny problem wspierania partnerstwa, ale dużo poważniejsza sprawa związana z postrzeganiem roli przedsiębiorstw i organizacji gospodarczych będących własnością prywatną"[203]. Można więc dostrzec w działaniach administracji USA następujący paradoks: choć uważa się za konieczne zwiększenie ochrony cyberbezpieczeństwa będących w prywatnych rękach kluczowych systemów infrastruktury krytycznej, to działań tych nie prowadzi się inaczej niż przez regulacje centralne, przy jednoczesnym pozostawianiu przy stanowisku odpowiedzialności własnej firm i koncernów za kwestie ochrony przed cyberterroryzmem. Tymczasem „przedsiębiorstwa nie potrzebują rad Waszyngtonu, jak zarządzać swoimi sieciami. I nie ma żadnego sposobu, aby zmusić ich do zarządzania tymi sieciami tak, jak chce tego [administracja]. Wszystkie raporty Komisji od 1997 roku mówią to samo, czyli o potrzebie koordynacji, dzielenia się informacją, budowie partnerstwa publiczno-prywatnego i zaufania. I nie można z tym polemizować […]. [Ale] to i tak nie wnosi nic nowego do dyskusji nad cyberbezpieczeństwem. Można wysnuć smutną konkluzję, że ostatnie pięć lat poświęciliśmy mówieniu o niczym, bo w gruncie rzeczy ten problem jest dla nas nieuchwytny"[204] – stwierdza M. Libicki. Paradoks ten, jak można by sądzić, ma kilka przyczyn, ale najistotniejszą pozostaje brak wzajemnego zaufania pomiędzy rządem USA a sektorem prywatnym, przy czym nieufność ta jest wyjątkowo mocna po obu stronach. Rząd oczekuje od firm przekazywania danych pozostających niewątpliwie w zakresie tajemnicy przedsiębiorstw, sam nader niechętnie dzieląc się własnymi informacjami dotyczącymi bezpieczeństwa narodowego. W opinii wielu specjalistów wiele złego we wzajemne relacje wniosła szczególnie ustawa *USA Patriot Act* [205] z 2001 roku dająca rządowi

[203] Healey J., *America's New Cyberspace Strategy, Atlantic Council*, 16.05.2011, http://www.acus.org/new_atlanticist/americas-new cyberspace-strategy, [dostęp: 05.02.2019]
[204] Dziwisz D., *op. cit.*, s. 135
[205] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*; Public Law Pub.L. 107-56.

daleko idące prerogatywy, a jednocześnie zwalniająca go od jakiejkolwiek symetrycznej współpracy. I choć ustawa ta wygasła w roku 2015, a Barack Obama czynił wiele, by zapewnić społeczeństwo i przedsiębiorców o wysokich standardach ochrony danych w swojej administracji, to jednak owa nieufność do rządu dość mocno zakorzeniła się w społecznej świadomości Amerykanów. Ważnym również niewątpliwie argumentem dla braku konstruktywnych działań administracji w zakresie cyberbezpieczeństwa jest kwestia kosztów, jakie należałoby ponieść w tym zakresie. Wydaje się bowiem, że skoro rząd federalny uznaje rolę państwa za wiodącą w partnerstwie z sektorem prywatnym, to oczywiste wydaje się, że to on powinien ponieść koszty ustanowienia standardów tej współpracy.

W tym kontekście warto może odwołać owe krytyczne uwagi dotyczące doktryny cyberbezpieczeństwa obowiązującej w Stanach Zjednoczonych i uznać ją za ściśle odpowiadającą obecnej sytuacji. Skuteczna cyberdefensywa oznacza bowiem konieczność współpracy rządu z sektorem prywatnym, natomiast skuteczna cyberofensywa – nie.

3.4. Dokumenty strategiczne dotyczące krajowego i międzynarodowego bezpieczeństwa cyberprzestrzeni opracowane przez USA

W odróżnieniu od przedstawionego w poprzednim podrozdziale podejścia Unii Europejskiej do kwestii prawnych regulacji kwestii ochrony przez cyberterroryzmem, Stany Zjednoczone przez dłuższy czas (w stosunku do UE) wdrażały tylko i wyłącznie krajową politykę cyberbezpieczeństwa. Oczywiście wyraźna różnica pomiędzy statusem Unii Europejskiej, będącej gospodarczo-politycznym związkiem 28 demokratycznych państw narodowych, a USA, czyli państwem federacyjnym, może stanowić o przyczynach takiego podejścia, to jednak pozycja Stanów Zjednoczonych jako międzynarodowego supermocarstwa oraz najważniejszego państwa NATO w sposób naturalny predestynowała je do roli lidera międzynarodowego porozumienia zapobiegania cyberterroryzmowi. Stan faktyczny przez wiele lat pozostawał jednak w ścisłej korelacji z omówioną już doktryną bezpieczeństwa cybernetycznego Stanów Zjednoczonych dającą pierwszeństwo działaniom ofensywnym. Dopiero w roku 2011 administracja Baracka Obamy zaprezentowała w Międzynarodowej Strategii USA dla Cyberprzestrzeni[206] swoją wizję

[206] *International Strategy for Cyberspace. Prosperity, Security, and Openness In a Networked World*, Waszyngton,2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf, [dostęp: 5.02.2019]

przyszłości cyberprzestrzeni, nie ograniczając jej wyłącznie do sposobów zapewniania bezpieczeństwa obywatelom własnego kraju.

3.4.1. Prezydencka Komisja ds. Zabezpieczania Infrastruktury Krytycznej (*President's Commission on Critical Infrastructure Protection*, PCCIP)

Komisja ta, powołana w roku 1996, pod koniec pierwszej kadencji Billa Clintona miała za zadanie ocenić ryzyko narażenia narodowej infrastruktury krytycznej na ataki terrorystyczne oraz opracować plan jej zabezpieczenia przed potencjalnymi zamachami. Komisja rozpoczęła pracę w kryzysowym dla nastrojów społecznych USA czasie, bo po dwóch atakach terrorystycznych – na World Trade Center w 1993 roku, kiedy zginęło 6 osób a ponad tysiąc zostało rannych oraz na budynek federalny w Oklahoma City w 1995 roku, w wyniku którego zginęło 168 osób, a 680 zostało rannych. To właśnie atak w Oklahoma City był największym atakiem terrorystycznym na terytorium Stanów Zjednoczonych do czasu zamachów z 11 września 2001 roku, okazał się też swego rodzaju punktem krytycznym dla administracji, która uświadomiła sobie skalę zagrożenia terroryzmem. Raport Komisji po raz pierwszy zwrócił uwagę na fakt, iż poszczególne systemy infrastruktury krytycznej, podłączone do Internetu, nie są w żaden sposób zabezpieczone przed atakiem.

Raport ten [207], opublikowany w 1997 roku, wyodrębniał osiem sektorów, których sprawne i niezakłócone działanie ma największy wpływ na obronność kraju i jego bezpieczeństwo ekonomiczne: „telekomunikację, bankowość i finanse, produkcję i dystrybucję energii elektrycznej, dystrybucję i magazynowanie ropy naftowej i gazu, dostawy wody, transport, służby ratownicze i usługi rządowe. Następnie wyodrębniono pięć sektorów, dla których zabezpieczania konieczna jest współpraca trzech stron, czyli rządu, właścicieli infrastruktur i operatorów sieci. Zaliczono do nich sektor energetyczny, finanse i bankowość oraz najważniejsze usługi społeczne – w tym dostawy wody, usługi rządowe, działania służb ratowniczych"[208].

Raport, choć nie ostrzegał bezpośrednio przed atakiem cyberterrorystycznym, skupiając się na „konwencjonalnych" zagrożeniach terrorystycznych, to jednak dopuszczał jego prawdopodobieństwo w przyszłości. To właśnie systemy teleinformatyczne i sieć Internet uznano za najsłabsze ogniwo i wyzwanie dla amerykańskiej infrastruktury krytycznej. „Jako sposób na

[207] *The Report of the President's Commission on Critical Infrastructure Protection*, October 1997, http://www.fas.org/sgp/ library/pccip.pdf, [dostęp: 11.02.2019]
[208] Denning D., *op. cit.*, s. 459–467

rozwiązanie tych problemów i podniesienie poziomu bezpieczeństwa infrastruktury krytycznej (IK), Komisja zaproponowała współpracę pomiędzy agencjami rządowymi i właścicielami/operatorami IK, polegającą przede wszystkim na dzieleniu się informacjami na temat potencjalnych zagrożeń, a także inwestycje w badania i rozwój nad nowymi technologiami. Sposobem na wdrożenie tych postanowień miało być właśnie ustanowienie ISAC – Centrów Wymiany i Analizy Informacji, które agregowałyby informacje na temat incydentów, a potem anonimizowały je i udostępniały wszystkim członkom ISAC"[209].

W Raporcie zaproponowano też utworzenie Biura Zapewnienia Działania Krajowych Infrastruktur (*Office of National Infrastructure Assurance*) działającego w ramach Rady Bezpieczeństwa Narodowego (*National Security Council*, NSC)[210] i koordynującego współpracę między rządem, agencjami oraz sektorem prywatnym. Miało też pomóc przedsiębiorstwom w szkoleniach i organizacji działań prewencyjnych zabezpieczającymi przed atakami i zmniejszającymi ich potencjalne skutki. Ponadto postulowano też konieczność powołania:

- „Rady Zapewnienia Działania Infrastruktur Krajowych (*National Infrastructure Assurance Council*) – miało to być forum wymiany poglądów dla właścicieli infrastruktur krytycznych oraz przedstawicieli władz krajowych i lokalnych; Rada miała też rekomendować odpowiednie działania prezydentowi;
- agencji federalnych kierujących poszczególnymi sektorami (*Federal Lead Agencies*), ułatwiających wymianę informacji pomiędzy właścicielami infrastruktur i operatorami"[211].

Łącznie Komisja wydała siedemdziesiąt dwa zalecenia, wśród których większość tyczy się właśnie rozwoju współpracy międzysektorowej i partnerstwa publiczno-prywatnego. Ten właśnie postulat, czyli „partnerstwo", będzie odtąd najważniejszym elementem każdego projektu legislacyjnego związanego z bezpieczeństwem cyberprzestrzeni. Uznać należy, że Raport ten stał się podstawą programową dla kolejnych działań administracji prezydenta Clintona mających już charakter przepisów wykonawczych.

[209] https://cyberpolicy.nask.pl/cp/dobre-praktyki/isac/69,ISAC-Information-Sharing-and-Analysis-Center-Centra-Wymiany-i-Analizy-Informacji.html [dostęp: 11.02.2019]
[210] *The Report of the President's Commission on Critical Infrastructure Protection*, October 1997, http://www.fas.org/sgp/ library/pccip.pdf, s.67, [dostęp: 11.02.2019]
[211] Dziwisz D., *op. cit.*, s. 201

3.4.2. Dyrektywa Prezydencka 63 (*Presidential Decision Directive 63*, *PDD-63*)[212]

Podpisana w 22 maja 1998 roku istotnie wykorzystała ustalenia poczynione podczas pracy Komisji ds. Zabezpieczania Infrastruktury Krytycznej. Była ona zbiorem zaleceń oraz decyzji administracyjnych zmierzających do stworzenia sprawnego systemu zabezpieczenia infrastruktury krytycznej przed ryzykiem ataku fizycznego i cybernetycznego.

W myśl jej zapisów celem administracji powinno być dążenie do takiego rozwoju systemu zabezpieczenia infrastruktury krytycznej, aby przerwy w jej działaniu, wywołane atakiem terrorystycznym lub cyberterrorystyczny, były „krótkie, nieczęste, łatwe do zarządzania, ograniczone geograficznie i w minimalnym stopniu zagrażające obronności Stanów Zjednoczonych"[213]. W celu realizacji tego postulatu „do każdego sektora infrastruktury zagrożonego atakiem fizycznym lub z cyberprzestrzeni przypisano odpowiedni departament lub agencję (*Lead Agency*). Są one na bieżąco informowane o stanie bezpieczeństwa danego sektora oraz ponoszą za niego odpowiedzialność. […) Sektor prywatny wybiera swojego koordynatora sektorowego (*Sector Coordinator*)"[214]. Ponadto „Dyrektywa 63 przypisała odpowiedzialność za bezpieczeństwo informacyjne infrastruktury krytycznej Radzie Bezpieczeństwa Narodowego (*National Security Council*, NSC). Do ściślej współpracy z Radą zobowiązany został krajowy koordynator ds. bezpieczeństwa, ochrony infrastruktury i antyterroryzmu (*National Coordinator for Security*, I*nfrastructure Protection, and Counter terrorism*)"[215].

Rzeczona Dyrektywa nie ogranicza się do podporządkowania istniejącym strukturom w administracji lub agencjom nowych zadań, ale powołuje także kilka nowych organów. Najważniejsze z punktu widzenia tego opracowania to Krajowa Rada Zapewnienia Działania Infrastruktur (*National Infrastructure Assurance Council*, NIAC) oraz Biuro Zapewniania Działania Infrastruktur Krytycznych (*Critical Infrastructure Assurance Office*, CIAO). Pierwsza z nich jest organem doradczym, którego zadaniem jest określanie kierunków efektywnej współpracy sektora prywatnego i publicznego dla bezpieczeństwa infrastruktury krytycznej; druga natomiast czuwa nad koordynacją polityk bezpieczeństwa infrastruktury krytycznej na szczeblu federalnym. Na działania na poziomie operacyjnym utworzono natomiast Federalną Sieć ds. Wykrywania Nieautoryzowanego Dostępu (*Federal Intrusion Detection Network*, FIDNet)

[212] *Presidential Decision Directive 63*, 22.05.1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, [dostęp: 12.02.2019]
[213] *Ibidem,* s. 17
[214] Dziwisz D., *op. cit.*, s. 202-203.
[215] *Ibidem.*

odpowiedzialną za wykrywanie i reagowanie na ataki cybernetyczne. W nowe uprawnienia wyposażono też FBI – na ich podstawie w ramach Biura rozpoczęło działalność Narodowe Centrum Ochrony Infrastruktury (*National Infrastructure Protection Center*, NIPC).

Bezpośrednim efektem wydania przez Billa Clintona omawianej Dyrektywy było także przyjęcie dwóch istotnych z punktu widzenia ochrony infrastruktury krytycznej dokumentów. Pierwszy z nich, o charakterze bardziej programowym, przyjęty w 2009 roku, nosi nazwę *Narodowego Planu Ochrony Infrastruktury* (*National Infrastructure Protection Plan*, NIPP)[216], tradycyjnie już podkreślając rolę partnerstwa publiczno-prywatnego, ale i precyzując też zasady współpracy pomiędzy partnerem publicznym, reprezentowanym przez Rządowe Rady Koordynacyjne (*Government Coordinating Councils*, GCC) a partnerem prywatnym – w tym przypadku Sektorowymi Radami Koordynacyjnymi (*Sector Coordinating Councils*, SCC).
Z kolei przyjęcie Narodowego Planu Zabezpieczenia Systemów Informacyjnych (*National Plan for Information Systems Protection*)[217] implikowało spore wydatki amerykańskiemu budżetowi. Plan nie tylko określił bowiem ramy działania dla rządu federalnego w zakresie zapobiegania, wykrywania, odpowiedzi i zabezpieczania narodowej infrastruktury krytycznej oraz federalnych systemów komputerowych przed atakiem, ale też przeznaczał na ten cel kwotę ponad 2 miliardów dolarów. Z uwagi na to, iż przyjęto go w ostatnim roku drugiej kadencji Billa Clintona, to jego wykonanie, również pod względem budżetowym, przypadło na okres prezydentury George'a W. Busha.

3.4.3. Narodowa Strategia Bezpieczeństwa Cyberprzestrzeni (*National Strategy to Secure Cyberspace*, NSSC)[218]

Półtora roku po zamachach 11 września, w lutym 2003 roku, administracja prezydenta Busha przyjęła do realizacji Narodową Strategię Bezpieczeństwa Cyberprzestrzeni jako element Narodowej Strategii Bezpieczeństwa Krajowego (*National Strategy for Homeland Security*). Wyznaczono w niej trzy strategiczne cele:

a) ochronę infrastruktury krytycznej,
b) zmniejszenie zagrożenia atakami z cyberprzestrzeni,

[216] U.S. Department of Homeland Security. (2013a). *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience.* Washington DC, 2009.
[217] https://www.nrc.gov/reading-rm/doc-collections/commission/secys/2000/secy2000-0088/2000-0088scy.pdf, [dostęp: 11.02.2019]
[218] https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf - [dostęp: 11.02.2019]

c) minimalizacja czasu odbudowy infrastruktury,

a także wskazano pięć strategicznych priorytetów. W celu ich realizacji dokument proponuje: „szeroko pojęte partnerstwo publiczno-prywatne, które obejmie jednostki administracji rządowej, małe i średnie przedsiębiorstwa prywatne oraz wielkie korporacje. Sektor prywatny wnosi do współpracy głównie *know-how*. Z kolei rola rządu ma sprowadzać się do ustalania ram współpracy i finansowania prac badawczo-rozwojowych. Przede wszystkim jednak działalność rządu to prace nad tworzeniem prawa, które ma ułatwiać współpracę i wymianę informacji. Prawo może zachęcać sektor prywatny do współpracy głównie poprzez zapewnienie bezpieczeństwa przepływu informacji. Przedsiębiorstwa muszą mieć gwarancję, że informacje poufne nie dostaną się w niepowołane ręce. Utworzenie sieci ściśle współpracujących partnerów jest szczególnie ważne dla zmniejszenia problemów koordynacji działań, sprawnej wymiany informacji czy rozwoju technologicznego. Partnerstwo powinno mieć charakter międzynarodowy, gdyż nie można ograniczyć działania Internetu do terytorium jednego państwa”[219].

- W ramach priorytetu pierwszego Strategii stworzono Narodowy System Bezpieczeństwa w Cyberprzestrzeni (*A National Cyberspace Security Response System*), w którego skład wchodzą Ośrodki Wspólnego Użytkowania i Analizowania Informacji (*Information Sharing and Analysis Center*, ISACs) – szerzej omówione w podrozdziale 3.4.2. Dla sprawnego i niezakłóconego w warunkach ataku cybernetycznego kontaktu między sektorami prywatnym i publicznym, czyli w praktyce pomiędzy ISACs a Departamentem Bezpieczeństwa Krajowego (DHS), Strategia postulowała utworzenie Sieci Ostrzegania i Wymiany Informacji (*Cyber Warning and Information Network*, CWIN), tj. bezpiecznej sieci o zabezpieczonej i stabilnej infrastrukturze.
- Priorytet drugi dotyczy działań przyspieszających opracowanie planu, który będzie ograniczał zagrożenia cyberprzestrzeni i podatność cyberprzestrzeni na ataki (*A National Cyberspace Security Threat and Vulnerability Reduction Program).* Intencją ustawodawcy było wskazanie zależności bezpieczeństwa systemu informatycznego od precyzyjnego zdiagnozowania słabości zabezpieczeń infrastruktury krytycznej – rzeczony Plan jako kluczowe ocenia zapewnienie bezpieczeństwa systemów cyfrowej kontroli (*Digital Control Systems*, DCS) oraz systemów SCADA (*Supervisory Control and Data Acquisition*).

[219] Dziwisz D., *op. cit.*, s. 208

- W priorytecie trzecim zawarto Narodowy Program Szkoleń i Budowania Świadomości Zagrożeń (*A National Cyberspace Security Awareness and Training Program*), czym autorzy Strategii zwrócili uwagę na fakt, iż to czynnik ludzki może być najsłabszym elementem nawet najbardziej zaawansowanego systemu zapewnienia cyberbezpieczeństwa. Stąd też zaleceniem Strategii jest „podniesienie poziomu edukacji nie tylko specjalistów z dziedziny informatyki, ale także każdej osoby korzystającej z komputera i Internetu. Strategia podkreśla konieczność włączenia wszystkich użytkowników sieci w działania mające na celu zabezpieczenie elementów, nad którymi sprawują oni kontrolę”[220]. Dodatkowo sugerowane jest wprowadzenie certyfikacji specjalistów sektora IT, a zadanie to przewidziano do wykonania w ramach zadań Departamentu Bezpieczeństwa Krajowego.
- Zadanie zabezpieczenia teleinformatycznej infrastruktury rządowej (*Securing Governments' Cyberspace*) opisano w priorytecie czwartym. „Większość elementów infrastruktury krytycznej stanowi własność sektora prywatnego. Jednakże rząd pełni wiele kluczowych funkcji, choćby zapewnia bezpieczeństwo kraju, prowadzi politykę podatkową, jest odpowiedzialny za działanie publicznej służby zdrowia. Wszystkie aktywności rządu są zależne od systemów informatycznych. Dla zapewnienia ciągłości działania konieczne jest ich odpowiednie zabezpieczenie”[221]. Strategia zaleca też „używanie kart elektronicznych dla bezpiecznego logowania użytkownika, kontroli dostępu i zawartych na niej danych. Rekomenduje także stosowanie silnych haseł, tokenów, czyli generatorów jednorazowych haseł albo zabezpieczeń biometrycznych, czyli takich, które opierają się na wizerunku twarzy, zapisie linii papilarnych palców czy zapisie obrazu tęczówki”[222].
- W priorytecie piątym zawarto natomiast postulat nawiązania szerokiej, międzynarodowej współpracy w cyberprzestrzeni, co ma zapewniać zwiększenie poziomu bezpieczeństwa USA. Zadania związane z tą współpracą powierzono Departamentowi Stanu. Zaplanowano także powołanie Północnoamerykańskiej Strefy Cyberbezpieczeństwa obejmującej: USA, Kanadę i Meksyk. „W ramach budowania sieci współpracy

[220] Janiec M., *Narodowa Strategia Ochrony Cyberprzestrzeni*, Obserwatorium Cyfrowego Państwa, http://www.egov.pl/index2.php?option=content&task=view&id=11&pop=1&page=0, [dostęp: 12.02.2019]
[221] Dziwisz D., *op. cit.*, s. 215.
[222] Gancarz G., *Podstawy współpracy z zakresie zwalczania terroryzmu w prawie Unii Europejskiej, Warszawa 2008, s. 2.*

międzynarodowej Strategia zapowiada, że Stany Zjednoczone podejmą starania dla lepszego wypełniania postanowień Europejskiej Konwencji o Cyberprzestępczości z listopada 2001 roku. Celem tego dokumentu jest ujednolicenie polityki zwalczania i ścigania cyberprzestępstw"[223]. W celu ułatwienia wymiany doświadczeń i informacji sugerowana jest współpraca z Forum Zespołów ds. Bezpieczeństwa i Reagowania na Wypadki (*Forum of Incident Response and Security Teams*, FIRST). Obszerniej o tej – zdaniem autora – interesującej inicjatywie traktuje podrozdział 3.2.4 analizujący kwestię współpracy międzynarodowej w zapewnieniu bezpieczeństwa cyberprzestrzeni.

3.4.4. Kompleksowa Narodowa Inicjatywa Cyberbezpieczeństwa (*Comprehensive National Cybersecurity Initiative*, CNCI)[224]

Przedstawiony w Narodowej Strategii Bezpieczeństwa Cyberprzestrzeni model współpracy pomiędzy sektorem publicznym a prywatnym zobrazował konieczność pilnego wprowadzenia systematyki działań na poziomie zabezpieczenia sieci i infrastruktury państwowej. Opracowana w tym celu dopiero w 2008 roku, czyli ostatnim roku prezydentury G.W. Busha, Kompleksowa Narodowa Inicjatywa Cyberbezpieczeństwa miała za zadanie zabezpieczyć przede wszystkim przed kradzieżą i wyciekiem informacji z sieci rządowych – głównie Departamentu Obrony. Na realizację Inicjatywy przeznaczono 40 mln dolarów. Warto jednak podkreślić, że nie zawierała ona jednak żadnych rozwiązań, czy chociażby propozycji działań, dla sektora prywatnego. Dopiero kiedy administracja Baracka Obamy ujawniła wszystkie części Inicjatywy[225], plan ten stał się częścią uaktualnionej Narodowej Strategii Cyberbezpieczeństwa. Oparto go na trzech strategicznych celach ramowych:

- Pierwszy cel przewiduje: „zdefiniowanie linii obrony przez wzmocnienie świadomości słabych punktów infrastruktury informatycznej i świadomości zagrożeń. Przewidziane jest także zwiększenie zdolności do szybkiego reagowania, aby zniwelować obecnie istniejące luki w zabezpieczeniach. W tym celu nastąpi centralizacja czynności administracyjnych i infrastruktury sieciowej agend federalnych według zaleceń inicjatywy Bezpieczne Połączenia Internetowe (*Trusted Internet Connections*, TIC). Dla większego

[223] Dziwisz D., *op. cit*., s. 217
[224] https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf; [dostęp: 12.02.2019]
[225] Barack Obama dokonał przeglądu CNCI oraz zniósł klauzulę tajności z dwunastu inicjatyw, które obejmują zadania od zwiększenia nakładów na badania i rozwój, poprzez zwiększoną promocję cyberedukacji, aż po opracowanie strategii cyberobrony. Informacja podana [za:] Dziwisz D., *op. cit.*, s. 237.

bezpieczeństwa przepływu informacji w agencjach rządowych mają zostać także zainstalowane sieci sensorów, które ułatwią wykrywanie włamań”[226].

- „Drugi cel sprowadza się do zwiększenia zdolności kontrwywiadu USA w zakresie bezpieczeństwa cybernetycznego. Stworzenie cybernetycznego kontrwywiadu jest jednym z celów krótkoterminowych. Kontrwywiad, który swoim zakresem działania obejmowałby wszystkie agencje i departamenty rządowe, jest niezbędny, aby skoordynować operacje mające przeciwdziałać grupom hakerów. W celu poprawy bezpieczeństwa przeprowadzone zostaną szkolenia dla pracowników administracji publicznej wszystkich szczebli.
- Ostatni z celów ramowych przewiduje lepszą edukację w zakresie cyberbezpieczeństwa, koordynację i podejmowanie prac badawczo-rozwojowych”[227].

Motywacje stojące za ujawnieniem w marcu 2010 roku niejawnych części Inicjatywy wydają się nawiązywać do wielokrotnie podkreślanego przez Baracka Obamę dążenia do zmiany polityki nieufności charakteryzującej obie kadencje George’a W. Busha. I choć nietrudno zrozumieć także intencje poprzednika Obamy – zamachy 11 września 2001 roku i ich dalsze konsekwencje z pewnością zdeterminowały jego prezydenturę – to jednak prezydent Obama wielokrotnie i konsekwentnie odcinał się od modelu „supertajnego państwa”. Jak sam powiedział – „moja administracja została zobowiązana do stworzenia bezprecedensowego poziomu jawności działania”[228]. Z drugiej strony, już w czasie pierwszej prezydenckiej kampanii wyborczej zapowiadał, że kwestie cyberbezpieczeństwa ocenia jako bardzo istotne, zatem dążenie do jawności nie przełożyło się w żaden sposób na spadek zaangażowania jego administracji w proces ochrony cyberprzestrzeni. Świadczyć o tym może zdecydowanie najważniejszy dokument programowy opracowany przez Stany Zjednoczone w czasie jego prezydentury – Międzynarodowa Strategia USA dla Cyberprzestrzeni.

[226] *The Comprehensive National Cybersecurity Initiative*, The White House, http://www.whitehouse.gov/cybersecurity/ comprehensive-national-cybersecurity-initiative, [dostęp: 12.02.2019] [oraz:] Dziwisz D., *op. cit.*, s. 238-239
[227] *Ibidem*.
[228] http://www.whitehouse.gov/blog/2010/03/02/transparent-cybersecurity, [dostęp: 12.02.2019]

3.4.5. Międzynarodowa Strategia USA dla Cyberprzestrzeni (*U.S. International Strategy for Cyberspace*) i jej znaczenie dla światowego cyberbezpieczeństwa

Dokument ten, przedstawiony 16 maja 2011 roku, jest pod wieloma względami przełomowy i to nie tylko z tego względu, że prezentując go, USA po raz pierwszy w swojej historii zaproponowały swój udział w międzynarodowym procesie zabezpieczenia cyberprzestrzeni. Jego ogłoszenie jest bowiem precedensem w skali globalnej także z uwagi na fakt, że rząd USA zdecydował się podzielić z innymi państwami swoim programem rozwoju i zabezpieczenia cyberprzestrzeni. I choć program ten nie przedstawia szczegółowych rozwiązań problemów, to stosunkowo precyzyjnie wyznacza kierunki działania, oferując globalną strategię budowy i rozwoju „otwartej, interoperacyjnej, bezpiecznej i niezawodnej globalnej sieci"[229] nie tylko własnym agencjom rządowym, ale potencjalnym partnerom na całym świecie. „I chociaż strategia nie szereguje działań pod względem ważności, to jest wyraźną informacją dla międzynarodowych i narodowych partnerów, że USA mają sprecyzowaną wizję i pomysły na zapewnienie zrównoważonego rozwoju Internetu, czego ważnym elementem jest zapewnienie międzynarodowego bezpieczeństwa cybernetycznego"[230].

Twórcy Strategii dostrzegając fakt, iż żadne państwo, nawet o statusie „cybermocarstwa", jak USA, nie jest zdolne do samodzielnego zapewnienia bezpieczeństwa w cyberprzestrzeni, proponują współpracę w zakresie międzynarodowego ukierunkowania rozwoju technik teleinformatycznych i rozwoju globalnej sieci. To, co zamierzają realizować, porządkują w siedmiu priorytetowych obszarach działania:

- „gospodarce – poprzez wspieranie międzynarodowych standardów, wolnego rynku oraz ochronę własności intelektualnej;
- ochronie sieci – poprzez zwiększanie bezpieczeństwa, niezawodności i odporności sieci, usprawnienie systemu reagowania na sytuacje kryzysowe, tworzenie międzynarodowych partnerstw i jednolitych norm zachowań w sprawie bezpieczeństwa cyberprzestrzeni;
- egzekwowaniu prawa – poprzez tworzenie międzynarodowej polityki walki z cyberprzestępczością, harmonizowanie prawa dotyczącego cyberprzestępczości, aby było zgodne z konwencją z Budapesztu, ograniczenie terrorystom i przestępcom możliwości

[229] *U.S. International Strategy for Cyberspace*, *op. cit.*, s. 5
[230] Dziwisz D., *op. cit.*, s. 213

wykorzystywania Internetu do planowania operacji, finansowania oraz podejmowania ataków;

- współpracy wojskowej – poprzez dostosowanie sił zbrojnych do nowych zagrożeń w celu zapewnienia bezpieczeństwa sieci wojskowych, tworzenie nowych i wzmacnianie istniejących sojuszy oraz poszerzanie współpracy w zakresie kolektywnej obrony cyberprzestrzeni;
- zarządzaniu globalną siecią – poprzez wspieranie otwartości i innowacji w Internecie, tworzenie bezpiecznej i stabilnej infrastruktury, prowadzenie wielostronnej dyskusji na temat rozwoju Internetu;
- rozwoju międzynarodowym – poprzez tworzenie globalnej społeczności odpowiedzialnej za rozwój cyberprzestrzeni, rozpowszechnianie doświadczeń, wiedzy i umiejętności partnerom USA, rozwój dobrych praktyk, szkolenia dla organów ścigania, prawników i prawodawców, rozwój relacji na szczeblu politycznym i eksperckim;
- wolności Internetu – poprzez wspieranie społeczeństwa obywatelskiego i praw podstawowych, wolności wypowiedzi oraz prawa do stowarzyszania, współpraca z organizacjami pozarządowymi, współpraca na rzecz efektywnej ochrony danych i prywatności oraz zapewnienie wolnego przepływu informacji (m.in. zapobieganie cenzurze w Internecie"[231].

Zaangażowanie w powyższe zakresy działań dotyczy przede wszystkim agencji i departamentów administracji USA, niemniej jednak – zdaniem twórców Strategii – współpraca między instytucjami państwa nie jest wystarczająca. Jako konieczną określono więc współpracę rządu z sektorem prywatnym oraz innymi krajami i organizacjami międzynarodowymi do działań na płaszczyźnie dyplomatycznej, w ramach Departamentu Stanu utworzono Biuro Koordynatora ds. Cyberprzestrzeni (*Office of the Coordinator for Cyber Issues*, S/CCI)[232]. Jego zadaniem jest „wykorzystywanie członkostwa w organizacjach międzynarodowych, a także tworzenie nowych dwustronnych i wielostronnych międzynarodowych partnerstw, prowadzenie ponadnarodowej dyskusji oraz rozwijanie i wdrażanie norm dotyczących działania w cyberprzestrzeni"[233].

Warto zauważyć, iż przedstawione przez USA rozwiązania, zwłaszcza te zawarte w punktach dotyczących ochrony sieci, egzekwowania prawa i współpracy wojskowej, są

[231] Grzelak M, Międzynarodowa strategia USA dla cyberprzestrzeni, „Bezpieczeństwo Narodowe" II-2011/18, s. 131
[232] U.S. Department of State, http://www.state.gov/s/cyberissues/, [dostęp: 3.02.2019]
[233] Grzelak M, *op. cit.,* s. 141

komplementarne z zapisami Koncepcji Strategicznej NATO, podpisanej w Lizbonie w roku 2010, oraz z wcześniejszą Konwencją Rady Europy o Cyberprzestępczości z 2001 roku (tzw. Konwencją Budapeszteńską). Pozwala to sądzić, iż propozycja współpracy w ramach Strategii skierowana jest głównie do krajów członkowskich NATO oraz państw UE.

Prezentacja Międzynarodowej Strategii USA dla Cyberprzestrzeni spotkała się z nieprzychylną raczej reakcją opinii publicznej. Kryterium zaufania, mocno podważone za sprawą kontrowersyjnego *Patriot Act*, a także działań administracji prezydenta Busha oraz – choć w znacznie w mniejszym stopniu – prezydenta Obamy na arenie międzynarodowej, wywołało powszechny (i zrozumiały) sceptycyzm co do intencji autorów Strategii. Nie powinno dziwić, że największą jej krytykę wytoczyły Chiny i Rosja, choć odzew w krajach europejskich oraz samych USA także nie należał do pozytywnych. Mimo że autorzy dokumentu nie ukrywali wcale, że przewidują dla Stanów Zjednoczonych rolę lidera zarówno w dziedzinie rozwoju i utrzymania bezpieczeństwa cyberprzestrzeni, jak i w sferze działań o charakterze militarnym, to Strategii zarzucano, iż jest wyrazem amerykańskiej hipokryzji, która pod pozorami partnerskiej współpracy skrywa dążenie do supremacji i zdominowania pozostałych partnerów. Najwyraźniej promowana przez Baracka Obamę i istotnie w pewnym stopniu realizowana idea ‘bezprecedensowego poziomu jawności działania’ nie wystarczyła, by w świadomości globalnej społeczności uznano ją za coś niewiele więcej niż chwyt marketingowy. Tak też niekiedy odbierano samą Strategię – jako rodzaj kampanii promującej nowy wizerunek transparentnej i respektującej prawo do prywatności administracji. Niemniej jednak Międzynarodową Strategię USA dla Cyberprzestrzeni należałoby – jednoznacznie uznać za dokument konstytutywny dla charakteru i kierunków rozwoju współpracy międzynarodowej w zakresie zwalczania cyberterroryzmu.

Rozdział IV

Polityki i strategie ochrony cyberprzestrzeni w Rzeczypospolitej Polskiej

4.1. Strategie Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej przyjęte w latach 1990-2017

4.1.1. Polska przed wstąpieniem do NATO

W pierwszym czasookresie po zmianie ustrojowej w roku 1989 kolejne rządy w zakresie bezpieczeństwa narodowego stawiały sobie za zadanie strategiczne usamodzielnienie Polski po latach funkcjonowania w strefie wpływów Związku Radzieckiego. Prace nad kluczowymi dokumentami służyły redefinicji roli Polski w całkowicie zmienionej perspektywie geopolitycznej oraz umocnieniu bezpieczeństwa kraju i jego obywateli. W początkowym okresie transformacji ramy strategiczne wyznaczały: Doktryna obronna Rzeczypospolitej Polskiej z 1990 roku[234], a także przyjęte w 1992 roku Założenia polskiej polityki bezpieczeństwa oraz Polityka bezpieczeństwa i strategia obronna Rzeczypospolitej Polskiej. Dokumenty te, ich Zapisy tych dokumentów nie stanowią przyczynku do rozważań mieszczących się w zakresie badawczym niniejszej pracy, stąd nie będą poddawane analizie ani też szerzej omawiane, niemniej jednak warto tylko wspomnieć, że w chwili przyjęcia Doktryna ta była już nieaktualna, bowiem zgodnie z jej zapisami Polska nadal funkcjonowała w ramach Układu Warszawskiego, a największe zagrożenie postrzegano w konflikcie między właśnie Układem Warszawskim a NATO. Dokument miał charakter zgodny z koalicyjną doktryną obronną przyjętą przez Doradczy Komitet Polityczny Układu Warszawskiego w Berlinie w 1987 roku, z drugiej strony - w przypadku konfliktu nie zobowiązywał do jakiegokolwiek zaangażowania się Polski po stronie Układu, a wręcz sygnalizował zamiar opuszczenia go.[235]

[234] Uchwała Komitetu Obrony Kraju z dnia 21 lutego 1990 r. w sprawie doktryny obronnej Rzeczypospolitej Polskiej. http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP19900090066, [dostęp: 16.02.2019]

[235] Zapis art. II *Doktryny...*, *op. cit.*, s. 3 stanowi, iż: „Podstawę bezpieczeństwa Narodu Polskiego stanowią jego Siły Zbrojne, odpowiednio przygotowany do obrony organizm państwowy oraz świadome potrzeb obronnych społeczeństwo. Ważnym elementem tego bezpieczeństwa są nadal dwu- i wielostronne sojusze Polski oraz jej przynależność do Układu Warszawskiego, aczkolwiek ich rola może się zmieniać w miarę budowy nowego, ogólnoeuropejskiego systemu bezpieczeństwa"

4.1.2. Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2000 roku[236]

Również i ten dokument z punktu widzenia podjętej tematyki nie wnosi zbyt wiele do kwestii bezpieczeństwa infrastruktury krytycznej w Polsce, niemniej jednak wzmiankowanie o nim podyktowane jest zarówno chronologią, jak i zamiarem wyodrębnienia punktów krytycznych w formułowaniu wizji bezpieczeństwa krajowego. Strategia jest bowiem pierwszą w historii Polski Strategią Bezpieczeństwa Narodowego w warunkach członkostwa w NATO. Dokument ten przyjęto w roku 2000, choć pracę nad jej ramowymi postulatami podjęto już znacznie wcześniej, bo w 1997 roku, niedługo po rozpoczęciu procesu akcesyjnego do Sojuszu. Jednocześnie strona polska brała udział w opracowywaniu uaktualnianej koncepcji strategicznej NATO, której ważnym elementem było właśnie przyjęcie nowych członków. Niemniej jednak Strategię przyjęto nieco ponad rok później niż Polska stała się członkiem Sojuszu. Jak wyjaśnia Stanisław Koziej, powodem opóźnienia było przekonanie, że „lepiej będzie poczekać, aż NATO przyjmie swoją koncepcję strategiczną na szczycie w Waszyngtonie, wtedy, na jej podstawie, będzie można opracować własną strategię. Była to jednakże przesłanka z gruntu błędna. Zasadzała się ona na (chyba podświadomym) traktowaniu sojuszu NATO wedle wzorców Układu Warszawskiego, uznawaniu, że strategia sojusznicza jest nadrzędną w stosunku do strategii narodowej. […]. Ale w NATO […] pierwotne są strategie narodowe, jasno zdefiniowane interesy i cele narodowe oraz środki, jakie państwo wydziela do ich osiągnięcia i dopiero ze zderzenia tychże narodowych strategii wyłania się, w drodze negocjacji i przyjmowana na zasadzie konsensusu, wspólna strategia sojusznicza”[237]. Dostrzeżenie tego faktu pozwala więc skonstatować, iż koncepcja partnerstwa strategicznego, opartego na rzeczywiście na równoważnym członkostwie w organizacji, z równością praw i obowiązków była dla autorów Strategii niekoniecznie wiarygodna. Zdaniem autora to istotna przesłanka w dyskusjach nad rozwojem krajowej koncepcji bezpieczeństwa, wskazuje ona bowiem na fakt, iż tak diametralna zmiana partnerstwa strategicznego (czyli przystąpienie do NATO) znacznie wyprzedziła reorientację świadomości i podejścia polskiej racji stanu.

Dokument koncentruje się na ustaleniu podstaw polskiej polityki bezpieczeństwa, ocenie zagrożeń i wyzwań oraz na określeniu rodzajów aktywności i instrumentów realizacji tej polityki. Definiował on również podstawy strategii obronności, które zostały rozwinięte w odrębnym

[236] https://www.academia.edu/19961908/Strategia_Obronna_RP_z_2000_r, [dostęp: 16.02.2019]
[237] Koziej S., Brzozowski A., *25 lat polskiej strategii bezpieczeństwa,* [w:] „Bezpieczeństwo Narodowe”, II-2014/30, s. 13.

dokumencie. Strategię tę, przygotowaną przez MSZ, charakteryzowała pewna niekonsekwencja, jako że ograniczała się ona w zasadzie jedynie do dwóch dziedzin bezpieczeństwa państwa, a mianowicie polityki zagranicznej i obronności. Niestety, całkowicie zrezygnowano z zajmowania się innymi dziedzinami bezpieczeństwa narodowego, z kontekstu szerszej perspektywy społecznej, nie wspominając o jakiejkolwiek formie koordynacji działań.

4.1.3. Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2003 roku[238]

Opracowana w 2003 roku Strategia Bezpieczeństwa RP zawierała „oficjalną i obowiązującą wykładnię podejścia państwa do spraw swego bezpieczeństwa, w tym ocenę wyzwań i zagrożeń, koncepcję działania państwa w sferze bezpieczeństwa, zadania poszczególnych służb państwowych oraz gospodarki narodowej". Dokument zastąpił omawianą powyżej Strategię bezpieczeństwa RP z 2000 roku i został przedłożony do podpisu Prezydentowi RP, co różni go od uprzedniego mającego status dokumentu tylko rządowego. Jest to także pierwszy dokument o charakterze strategicznym, w którym nadmienia się o „zagrożeniach w sferze teleinformatycznej", które autorzy definiują jako „operacje mające na celu dezorganizację systemów informacyjnych instytucji rządowych i samorządowych, a także niektórych sfer sektora prywatnego, związanych z systemem bezpieczeństwa państwa"[239]. W celu przeciwdziałania im, Strategia zaleca ochronę infrastruktury krytycznej rządowej i samorządowej (i tu również należy zauważyć, iż jest to istotne, acz niekoniecznie zrozumiałe zawężenie tego terminu) „przez wyspecjalizowane komórki cywilne i wojskowe służb państwowych przeciwko działaniu ze strony obcych służb specjalnych a także ugrupowań terrorystycznych, ekstremistycznych i zorganizowanych grup przestępczych. Zagrożenia powstają w wyniku penetracji baz danych oraz prowadzenia działań dezinformacyjnych polskiej opinii publicznej oraz społeczeństwa"[240].

Znawcy przedmiotu zwracają uwagę, że Strategię należy oceniać jako próbę wypracowania zintegrowanego podejścia do kwestii bezpieczeństwa narodowego. Traktuje ona bowiem bezpieczeństwo narodowe jako „kategorię obejmującą wszystkie aspekty i dziedziny bezpieczeństwa państwa: zewnętrzne i wewnętrzne, wojskowe i cywilne […][241]. W istocie jednak trudno dostrzec *expressis verbis* owo „zintegrowane pojęcie" w zapisach Strategii, gdyż

[238] Koziej S, *Strategie Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2003 i 2007 roku,* Warszawa 2008, s.4. II – 2014/30, BBN, Warszawa 20154, s. 15
[239] Trejnis Z, Trejnis P.Z., *Polityka ochrony cyberprzestrzeni w państwie współczesnym* [w:] *Studia Bobolanum 28 nr 3, Warszawa 2017, s. 29*
[240] *Ibidem.*
[241] Koziej S., *op. cit*., s. 5

dokument raczej zestawia ze sobą, niż łączy w całość, podejścia poszczególnych resortów. A jak zauważył Stanisław Koziej, „nie został m.in. wyodrębniony rozdział traktujący o interesach i strategicznych celach bezpieczeństwa Polski. Mało – w całej strategii w ogóle nie padają słowa <<interesy narodowe>>. Jest to o tyle dziwne, że właśnie interesy narodowe i potrzeba zapewnienia możliwości ich realizacji są najbardziej pierwotną przyczyną wszelkiego myślenia o bezpieczeństwie narodowym”[242].

Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej przyjęta, jak wspomniano w roku 2003, jest dokumentem państwa będącego już członkiem NATO, co diametralnie zredefiniowało pozycję Polski w europejskim, ale i światowym układzie sił. Jako kraj członkowski Sojuszu Polska posiadała już wiarygodne gwarancje bezpieczeństwa, choć jednocześnie została narażona na nowy typ zagrożeń (wynikających właśnie z członkostwa), a związanych głównie z Rosją, niestabilnością niektórych państw dawnego Układu Warszawskiego oraz międzynarodowym terroryzm. Sytuacja na Bałkanach, w byłych republikach kaukaskich ZSRR również stanowiła przyczynę napięć międzynarodowych i stwarzała ryzyko wybuchu konfliktu na większą skalę. Autorzy Strategii wyraźnie podkreślają jednak, że pomimo szeregu różnorodnych zagrożeń kierunek zmian w euroatlantyckim systemie bezpieczeństwa jest pozytywny z tendencją do utrwalenia jego stabilności. „Istota zmian w […] środowisku bezpieczeństwa polega […] na przesuwaniu się punktu ciężkości z zagrożeń klasycznych (inwazja zbrojna), których znaczenie się zmniejsza, na zagrożenia nietypowe, których źródłem stają się także trudne do zidentyfikowania podmioty pozapaństwowe. Zagrożenia te mogą dotyczyć bezpieczeństwa naszych obywateli, obiektów oraz służb istotnych dla sprawnego funkcjonowania państwa” [243].

Strategia ostrzega także, iż stale rośnie zagrożenie zarówno próbami uzyskania nieuprawnionego dostępu do niejawnych zasobów informacyjnych (również tych związanych z obecnością Polski w NATO), jak i „operacjami dezorganizację kluczowych systemów informacyjnych instytucji rządowych oraz niektórych sfer sektora prywatnego, oddziałujących na system bezpieczeństwa państwa, a także operacjami związanymi z penetracją baz danych i prowadzeniem działań dezinformacyjnych”[244]. Za szczególnie istotny przyczynek do uwzględnienia w przyszłych działaniach dotyczących ochrony infrastruktury krytycznej należy

[242] *Ibidem.*
[243] Ibidem, s. 8.
[244] Trejnis Z, Trejnis P.Z, *op. cit.,* s. 36

uznać konstatację dotyczącą potrzeby utworzenia państwowego kompleksowego systemu reagowania kryzysowego, który będzie odpowiadał na potrzeby wynikające z zagrożenia bezpieczeństwa zarówno międzynarodowego, jak i wewnętrznego. W myśl zapisów Strategii „odpowiednie instytucje państwowe będą prowadzić działania zmierzające do powołania zintegrowanego systemu kierowania i zarządzania na wypadek kryzysu. Niezbędne staje się spójne uregulowanie zadań i kompetencji organów i instytucji państwowych, a także organizacji społecznych działających na rzecz bezpieczeństwa państwa"[245]. Dokument ten stanowi też intencjonalną, acz dość ściśle sprecyzowaną wykładnię dotyczącą roli państwa w ochronie bezpieczeństwa infrastruktury krytycznej (choć tego terminu nie użyto w dokumencie, zastąpiwszy go sformułowaniem „zaplecze społeczno-gospodarcze"). „Polegać ma ona przede wszystkim na zapewnianiu materialnych podstaw realizacji zadań obronnych, w tym na tworzeniu i utrzymywaniu rezerw państwowych, gospodarczych i mobilizacyjnych, zagwarantowaniu zaopatrzenia w żywność, dostaw energii i surowców energetycznych, utrzymywaniu infrastruktury obronnej"[246].

4.1.4. Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2007 roku[247]

Prace nad nową Strategią rozpoczęły się w lutym 2006 roku, jednakże jej przyjęcie nastąpiło znacznie później, bo w kwietniu 2007 roku, a prezydent Lech Kaczyński podpisał go jeszcze później – w listopadzie 2007 – czyli tuż po ówczesnych wyborach parlamentarnych, kiedy rządu RP właściwie nie było, a sam wynik wyborów przyniósł dużą zmianę na scenie politycznej. W konsekwencji w dniu przyjęcia Strategia zakładała inne cele niż te, które stawiał sobie nowy rząd, zatem jej założenia nie były w pełni realizowane, stąd nowelizacja została zaplanowana już na 2009 rok. Pomimo tego faktu, *Strategię Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2007 roku* należy uznać za bardzo istotny dokument z uwagi na zauważalną zmianę podejścia intencyjnego do kwestii bezpieczeństwa narodowego, zaś sama jego konstrukcja merytoryczna zapowiada objęcie znacznie szerszego spektrum zagadnień, niż miało to miejsce w przypadku dokumentów poprzedzających. Kolejne rozdziały poświęcone są interesom narodowym i celom

[245] Koziej S., *op. cit*., s. 13.
[246] *Ibidem*.
[247] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, przyjęta przez Radę Ministrów w dniu 9 kwietnia 2007 r., a zatwierdzona przez Prezydenta RP w dniu 13 listopada 2007 r, https://www.msz.gov.pl/resource/7d18e04d-8f23-4128-84b9-4f426346a112, [dostęp: 20.02.2019]

strategicznym w dziedzinie bezpieczeństwa, ocenie środowiska bezpieczeństwa Rzeczypospolitej Polskiej oraz sformułowaniu operacyjnej koncepcji strategii bezpieczeństwa[248].

Szczególnie istotnym wyrazem nowego podejścia, czyli próby stworzenia zintegrowanego podejścia do elementów polityki bezpieczeństwa narodowego, wydaje się wprowadzenie kategoryzacji interesów narodowych usystematyzowanych w trzech grupach[249]:

- żywotne interesy RP – determinujące zapewnienie przetrwania państwa i jego obywateli (potrzeba zachowania niepodległości i suwerenności państwa, jego integralności terytorialnej i nienaruszalności granic oraz zapewnienia praw człowieka i podstawowych wolności, a także umacnianie demokratycznego porządku prawnego);
- ważne interesy RP – gwarantujące trwały i zrównoważony rozwój cywilizacyjny oraz gospodarczy kraju, stworzenie warunków do wzrostu dobrobytu mieszkańców, do rozwoju nauki i techniki oraz do ochrony dziedzictwa narodowego i tożsamości narodowej, a także środowiska naturalnego;
- inne istotne interesy RP – związane z dążeniem do zapewnienia silnej pozycji międzynarodowej państwa oraz możliwości skutecznego promowania polskich interesów na arenie międzynarodowej[250].

Najistotniejszą jednak – zdaniem autora – innowacją (a jednocześnie dowodem na ustabilizowanie się w świadomości twórców obecności Polski w NATO) jest przypisanie Strategii w roli nadrzędnego dokumentu koncepcyjnego, czyli strategii bezpieczeństwa narodowego, którego zapisy implikują treści wykonawczych dokumentów planistycznych. Schemat ten, obecny w strategicznym zarządzaniu bezpieczeństwem wielu państw, zwłaszcza członków NATO, będzie odtąd stałym elementem polskiej polityki bezpieczeństwa.

4.1.5. Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2014 roku[251]

W grudniu 2010 roku rozpoczął się Strategiczny Przegląd Bezpieczeństwa Narodowego, którego wnioski zawarte w Raporcie Komisji SPBN stanowiły punkt wyjścia do pracy nad Strategią Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej. Przegląd ten zakończono w grudniu 2012 roku i – jak zapisano w jej preambule – był to „pierwszy tak szeroko zakrojony

[248] *Ibidem*, pkt 7-10
[249] *Ibidem*, pkt. 11-13
[250] Koziej S., Brzozowski A., *op. cit.,* s. 32.
[251] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, przyjęta przez Radę Ministrów w dniu 9 kwietnia 2007 r., a zatwierdzona przez Prezydenta RP w dniu 13 listopada 2007 r, https://www.msz.gov.pl/resource/7d18e04d-8f23-4128-84b9-4f426346a112, [dostęp: 20.02.2019]

projekt analityczny odnoszący się do stanu systemu bezpieczeństwa narodowego i kierunków jego rozwoju"[252]. Prezydent Bronisław Komorowski przyjął Strategię 5 listopada 2014 roku, tym samym pozbawiając mocy prawnej Strategii Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z roku 2007. „Dokument identyfikuje interesy narodowe i cele strategiczne w dziedzinie bezpieczeństwa, w zgodzie z zasadami i wartościami zawartymi w Konstytucji Rzeczypospolitej Polskiej. Określa potencjał bezpieczeństwa narodowego oraz ocenia środowisko bezpieczeństwa Polski w wymiarze globalnym, regionalnym i krajowym, a także prognozuje jego trendy rozwojowe. Przedstawia działania państwa niezbędne dla osiągnięcia zdefiniowanych interesów i celów oraz wskazuje kierunki i sposoby przygotowania systemu bezpieczeństwa narodowego. Zapisy dokumentu są zbieżne ze strategiami Organizacji Traktatu Północnoatlantyckiego (NATO) i Unii Europejskiej (UE) oraz dokumentami strategicznymi tworzącymi nowy system zarządzania rozwojem kraju […]"[253].

Analizując Strategię Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2014 roku, z pewnością warto pochylić się nad konstrukcją tego dokumentu oraz nieco więcej uwagi poświęcić kilku konkretnym zapisom z uwagi na ich istotność dla podjętego w temacie pracy zagadnienia.

W zakresie interesów narodowych RP (Rozdział I) Strategia. odwołuje się do art. 5 Konstytucji RP[254] Traktuje on o konieczności posiadania skutecznego potencjału bezpieczeństwa, silnej pozycji Polski na arenie międzynarodowej, ochronie indywidualnej i zbiorowej obywateli i zapewnienie im swobody korzystania z wolności i praw oraz zapewnienie trwałego i zrównoważonego rozwoju potencjału społecznego i gospodarczego państwa. „Na tej podstawie Strategia formułuje cele strategiczne w dziedzinie bezpieczeństwa, stawiając na pierwszym miejscu utrzymywanie i demonstrowanie gotowości zintegrowanego systemu bezpieczeństwa narodowego do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania zagrożeniom […]. Wskazując elementy strategicznego potencjału bezpieczeństwa narodowego Strategia wskazuje na kluczowe znaczenie systemu bezpieczeństwa narodowego rozumianego jako siły i środki przeznaczone do realizacji zadań i osiągania celów strategicznych w sferze bezpieczeństwa"[255].

[252] *Ibidem*, s. 7.
[253] *Ibidem*.
[254] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970780483* [dostęp: 21.02.2019]
[255] Aleksandrowicz T., *Strategia Bezpieczeństwa Narodowego RP [w;] „*Wszystko Co Najważniejsze", 11/14, Warszawa

Poddając ocenie warunki geopolityczne, w jakich znajduje się Polska (Rozdział II), autorzy Strategii przyjęli aktualne założenie, że zarówno globalizacja, jak i będąca jej skutkiem coraz większa współzależność państw determinują pojawienie się szeregu nowych zagrożeń dla bezpieczeństwa krajowego.

Charakter i zasięg tych zagrożeń nie jest określony barierami geograficznymi, systemami politycznymi czy gospodarczymi, oddziałują bowiem na wiele systemów państwa jednocześnie, są asymetryczne. „Wśród zagrożeń na poziomie globalnym Strategia wymienia także terroryzm i zorganizowaną przestępczość, cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych oraz cyberwojny – konfrontację w cyberprzestrzeni pomiędzy państwami, a także ekstremizm”[256].. Odnotować należy, iż termin ’bezpieczeństwo narodowe’ jest przez autorów rozumiany interdyscyplinarnie i kompleksowo, gdzie za jego elementy uważa się także kwestie demograficzne, wykształcenie społeczeństwa, rozwój nauki i szkolnictwa, a nawet bezpieczeństwo ruchu drogowego i imprez masowych.

W części poświęconej Strategii Operacyjnej (Rozdział III), Strategia określa priorytety polityki bezpieczeństwa, podkreślając, że podstawowym warunkiem ich realizacji jest społeczne przyzwolenie i polityczne porozumienie co do nadrzędnego traktowania spraw bezpieczeństwa narodowego w polityce państwa. Najważniejsze wektory działań strategicznych na poziomie operacyjnym wyznaczają trzy priorytety*:*

- „zapewnienie gotowości i demonstracja determinacji do działania w sferze bezpieczeństwa i obrony oraz wzmocnienie narodowych zdolności obronnych, ze szczególnym uwzględnieniem tych obszarów bezpieczeństwa narodowego, w których działania sojusznicze mogą być utrudnione;
- wspieranie procesów służących wzmocnieniu zdolności NATO do kolektywnej obrony, rozwój Wspólnej Polityki Bezpieczeństwa i Obrony Unii Europejskiej, umacnianie strategicznych partnerstw (w tym z USA) oraz strategicznych relacji z partnerami w regionie;
- wspieranie i selektywny udział w działaniach społeczności międzynarodowej, realizowanych na podstawie norm prawa międzynarodowego, mających na celu

[256] Aleksandrowicz T., *op. cit.,* s. 4.

zapobieganie powstawaniu nowych źródeł zagrożeń, reagowaniu na zaistniałe kryzysy oraz przeciwdziałanie ich rozprzestrzenianiu się”[257].

Natomiast w rozdziale IV, odnoszącym się do strategii preparacyjnej, przedstawiono koncepcję przygotowań strategicznych. W jej ramach wykazano konieczność integracji w systemie bezpieczeństwa narodowego struktur militarnych i pozamilitarnych. Również i w tej części Strategia określa trzy priorytety:

- „integracja podsystemów kierowania bezpieczeństwem narodowym;
- profesjonalizacja podsystemów operacyjnych – obronnego i ochronnych;
- powszechność przygotowań podsystemów wsparcia – społecznych i gospodarczych”[258].

W punktach 1.2 (Cele strategiczne w dziedzinie bezpieczeństwa) oraz 1.3. (Strategiczny potencjał bezpieczeństwa narodowego) dokument wymienia szereg postulowanych działań związanych pośrednio z ochroną infrastruktury krytycznej, choć po raz kolejny termin ten nie jest jeszcze użyty. Punkty: 1.2.7, czyli „zapewnienie bezpieczeństwa powszechnego poprzez doskonalenie krajowego systemu ratowniczo-gaśniczego oraz systemu monitorowania, powiadamiania, ostrzegania o zagrożeniach i likwidowania skutków klęsk żywiołowych oraz katastrof, a także wdrożenie rozwiązań prawnych i organizacyjnych w zakresie systemu ochrony ludności oraz obrony cywilnej”[259], 1.2.8 „doskonalenie i rozwój krajowego systemu zarządzania kryzysowego w kierunku zapewnienia jego wewnętrznej spójności i integralności oraz umożliwienia niezakłóconej współpracy w ramach systemów zarządzania kryzysowego organizacji międzynarodowych”[260] oraz 1.2.11 „czyli zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni[261] dotyczą zagadnień bezpieczeństwa infrastruktury krytycznej, jednakże warto w tym miejscu podkreślić, że w stopniu niewystarczającym.

Opisując zadania stojące przed Polską w zakresie bezpieczeństwa w wymiarze regionalnym, w punkcie 1.4.47 Strategia nadmienia o znaczeniu cyberprzestrzeni – ocenione jest ono jako rosnące, jak i rosnąca jest też odpowiedzialność państw za jej ochronę. „Istotne znaczenie dla zwiększenia poziomu bezpieczeństwa Rzeczypospolitej Polskiej w

[257] *Ibidem,* s. 5.
[258] *Ibidem,* s. 5.
[259] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, przyjęta przez Radę Ministrów w dniu 9 kwietnia 2007 r zatwierdzona przez Prezydenta RP w dniu 13 listopada 2007 r,* [dostęp: 20.02.2019], s. 12.
[260] *Ibidem.*
[261] *Ibidem.*

cyberprzestrzeni ma polityka organizacji i struktur współpracy międzynarodowej, w pracach, w których Polska uczestniczy oraz współpraca dwustronna z wybranymi państwami, w szczególności z państwami NATO i UE"[262]. Z kolei wśród zadań o wymiarze krajowym, w punkcie 2.4.56 autorzy Strategii nadmieniają, iż „rosnąca pozycja Polski na arenie międzynarodowej oraz członkostwo w NATO i UE wpływają na zwiększone zainteresowanie obcych służb wywiadowczych naszym krajem. Ewentualne nieuprawnione ujawnienie czy kradzież informacji niejawnych oraz innych chronionych prawem danych może spowodować straty dla bezpieczeństwa narodowego i interesów Rzeczypospolitej Polskiej"[263]. Szczególną uwagę zwraca punkt 2.3.55, który jedynie wspomina o zagrożeniu terroryzmem i to nawet nie państwowym czy międzynarodowym, ponieważ – zdaniem autorów – „szczególnie niebezpieczne mogą okazać się pojedyncze osoby lub małe grupy osób wykorzystujące metody terroru jako narzędzia do realizowania własnych celów o podłożu politycznym, społecznym, ekonomicznym lub religijnym"[264]. Warto w tym miejscu skonstatować, że śledząc na przestrzeni ostatnich dekad proces wyodrębniania się na forum międzynarodowym kwestii zagrożenia terroryzmem, który w tej pracy został wcześniej nakreślony, zaprezentowane w tym dokumencie rozumienie terroryzmu i jego charakteru (w 2014 roku) może przyprawiać o zdumienie. Punkt 2.3.57 dotyczy z kolei bezpiecznego funkcjonowania systemu teleinformatycznego Rzeczypospolitej Polskiej, a w ocenie autorów jest ono „warunkiem niezakłóconego działania całego państwa. Wyzwaniem pozostaje zapewnienie dostępności, integralności i poufności danych przetwarzanych w systemach teleinformatycznych administracji publicznej oraz brak jednolitych zabezpieczeń teleinformatycznych. Istotne znaczenie z punktu widzenia bezpieczeństwa ma niewystarczająca wiedza użytkowników o zagrożeniach w cyberprzestrzeni oraz konieczność rozwiązania dylematu pomiędzy wolnością osobistą i ochroną praw jednostki, a stosowaniem środków służących zachowaniu bezpieczeństwa państwa"[265].

Kolejny, trzeci rozdział Strategii poświęcony koncepcji działań strategicznych na poziomie operacyjnym, zawiera postulat zwiększenia zdolności Sił Zbrojnych RP do walki w cyberprzestrzeni. Zgodnie z założeniami, muszą one „dysponować zdolnościami defensywnymi i ofensywnymi w tej sferze, tak aby realizować funkcję odstraszania potencjalnego przeciwnika.

[262] *Ibidem, s. 23.*
[263] *Ibidem, s. 25*
[264] *Ibidem.*
[265] *Ibidem.*

W szczególności muszą być one gotowe, samodzielnie i we współpracy z sojusznikami, do prowadzenia operacji ochronnych i obronnych na większą skalę w razie cyberkonfliktu lub cyberwojny”[266]. W zakresie działań ochronnych natomiast (Punkt 3.2.84) do najważniejszych zadań Strategia zalicza zapewnienie „bezpieczeństwa Polski w cyberprzestrzeni, w tym bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej. […] Powinno być ono realizowane zarówno poprzez rozwój zdolności do działań defensywnych (obejmujących ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni), jak i ofensywnych. Szczególnie ważna jest: współpraca i koordynacja działań ochronnych z podmiotami sektora prywatnego – przede wszystkim finansowego, energetycznego, transportowego, telekomunikacyjnego i opieki zdrowotnej; prowadzenie działań o charakterze prewencyjnym i profilaktycznym w odniesieniu do zagrożeń w cyberprzestrzeni; wypracowanie i stosowanie właściwych procedur komunikacji społecznej w tym zakresie; rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców; prowadzenie walki informacyjnej w cyberprzestrzeni; współpraca sojusznicza, także na poziomie działalności operacyjnej służącej do aktywnego zwalczania cyberprzestępstw, w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych”[267]. Punkt 3.2.85 porusza kwestię bezpieczeństwa informacyjnego, a strategiczne zadania państwa w zakresie jego ochrony obejmują „zapewnienie bezpieczeństwa informacyjnego państwa poprzez zapobieganie uzyskaniu nieuprawnionego dostępu do informacji niejawnych i ich ujawnieniu; zapewnianie personalnego, technicznego i fizycznego bezpieczeństwa informacji niejawnych; akredytację systemów teleinformatycznych służących przetwarzaniu tych informacji; zapewnienie realizacji funkcji krajowej władzy bezpieczeństwa w celu umożliwienia międzynarodowej wymiany informacji niejawnych”[268].

Ostatnimi z bardzo istotnych (z perspektywy tematyki niniejszego opracowania) zapisów Strategii są: punkt 3.2.86 poświęcony ochronie infrastruktury krytycznej państwa: „[…) ochrona infrastruktury krytycznej jest obowiązkiem operatorów i właścicieli, którzy są wspierani przez potencjał administracji publicznej. W Polsce wdrażane jest nowatorskie podejście w tym zakresie, bazujące na zasadach współodpowiedzialności zainteresowanych stron, rozbudowanej współpracy i wzajemnego zaufania. Działania państwa polegają na ewentualnym uruchomieniu

[266] *Ibidem, s. 32.*
[267] *Ibidem, s. 33-34.*
[268] *Ibidem, s. 35.*

sytemu zarządzania kryzysowego na wypadek zakłócenia funkcjonowania infrastruktury krytycznej, a także na podnoszeniu świadomości, wiedzy i kompetencji oraz propagowaniu współpracy w tym obszarze"[269] oraz punkt 4.3.132. (podsystemy ochronne – Instytucje ochrony infrastruktury krytycznej), w myśl którego „ochrona kluczowej infrastruktury państwa wymaga uporządkowania przepisów w celu stworzenia jednej kategorii obiektów infrastruktury krytycznej. Wiązać się to będzie z potrzebą zmian zarówno w przepisach dotyczących obiektów podlegających obowiązkowej ochronie, jak i obiektów podlegających szczególnej ochronie. Spójne przepisy zagwarantują podniesienie odporności wszystkich elementów infrastruktury krytycznej, za co odpowiadać powinien powołany ustawowo organ do spraw ochrony infrastruktury krytycznej. Nowe przepisy powinny również stworzyć system realnych zachęt dla właścicieli infrastruktury krytycznej do inwestowania w bezpieczeństwo"[270].

Podsumowując, należy uznać, iż Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2014 roku jest znaczącą zmianą jakościową w stosunku do dokumentów poprzedzających. Prezentuje komplementarne podejście do poruszanego zakresu tematycznego, przez co stanowić mogłaby dobry punkt wyjścia dla realizacji zadania stworzenia sprawnie działającego systemu bezpieczeństwa narodowego. „Przedstawiając środowisko bezpieczeństwa Polski w wymiarze globalnym, regionalnym i krajowym, podkreśla znaczenie bezpieczeństwa w cyberprzestrzeni oraz zwraca uwagę, że wraz z rozwojem sieci Internet pojawiły się nowe zagrożenia, mogące poważnie zakłócić funkcjonowanie społeczeństw i państw, takie jak: cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty, z udziałem podmiotów niepaństwowych, i cyberwojna rozumiana jako konfrontacja między państwami"[271].Niemniej jednak zauważyć należy także, iż owo „nowatorskie spojrzenie" na kwestię ochrony IK okazać się może źródłem wielu niejasności i komplikacji interpretacyjnych – tematyka ta podjęta zostanie w rozdziale VII.

[269] *Ibidem.*
[270] *Ibidem, s. 50.*
[271] Trejnis Z, Trejnis P.Z, *op. cit.,* s. 31.

4.2. Polityki i programy ochrony cyberprzestrzeni Rzeczpospolitej Polskiej

4.2.1. Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2009-2011[272]

W dniu 9 marca 2009 Komitet Stały Rady Ministrów przyjął dokument zatytułowany *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia*. Prace zostały zainicjowane przez Agencję Bezpieczeństwa Wewnętrznego i Ministerstwo Spraw Wewnętrznych i Administracji w związku z narastającymi na świecie zagrożeniami w obszarze szeroko pojętej teleinformatyki. W celu uzasadnienia podjętych nad programem prac powołano się między innymi na: cyberatak na Estonię, blokadę teleinformatyczną Gruzji, kradzież danych osobowych w Anglii, ataki hackerskie na portale administracji publicznej i banki w wielu krajach. Przyjęcie tego dokumentu można uznać za początek kierunkowych działań legislacyjnych rządu oraz administracji państwowej na rzecz zapewnienia bezpieczeństwa cyberprzestrzeni.

Jak podają we wprowadzeniu jego autorzy, celem strategicznym Programu jest wzrost poziomu bezpieczeństwa cyberprzestrzeni państwa. „Osiągnięcie celu strategicznego wymaga stworzenia ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy podmiotami administracji publicznej oraz innymi podmiotami, których zasoby stanowią krytyczną infrastrukturę teleinformatyczną kraju, na wypadek ataków terrorystycznych wykorzystujących publiczne sieci teleinformatyczne”[273]. W dokumencie zawarto propozycje działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności do zapobiegania i zwalczania cyberterroryzmu oraz innych pochodzących z publicznych sieci teleinformatycznych zagrożeń dla państwa.

Wprowadzenie zawiera też definicje cyberterroryzmu, cyberprzestrzeni oraz cyberprzestrzeni RP, i choć w intencji autorów są one obowiązujące jedynie w zakresie opracowania, to jednak po raz pierwszy pojawiają się one w rządowym dokumencie o charakterze strategiczno-programowym. Autorzy Programu postulują zresztą konieczność prawnego zdefiniowania tych terminów, zauważając, iż „brak precyzyjnych definicji może powodować wątpliwości polegające na trudności w ustaleniu organu właściwego dla ścigania sprawców cyberprzestępstwa”[274], zaś w tekście dokumentu proponują następujące zapisy:

[272] https://www.msz.gov.pl/resource/93e1e4c7-e129-41c7-8365-39dbad8b1c54:JCR [dostęp: 22.02.2019]
[273] *Ibidem,* s. 4
[274] *Ibidem.*

- cyberprzestrzeń rozumiana jako „przestrzeń komunikacyjna tworzona przez system powiązań internetowych”;
- jako cyberprzestrzeń państwa przyjmuje się „przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa. Cyberprzestrzeń państwa w przypadku Polski określana jest również mianem cyberprzestrzeni RP. Cyberprzestrzeń RP obejmuje między innymi systemy, sieci i usługi teleinformatyczne o szczególnie ważnym znaczeniu dla bezpieczeństwa wewnętrznego państwa, system bankowy, a także systemy zapewniające funkcjonowanie w kraju transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz systemy informatyczne”;
- cyberterroryzm, czyli „terroryzm wymierzony przeciwko newralgicznym dla państwa systemom, sieciom i usługom teleinformatycznym, stanowi kluczową i stale rosnącą postać ataków terrorystycznych”. W świetle dotychczasowych rozważań definicja ta budzi pewną niezgodę, gdyż przeciwko „newralgicznym dla państwa systemom, sieciom i usługom teleinformatycznym” atak można również przeprowadzić w konwencjonalny sposób i z całą pewnością nie będzie to atak cyberterrorystyczny.

Rzeczony Program zawiera sześć celów szczegółowych, z czego najistotniejsze wydają się cztery wymienione poniżej:

a. „zwiększenie poziomu bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa skutkujące zwiększeniem poziomu odporności państwa na ataki cyberterrorystyczne,
b. stworzenie i realizacja spójnej dla wszystkich zaangażowanych podmiotów administracji publicznej oraz innych współstanowiących krytyczną infrastrukturę teleinformatyczną państwa polityki dotyczącej bezpieczeństwa cyberprzestrzeni,
c. zmniejszenie skutków ataków cyberterrorystycznych, a przez to kosztów usuwania ich następstw,
d. stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami odpowiedzialnymi za zapewnianie bezpieczeństwa cyberprzestrzeni państwa oraz władającymi zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa […]” [275].

[275] *Ibidem,* s. 4

Adresatami programu są przed wszystkim organy administracji publicznej, jak i inne podmioty zarządzające zasobami krytycznej infrastruktury teleinformatycznej państwa, ale też beneficjenci systemów, sieci i usług teleinformatycznych stanowiących krytyczną infrastrukturę teleinformatyczną państwa. W intencji autorów Program ma być jednak adresowany do wszystkich obywateli Rzeczpospolitej Polskiej, zakłada też ścisłą współpracę „realizatorów programu" z sektorem prywatnym, czyli „operatorami telekomunikacyjnymi dysponujących infrastrukturą telekomunikacyjną stanowiącą podstawę zapewnienia komunikacji w państwie. Należy jednak podkreślić, że zagadnienie ochrony cyberprzestrzeni nie dotyczy jedynie sfery teleinformatycznej, ale również sfery innych usług, np. usług sektora bankowego"[276]. Realizatorami programu będą natomiast „[…] podmioty odpowiedzialne za ochronę infrastruktury krytycznej kraju, w tym przede wszystkim krytycznej infrastruktury teleinformatycznej. Z tego względu wiodące role w realizacji programu odgrywać będą: Ministerstwo Spraw Wewnętrznych i Administracji (MSWiA) jako podmiot odpowiedzialny za informatyzację państwa oraz infrastrukturę krytyczną oraz Agencja Bezpieczeństwa Wewnętrznego (ABW) jako podmiot odpowiedzialny za bezpieczeństwo wewnętrzne państwa. Ponieważ jedynie nieznaczna część infrastruktury krytycznej, w tym teleinformatycznej, jest własnością państwa, natomiast większość zasobów stanowi własność prywatną, dużą rolę w realizacji programu powinny mieć te podmioty prywatne, które są właścicielami zasobów stanowiących infrastrukturę państwa"[277].

4.2.2. Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016

Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011- 2016 zawiera trzy podstawowe założenia działań: w sferze technicznej, edukacyjnej oraz organizacyjno-prawnej. „Odbiorcami programu są obywatele polscy mieszkający i korzystający z sieci poza granicami kraju oraz wszyscy użytkownicy sieci na terytorium państwa. Zaproponowane rozwiązanie przewiduje wypracowanie i skuteczne wdrożenie regulacji prawnych, określających miejsce i rolę instytucji prawnych w obszarze cyberprzestrzeni, ale również definiujących rolę zwykłych użytkowników sieci. Do istotnych założeń programu zalicza

[276] *Ibidem*, s. 24
[277] *Ibidem*.

się wypracowanie systemu, który miałby ułatwić i zabezpieczyć proces wymiany informacji pomiędzy prywatnym sektorem i publicznym”[278]. W obszarze technicznym programu podejmowane są badania naukowe dotyczące rozwoju ochrony cyberprzestrzeni kraju oraz organizowane szkolenia. Edukacja ta dotyczy przede wszystkim urzędników oraz funkcjonariuszy i instytucji, na których spoczywa zapewnienie cyberbezpieczeństwa. Zmiany wprowadzone w kwestii funkcjonalno-organizacyjnej pozwalały na delegowanie zadań i podział odpowiedzialności za bezpieczeństwo w cyberprzestrzeni. Sprecyzowany podział ról i kompetencji usprawnia funkcjonowanie mechanizmu obronnego i umożliwia tym samym szybsze reagowanie na pojawiające się zagrożenie.

Warto odnotować kilka definicji, które autorzy zamieścili w Programie, bezpośrednio związanych z tematyką niniejszej pracy:

- „Cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.
- Cyberprzestrzeń RP) – cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe).
- Cyberprzestępstwo – czyn zabroniony popełniony w obszarze cyberprzestrzeni.
- Cyberterroryzm – cyberprzestępstwo o charakterze terrorystycznym.
- Cyberatak – celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni, bez konieczności angażowania personelu lub innych użytkowników. Umożliwia ominięcie lub osłabienie sprzętowych i programowych mechanizmów kontroli dostępu.
- Krytyczna infrastruktura teleinformatyczna – infrastruktura krytyczna wyodrębniona w systemie łączności i sieciach teleinformatycznych i ujawniona w wykazie Infrastruktury Krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym.
- Ochrona cyberprzestrzeni – zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu niezakłócone funkcjonowanie i bezpieczeństwo cyberprzestrzeni.

[278] El Ghamari M., *Ochrona cybeprzestrzeni – wyzwanie naszych czasów?* BiTP Vol. 49 Issue 1, 2018, pp. 24–33, doi: 10.12845/bitp.49.1.2018.2; [dostęp: 22.02.2019]

- Operator teleinformatycznej infrastruktury krytycznej – właściciel oraz posiadacz samoistny i zależny obiektów, instalacji, urządzeń i usług infrastruktury krytycznej, wyodrębnionych w systemie łączności i sieci teleinformatycznych i ujawnionych w wykazie infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym.
- Punkt sektorowy – punkt kontaktu pomiędzy podmiotami działającymi w tej samej branży umożliwiający przepływ informacji pomiędzy nimi a właściwymi zespołami CERT lub Abuse"[279].

4.2.3. Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 roku[280]

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, przyjęta w 2013 roku przez Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego, jest pierwszym krajowym dokumentem o charakterze strategicznym dotyczącym ściśle kwestii cyberbezpieczeństwa. Opracowana i przyjęta w 2013 roku Polityka. miała stać się podstawą działań na rzecz cyberbezpieczeństwa dla administracji rządowej i samorządowej, innych podmiotów państwowych, ale też dla wszystkich użytkowników cyberprzestrzeni, jak na przykład prywatni przedsiębiorcy czy operatorzy infrastruktury krytycznej. Wniosła ona, oprócz jednolitej definicji 'cyberprzestrzeni' określonej tu jako „przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformacyjne, określone w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne"[281], także próbę kodyfikacji tego pojęcia zawężonego terytorialnie do granic państwa, czyli „cyberprzestrzeni Rzeczpospolitej Polskiej". Tym samym dokument ten wiąże pojęcie cyberprzestrzeni z terytorium państwa polskiego w ujęciu zarówno fizycznym, jak i prawnym. Oznacza to, iż cyfrowa przestrzeń wirtualna może być traktowana jako terytorium określonego granicami państwa. Celem strategicznym Polityki jest „osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa. Osiągnięcie celu strategicznego jest realizowane poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami CRP (Cyberprzestrzeni Rzeczpospolitej Polskiej). Działania podejmowane w celu realizacji celu strategicznego są

[279] https://www.msz.gov.pl/resource/93e1e4c7-e129-41c7-8365-39dbad8b1c54:JCRm
[280] *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* z 25 czerwca 2013 r, https://cyberpolicy.nask.pl/cp/dokumenty-strategiczne/dokumenty-krajowe/20,Polityka-Ochrony-Cyberprzestrzeni-RP.html, [dostęp: 14.02.2019]
[281] *Ibidem.*

wynikiem oszacowań ryzyka prowadzonych przez uprawnione podmioty, w odniesieniu do zagrożeń występujących w cyberprzestrzeni”[282].

Oprócz celu głównego w Polityce sformułowano także następujące cele szczegółowe:

a) „Zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej Państwa;
b) Zwiększenie zdolności do zapobiegania i zwalczania zagrożeniom ze strony cyberprzestrzeni;
c) Zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne;
d) Określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni;
e) Stworzenie i realizacja spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych;
f) Stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni;
g) Zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni”[283].

Cele te realizowane są poprzez:

a) „system koordynacji przeciwdziałania i reagowania na zagrożenia i ataki na cyberprzestrzeń, w tym ataki o charakterze terrorystycznym;
b) powszechne wdrożenie wśród jednostek administracji rządowej, a także podmiotów niepublicznych mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń dla bezpieczeństwa cyberprzestrzeni oraz właściwemu postępowaniu w przypadku stwierdzonych incydentów;
c) powszechną oraz specjalistyczną edukację społeczną w zakresie bezpieczeństwa CRP”[284].

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej obowiązuje organy administracji rządowej, natomiast jej adresatami są „wszyscy użytkownicy cyberprzestrzeni w obrębie Państwa i poza jego terytorium, w miejscach, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)”[285]. Jednocześnie dokument ten jest rekomendowany dla „administracji samorządowej szczebla gminnego, powiatowego i

[282] *Ibidem, s. 6*
[283] *Ibidem.*
[284] *Ibidem, s. 7.*
[285] *Ibidem.*

wojewódzkiego oraz innych urzędów (jednostki nie należące do administracji rządowej i samorządowej)”[286]. Zawężony do struktur państwowych katalog adresatów sugeruje, iż dokument nie jest adresowany do sektora prywatnego, choć w punkcie 2. wskazano, że stanowi on jedynie „podstawę wypracowania koncepcji zarządzania bezpieczeństwem infrastruktury funkcjonującej w ramach CRP oraz wypracowania wytycznych do opracowania podstawy prawnej służącej wykonywaniu zadań w tym zakresie przez administrację rządową. Zasady zapewnienia bezpieczeństwa cyberprzestrzeni wypracowane w ramach współpracy, o której mowa w pkt 4.4, w zakresie infrastruktury CRP są rekomendowane również przedsiębiorcom”[287].

W Polityce ustanowiony został trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe:

Poziom I: poziom koordynacji - minister właściwy ds. informatyzacji;

Poziom II*:* reagowania na incydenty komputerowe:

- Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL
- Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych realizujące zadania w sferze militarnej;

Poziom III: poziom realizacji - administratorzy odpowiadający za poszczególne systemy teleinformatyczne funkcjonujące w cyberprzestrzeni.

Polityka zakłada, że do zapewnienia bezpieczeństwa CRP w zakresie niezbędnym dla niezakłóconego funkcjonowania administracji rządowej rolę głównego zespołu CERT wypełnia Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Do jego zadań zalicza się przede wszystkim: „zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa”[288]. Dla sektora militarnego funkcję głównego zespołu CERT wypełnia Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych.

[287] *Ibidem, s. 9.*
[288] *Ibidem, s. 8.*

W omawianym dokumencie nie wskazano żadnych zaleceń ani koordynatorów działania, którzy byliby związani z funkcjonowaniem krajowej infrastruktury krytycznej – w całym tekście ani razu nie wymieniono tego terminu. Należy jednak uznać, że zgodnie z obowiązującą w polskim ustawodawstwie definicją infrastruktury krytycznej, „systemy […] służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[289] niewątpliwie do niej należą. Ponadto, jak już zaznaczono, Polityka to pierwszy dokument strategiczny regulujący kwestię ogólnego bezpieczeństwa cybernetycznego i to nie tylko w zakresie ochrony cyberprzestrzeni sektora publicznego, ale też bezpieczeństwa teleinformatycznego szeroko rozumianego sektora społecznego. Zawarto w nim bowiem deklarację, że Rząd RP zobowiązuje się do czynnego udziału w zapewnieniu bezpieczeństwa zasobom informacyjnym państwa, ale także jego mieszkańców.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 roku doczekała się wielu analiz i recenzji, nie zawsze akceptujących niektóre z jej zapisów. Należy jednak oddać sprawiedliwość, że większość recenzentów dostrzega i bierze pod uwagę fakt, iż jest to pierwszy z dokumentów o tym charakterze, zatem jego prekursorstwo z założenia wpływa na jego zawartość merytoryczną. Zdaniem autora niniejszej rozprawy, najistotniejsze wnioski przedstawia wspólne stanowisko: Stowarzyszenia Euro-Atlantyckiego, Fundacji Bezpieczna Cyberprzestrzeń i Fundacji Instytut Mikromakro[290], w którym zawarto między innymi następujące zastrzeżenia:

a) „autorzy [Polityki…] trzymają się wadliwej aksjologii wcześniejszych wersji strategii lub polityki, najwyraźniej […] uwarunkowanie, że bezpieczeństwo państwa zależy od wielu różnych systemów informacyjnych, a nie tylko tych, które są bezpośrednio we władaniu jednostek organizacyjnych administracji publicznej. W konsekwencji, popełniają błąd już w tytułowej kwestii określając przedmiot polityki Cyberprzestrzenią RP. [Definiują to pojęcie] poprzez wydzielenie przestrzeni przetwarzania informacji w systemach informatycznych w obrębie państwa polskiego, a przecież podstawową cechą Internetu, w tym również technik telekomunikacyjnych opartych o protokoły wykorzystywane w Internecie jest oderwanie od fizycznego terytorium. Takie podejście ogranicza pole ochrony […] ogranicza także samo pojęcie bezpieczeństwa.

[289] http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/U/D20070590Lj.pdf, [dostęp: 14.02.2019]
[290] https://docplayer.pl/2820895-Polityka-ochrony-cyberprzestrzeni-rp.html, [dostęp 21.02.2019]

b) Fundamentalnym brakiem dokumentu jest ograniczenie do organizacji działań w ramach administracji rządowej, ewentualnie zalecanie wymagań innym organom administracji publicznej. Wiedza na temat zagrożeń, środków zaradczych, nie mówiąc o technologiach sieciowych lub organizacji systemów informacyjnych jest w ogromnej części poza instytucjami administracji. […] Istotne z punktu widzenia strategicznych interesów państwa i obywateli współczesne zagrożenia z cyberprzestrzeni, dotyczą systemów zarządzanych bez udziału organów administracji, w dużej części będących własnością prywatną. [Zagrożenia te] warunkują funkcjonowanie gospodarki, systemu bankowego, transportu, energetyki. […] Pewna część tego rodzaju systemów jest kwalifikowana jako infrastruktura krytyczna w ramach zarządzania kryzysowego.
c) [W Polityce…] brak ogólnej systemowej analizy rodzaju i charakteru zagrożeń, które powinny angażować działania służb rządowych, w tym powodów, dla których takie zagrożenia mogą wystąpić. Zagrożenia powinny być analizowane pod kątem znaczenia jakie mogą mieć dla gospodarki, bezpieczeństwa obywateli i stabilności państwa.
d) Polityka nie wskazuje jednoznacznie podmiotów odpowiedzialnych za realizację zadań w niej określonych, ani czasu ich choćby przybliżonej realizacji. W Polityce określone są ewentualnie podmioty odpowiedzialne za wykonanie jakiegoś zadania, brak jednak wskazania jakiegokolwiek czasu jego realizacji. Dodatkowo zadania nakładane są w formie zaleceń […]"[291].

Do zacytowanej analizy warto dodać jeszcze spostrzeżenie, iż Polityka nie przewiduje (ani nawet nie sugeruje) możliwości udziału sektora pozarządowego w tworzeniu zaleceń czy rekomendacji w zakresie bezpieczeństwa cyberprzestrzeni. Rezygnacja z udziału tego sektora nawet w zakresie konsultacji implikuje niedostateczny udział czynnika społecznego (czyli, tym samym, czynnika profesjonalnego) w procesie legislacyjnym.

[291] *Ibidem*, s. 2-4.

4.2.4. Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022[292] – Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022[293]

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[294] miała decydujący wpływ na opracowanie i przyjęcie przez Polskę Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022[295] będącą pierwszą krajową strategią w zakresie bezpieczeństwa systemów teleinformatycznych.
Warto w tym miejscu odnotować, że przed jej przyjęciem opracowano szereg dokumentów strategicznych i programowych dotyczących cyberbezpieczeństwa. Były to odpowiednio:

- Rządowy program ochrony cyberprzestrzeni RP na lata 2008-2011 (listopad 2008);
- Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 (styczeń 2009);
- Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 (marzec 2009);
- Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2015 (maj 2010);
- Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016 (czerwiec 2010);
- Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2020 (kwiecień 2011);
- Polityka bezpieczeństwa cyberprzestrzeni RP (maj 2011).

Niemniej jednak, żaden z tych dokumentów nie został przyjęty przez rząd RP do realizacji, ich przygotowanie oceniono bowiem jako nierzetelne, a efekty prac za niezadowalające[296]. Należy jednocześnie zauważyć, iż poza Dyrektywą z 6 lipca 2016 roku znaczącym przyczynkiem do wypracowania Strategii był raport pokontrolny Najwyższej Izby Kontroli z 30 czerwca 2016 roku[297]. Ustalenia powzięte w toku kontroli stały się bezpośrednią podstawą do opracowania omawianego w tym podrozdziale dokumentu. „W ocenie NIK, istotnym czynnikiem wpływającym negatywnie na realizację zadań w obszarze bezpieczeństwa w cyberprzestrzeni było niewystarczające zaangażowanie kierownictwa administracji rządowej, w tym Prezesa Rady Ministrów, w celu rozstrzygania kwestii spornych między poszczególnymi urzędami oraz

[292] *https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109,* [dostęp: 21.02.2019]
[293] http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersjapl.pdf [dostęp: 22.02.2019]
[294] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=BG [dostęp: 22.02.2019]
[295] https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022 [dostęp: 22.02.2019]
[296] Więcej informacji na temat wspomnianych dokumentów pod adresem: *https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/#_edn8* [dostęp: 22.02.2019]
[297] *https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/pobierz,kpb~p_14_043_201406171048381403002118~01,typ,kk.pd*f [dostęp: 22.02.2019]

zapewnienia współdziałania organów i instytucji związanych z bezpieczeństwem teleinformatycznym państwa. Ponadto stwierdzono, iż znaczącym osłabieniem poziomu cyberbezpieczeństwa jest fakt, iż że poszczególne kontrolowane podmioty posiadały własne, odrębne procedury zapobiegania zagrożeniom w cyberprzestrzeni. Ale suma tych systemów nie tworzyła spójnej całości – jednego spójnego systemu"[298].

Kontrola wykazała także szereg krytycznych uchybień na poziomie przyporządkowania zadań i obowiązków zarówno na poziomie ich przydziału, jak i na poziomie realizacji. I tak, odpowiednio:

- „Minister Administracji i Cyfryzacji, któremu bezpośrednio przypisano obowiązki związane z ochroną cyberprzestrzeni, nie realizował należących do niego zadań w zakresie inicjowania i koordynowania działań innych podmiotów w dziedzinie bezpieczeństwa teleinformatycznego państwa. [Ponadto] nie dysponował zasobami pozwalającymi na realną realizację zadań dotyczących zarządzania krajowym system ochrony cyberprzestrzeni oraz nie miał uprawnień do oddziaływania na inne instytucje [Choć minister ten] odpowiada za koordynację krajowego systemu reagowania na incydenty komputerowe, nie realizował żadnych zadań w tym zakresie"[299].
- „Minister Spraw Wewnętrznych nie realizował żadnych zadań związanych z budową krajowego systemu ochrony cyberprzestrzeni. Działania Ministra w obszarze bezpieczeństwa IT ograniczały się do własnych sieci oraz systemów resortowych […][300].
- „Rządowe Centrum Bezpieczeństwa – w niewystarczającym stopniu uwzględnia nowe zagrożenia dla infrastruktury krytycznej państwa, jakimi są zagrożenia występujące w cyberprzestrzeni, [a koordynowany przez nie] system zarządzania kryzysowego nie jest komplementarny i spójny z działaniami w zakresie bezpieczeństwa teleinformatycznego"[301].
- „Nie prowadzono żadnych prac legislacyjnych, które miałyby na celu unormowanie zagadnień związanych z bezpieczeństwem teleinformatycznym państwa. Nie przeprowadzono inwentaryzacji rozproszonych w różnych aktach prawnych przepisów związanych z cyberbezpieczeństwem ani nie zdefiniowano pożądanych kierunków zmian

[298] *Ibidem*.
[299] *Ibidem*.
[300] *Ibidem*.
[301] *Ibidem*.

legislacyjnych. Nie przygotowano nawet założeń aktu normatywnego, określającego strukturę krajowego systemu ochrony cyberprzestrzeni i jego uczestników[302].

- „Administracja publiczna nie wypracowała dotąd zintegrowanego i systemowego wspierania przez państwo badań w obszarze ochrony cyberprzestrzeni oraz możliwości praktycznego zastosowania ich wyników w celu poprawy bezpieczeństwa teleinformatycznego"[303].
- „Tworzone w Polsce plany kryzysowe, w tym w szczególności Krajowy Plan Zarządzania Kryzysowego, odnosiły się wyłącznie do zdarzeń konwencjonalnych, takich jak np. katastrofy naturalne i nie uwzględniały zmiany charakteru zagrożeń, wynikającej m.in. z postępu technologicznego […][304].
- „Komendant Główny Policji nie przedsięwziął (…) rzetelnych działań w celu wdrożenia w Policji realnego i kompleksowego systemu reagowania na zagrożenia i incydenty w cyberprzestrzeni"[305].

Raport NIK zwrócił także uwagę na bardzo istotny aspekt związany ze zdolnością państwa do ochrony cyberprzestrzeni, a mianowicie, iż nie zostały opracowane założenia systemu finansowania działań związanych z tym zadaniem. Nie przydzielono żadnych dodatkowych środków na ich realizację, co w ocenie NIK praktycznie sparaliżowało działania podmiotów państwowych w zakresie bezpieczeństwa teleinformatycznego. Bardzo negatywnie oceniono też przyjętą w czerwcu 2013 roku Politykę ochrony cyberprzestrzeni Rzeczypospolitej Polskiej (omawianą szczegółowo w pkt. 3.2.3.4.3 tego dokumentu) jako: „dokument będący wynikiem źle rozumianego kompromisu, nieprecyzyjny i obarczony licznymi błędami merytorycznymi". Pomimo jego przyjęcia, „w Polsce wciąż nie funkcjonuje spójny krajowy system reagowania na incydenty komputerowe. Czynności z zakresu reagowania na incydenty są realizowane przez funkcjonujące niezależnie od siebie państwowe i prywatne zespoły CERT, zajmujące się swoimi własnymi obszarami oddziaływania. Kierownictwo administracji państwowej nie podejmowało działań w celu wypracowania założeń pożądanej struktury zespołów reagowania, ustanowienia kanałów wymiany informacji oraz powołania CERTu narodowego, koordynującego działania wielu podmiotów i odpowiadającego za współpracę międzynarodową".[306] Odnotować jednakże należy, że działania Naukowej i Akademickiej Sieci Komputerowej (NASK) zostały przez NIK

[302] *Ibidem.*
[303] *Ibidem.*
[304] *Ibidem.*
[305] *Ibidem.*
[306] *Ibidem.*

ocenione pozytywnie w szczególności w zakresie powołania i utrzymania CERT Polska. „Niemniej jednak wniosek ostateczny jest bardzo negatywny – Administracja państwowa nie dysponuje wiedzą na temat skali i rodzaju incydentów występujących w cyberprzestrzeni, a ustanowiony w Prawie telekomunikacyjnym system zbierania i rejestrowania takich informacji okazał się być całkowicie nieskuteczny”[307].

Nie sposób tym samym jednoznacznie ocenić, że przyjęty w roku 2017 przez rząd Rzeczypospolitej Polskiej dokument jest *de facto* kontynuacją uprzednich działań w zakresie zapewnienia cyberbezpieczeństwa, a w szczególności przyjętej w roku 2013 Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Raport NIK pozwala sądzić, że w dokumencie tym należało poczynić znaczące zmiany w stosunku do bezpośrednio go poprzedzających opracowań. W intencji autorów taki postęp z pewnością został uczyniony – dokument ten ma charakter znacznie bardziej interdyscyplinarny, został bowiem przygotowany przez szereg ministerstw: Cyfryzacji, Obrony Narodowej, Spraw Wewnętrznych i Administracji oraz przez pracowników Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa i Biura Bezpieczeństwa Narodowego, dodatkowo pierwszy raz w pracach nad dokumentem uczestniczyli także przedstawiciele NASK.

W rozdziale 2. (Kontekst strategiczny) określono Krajowe Ramy jako dokument, „który wpisuje się w kontynuację działań, podejmowanych w przeszłości przez administrację rządową, mających na celu podniesienie poziomu bezpieczeństwa w cyberprzestrzeni RP, w tym przyjętą przez rząd w 2013 roku Politykę Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. [Jego celem] jest określenie ramowych działań, mających na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni. Proponowane kierunki strategiczne mają również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni. Krajowe Ramy Polityki Cyberbezpieczeństwa są spójne z prowadzonymi działaniami dotyczącymi operatorów infrastruktury krytycznej wykorzystujących systemy teleinformatyczne oraz uwzględnia potrzeby zaangażowania Sił Zbrojnych Rzeczypospolitej

[307] *Ibidem.*

Polskiej”[308]. W punkcie tym zawarto również deklarację, iż „[…] rząd będzie w pełni respektować prawo do prywatności oraz stać na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa”[309].

Przedstawiona w rozdziale 4.1. wizja programowa dokumentu zakłada, iż w roku 2022 „Polska będzie krajem bardziej odpornym na ataki i zagrożenia płynące z cyberprzestrzeni”, zaś jej cyberprzestrzeń (warto zauważyć, że także i tutaj ograniczona do cyberprzestrzeni RP) stanowić będzie „bezpieczne środowisko umożliwiające realizowanie wszystkich funkcji państwa i pozwalać na pełne wykorzystywanie potencjału gospodarki cyfrowej, przy równoczesnym poszanowaniu praw i wolności obywateli.[310] Jako cel główny (rozdział 4.2) dokument stawia sobie zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych”[311], a jego realizacja będzie osiągana za pomocą zadań sformułowanych w czterech celach szczegółowych (rozdział 4.2). Są nimi:

1. „Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa,
2. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom,
3. Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni,
4. Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa”[312].

Pierwszy ze wskazanych celów szczegółowych zostanie omówiony nieco szerzej, gdyż w kontekście ochrony infrastruktury krytycznej wydaje się bowiem szczególnie istotny, bo związany przede wszystkim z dostosowaniem obowiązującego prawa do zadań, które stoją przed państwem w zakresie zapewnienia cyberbezpieczeństwa. Ramy zapowiadają przegląd przepisów w tym zakresie, w celu „ich harmonizacji, zwiększenia efektywności działania i poprawy przepływu informacji pomiędzy wszystkimi interesariuszami zaangażowanymi w aktywne budowanie krajowego systemu cyberbezpieczeństwa”[313]. Jako priorytetowe autorzy oceniają zmiany związane z dostosowanie się do regulacji UE, w tym przede wszystkim do Dyrektywy

[308] *Ibidem*, s. 5.
[309] *Ibidem*.
[310] *Ibidem*, s. 6-7.
[311] *Ibidem*, s. 7.
[312] *Ibidem*.
[313] *Ibidem*, s. 8.

Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych (opisanej w rozdziale 3.1.2. niniejszej pracy). „Uregulowane zostaną [także] kwestie współpracy operacyjnej, w tym właściwej koordynacji działań i wymiany informacji pomiędzy instytucjami odpowiedzialnymi za bezpieczeństwo narodowe, działania antyterrorystyczne oraz bezpieczeństwo wewnętrzne i porządek publiczny”[314]. Autorzy dokumentu zauważają też, że „[…] dotychczasowe działania w obszarze cyberbezpieczeństwa podmiotów ze sfery cywilnej, wojskowej, sektora publicznego i prywatnego oraz instytucji odpowiedzialnych za zwalczanie cyberprzestępczości miały charakter rozproszony, co bezpośrednio wpływało na niską efektywność tego systemu. Wdrożenie skutecznego systemu cyberbezpieczeństwa będzie możliwe poprzez skonsolidowanie i zharmonizowanie działań wszystkich interesariuszy”[315]. Poważne podejście do tej deklaracji widoczne jest zarówno na poziomie opracowania samego dokumentu (jak wspomniano, jest on stworzony przez znacznie szerszy niż dotąd zespół autorów), jak i wskazania, iż „warunkiem prawidłowego działania systemu będzie również doprecyzowanie wzajemnych powiązań pomiędzy poszczególnymi interesariuszami krajowego systemu cyberbezpieczeństwa, w tym organów odpowiedzialnych za bezpieczeństwo narodowe, działania antyterrorystyczne, bezpieczeństwo wewnętrzne oraz porządek publiczny, prokuraturę oraz sądownictwo”[316].

W ramach celu pierwszego postuluje się także zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej. W pierwszej kolejności ma zostać zapewniona spójność działań w zakresie opracowywania kryteriów identyfikacji operatorów infrastruktury krytycznej i usług kluczowych uwzględniająca potrzebę włączenia tych podmiotów do systemu zarządzania kryzysowego. Proces ten w intencji autorów ma przebiegać we współpracy ze wszystkimi sektorami, w tym z sektorem prywatnym czy społecznym. Ponadto „ważnym elementem struktury krajowego systemu cyberbezpieczeństwa na poziomie technicznym staną się bezpieczne sieci typu intranet, oferujące połączenia wewnątrz sieci, usługi bezpieczeństwa oraz bezpieczny dostęp do sieci Internet, zwane klastrami bezpieczeństwa”[317].

[314] *Ibidem*.
[315] *Ibidem*.
[316] *Ibidem*.
[317] *Ibidem*, s. 12.

W ramach celu drugiego – tj. wzmocnienia zdolności do przeciwdziałania cyberzagrożeniom – Ramy przewidują między innymi „zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich ich fazach”[318], a także transgraniczną współpracę organów ścigania oraz podmiotów typu CERT/CSIRT (choć warto zauważyć, iż współpraca taka istniała już wcześniej, zatem należałoby mówić raczej o jej umocnieniu czy rozwoju).

W kwestii zadań wymienionych w zakresie celu trzeciego – Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni – warto wymienić punkt 7.2, w którym autorzy deklarują, iż rząd RP „[(...] będzie dążył do zbudowania efektywnego systemu partnerstwa publiczno-prywatnego opartego na zaufaniu i wspólnej odpowiedzialności za bezpieczeństwo w cyberprzestrzeni”[319] oraz „aktywnie angażować się w istniejące i powstające formy europejskiej współpracy publiczno-prywatnej […][320].

Ostatni cel szczegółowy – czwarty – nawiązuje do konieczności aktywnej współpracy międzynarodowej na poziomie strategicznym, operacyjnym i politycznym, głównie w ramach NATO i ONZ, ale także Grupy Wyszehradzkiej. Ma być ona realizowana między innymi także za pomocą Sieci CSIRT[321] – w ramach UE oraz FIRST – w zakresie globalnym.

Reasumując, zdaniem autora należy dostrzec znaczącą zmianę podejścia do problematyki ochrony cyberprzestrzeni i jest to niewątpliwie zmiana na lepsze. Niemniej jednak dokument powiela wady poprzednich strategii, a są nimi niewątpliwie zarówno znaczny stopień jego ogólności, jak i szeroka deklaratywność, przy jednoczesnej świadomości autorów, iż aktualne przepisy nie pozwalają na właściwą realizację większości z tych deklaracji. Niemniej jednak obie wskazane „wady” można jednocześnie odbierać jako schematyzację, właściwą niejako dla dokumentów programowych i strategicznych o tym charakterze, zaś ocenie poddać realizację Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa, przyjętego w październiku 2017 roku. Ta z kolei jest jeszcze odległą perspektywą.

[318] *Ibidem*, s. 13
[319] *Ibidem*, s. 18.
[320] *Ibidem*.
[321] Autorzy poprzez „Sieć CSIRT” określają strukturę organizacyjną, o której mowa w art. 12 Dyrektywy NIS *https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148* [dostęp: 22.02.3019]

Rozdział V

Strategiczne założenia ochrony infrastruktury krytycznej Rzeczypospolitej Polskiej

5.1. Definicja infrastruktury krytycznej w Polsce i Unii Europejskiej

W Rzeczypospolitej Polskiej infrastruktura krytyczna wchodzi w skład jedenastu systemów, które mają kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli oraz służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Większość przyjętych definicji wywodzi się z treści obowiązujących aktów prawnych, które w precyzyjny sposób określają środki o ogromnym znaczeniu dla sprawnego funkcjonowania społeczeństwa, ale także i gospodarki.

W polskim systemie prawnym zagadnienie infrastruktury krytycznej przedstawia *Ustawa z dnia 27 kwietnia 2007 roku o zarządzaniu kryzysowym*, która szczegółowo zostanie omówiona w kolejnym podrozdziale. W artykule 3 ust. 2 doprecyzowano, że jako infrastrukturę krytyczną należy rozumieć „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców”[322]. Zgodnie z treścią tego artykułu można przyjąć, że trwale i niezmiennie do elementów tworzących infrastrukturę krytyczną zalicza się systemy:

- zaopatrzenia w energię, surowce energetyczne i paliwa;
- łączności;
- sieci teleinformatycznych;
- finansowe;
- zaopatrzenia w żywność;
- zaopatrzenia w wodę;
- ochrony zdrowia;
- transportowe;
- ratownicze;
- zapewniające ciągłość działania administracji publicznej;

[322] Art. 3, ust. 2, Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 nr 89 poz. 590.

- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[323].

Powyższe zestawienie systemów wchodzących w skład infrastruktury krytycznej wykazuje, że tworzą ją obiekty o użyteczności publicznej, które odgrywają strategiczną rolę dla bezpieczeństwa państwa oraz jego obywateli. Stąd też wszystkie działania skierowane przeciwko niej są uznawane za przestępstwa, w efekcie czego ścigane i podlegające penalizacji[324]. W treści artykułu 3 ust. 2a wspomniano również o europejskiej infrastrukturze krytycznej. Jest ona rozumiana jako infrastruktura krytyczna, która znajduje się na terenie jakiegokolwiek państwa członkowskiego Unii Europejskiej, a jej zniszczenie bądź też uszkodzenie będzie miało konsekwencje dla co najmniej dwóch z nich. Mowa tutaj o systemach: „energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego, śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów"[325]. Jej definicja została zawarta w Dyrektywie Rady Europejskiej 2008/114/WE. Zgodnie z treścią artykułu 2 tego dokumentu infrastruktura krytyczna „oznacza składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji"[326]. Przedstawiona egzemplifikacja powstała na gruncie coraz intensywniejszych rozmów o sposobach zabezpieczania infrastruktury krytycznej i potencjalnych działaniach prewencyjnych oraz ochronnych, które rozpoczęły się w 2004 roku. Był to moment, kiedy Rada Europejska podjęła decyzję o konieczności stworzenia europejskiego programu ochrony infrastruktury krytycznej. Prace nad programem zostały w konsekwencji zlecone Komisji Europejskiej. Ich efektem było stworzenie komunikatu pt. *Ochrona infrastruktury krytycznej w walce z terroryzmem*. Jego treść zawierała podsumowanie dotychczasowych działań oraz osiągnięć Unii Europejskiej w tym zakresie, a także przedstawiała propozycję stworzenia nowych instrumentów, które miały pomóc chronić infrastrukturę krytyczną[327]. Komisja Europejska postulowała utworzenie:

[323] *Ibidem*.
[324] Żuber M., *Infrastruktura krytyczna państwa jako obszaru potencjalnego oddziaływania terrorystycznego*, „Rocznik Bezpieczeństwa Międzynarodowego", nr 2, 2014, s. 179.
[325] Art. 3, ust. 2a, Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 nr 89 poz. 590.
[326] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony.
[327] Szewczyk T., *Europejski program ochrony infrastruktury krytycznej*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 6(4), 2012, s. 157.

- EPOIK – europejskiego programu ochrony infrastruktury krytycznej;
- SOZIK – sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej[328].

Propozycje przedstawione przez Komisję Europejską uzyskały aprobatę Rady Europejskiej i stały się przedmiotem dalszych obrad oraz negocjacji. Państwa członkowskie Unii Europejskiej zgodnie przyznały, że muszą połączyć siły i stworzyć system wymiany doświadczeń, wiedzy czy dobrych praktyk, który pomoże chronić ich społeczeństwa oraz gospodarki przed atakami na infrastrukturę krytyczną. Pod koniec 2005 roku Komisja Europejska udostępniła tak zwaną Zieloną Księgę, której treść skupiała się na europejskim programie ochrony infrastruktury krytycznej. Dokument ten trafił zarówno do członków Unii, jak i do podmiotów z sektora prywatnego. W ten sposób Komisja Europejska chciała pozyskać jak największą ilość opinii na temat samej infrastruktury krytycznej, jej definicji czy sposobów ochrony, które zostaną zamieszczone w EPOIK[329]. Zebrane informacje zostały podsumowane i zaprezentowane w Komunikacie Komisji w sprawie europejskiego programu ochrony infrastruktury krytycznej z 2006 roku, stanowiły również ważny element w trakcie opracowywania Dyrektywy Rady Europejskiej 2008/114/WE, która była pierwszym dokumentem wyjaśniającym definicję infrastruktury krytycznej[330].

5.2. Podstawy prawne ochrony infrastruktury krytycznej w Polsce

5.2.1. *Ustawa z dnia 26.04.2007 roku o zarządzaniu kryzysowym*[331]

Podstawowym aktem prawnymi regulującym procedury identyfikacji i ochrony infrastruktury krytycznej jest *Ustawa z dnia 26.04.2007 roku o zarządzaniu kryzysowym* ze zmianami wprowadzonymi *ustawą z dnia 17.07.2009 roku o zmianie ustawy o zarządzaniu kryzysowym*[332], która weszła w życie 19.09.2009 roku.

Nie należy jednakże zakładać, że do czasu uchwalenia powyższej ustawy w polskiej legislacji nie były obecne zapisy dotyczące ochrony systemów wchodzących w skład infrastruktury krytycznej. Zapisy takie istniały[333], niemniej jednak znajdowały się w wielu

[328] Ibidem, s. 157.
[329] *Zielona księga w sprawie europejskiego programu ochrony infrastruktury krytycznej*, Komisja Wspólnot Europejskich, Bruksela, dnia 17.11.2005 r., KOM (2005) 576 wersja ostateczna.
[330] Szewczyk T., op. cit., s. 158.
[331] *Ustawa z 26.04.2007 r. o zarządzaniu kryzysowym (Dz.U.07.89.590 z pó źn. zm.), http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=* WDU20070890590 – [dostęp: 25.02.2019]
[332] *Ustawa z 17.07.2009 r. o zmianie ustawy o zarządzaniu kryzysowym* (Dz.U.09.131.1076) http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id= WDU20091311076 [dostęp: 25.02.2019]
[333] Poniżej podano jedynie dokumenty o randze ustawy, dokumenty niższego zaszeregowania zostały pominięte, wobec czego zestawienie poniższe zawiera: *ustawy z 21.11.1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (Dz. U. z 2004 r. Nr 241, poz. 2416, z

różnych aktach prawnych, o zróżnicowanej randze (poza ustawami były to m.in. rozporządzenia będące dokumentem *stricte* rządowym czy ministerialnym) oraz w sporym rozproszeniu instytucjonalnym organów ustanawiających. Dopiero jednak omawiana ustawa wniosła spójne – co nie oznacza wcale, że kompletne – regulacje dotyczące umocowania prawnego działań w zakresie ochrony infrastruktury krytycznej. Definicja infrastruktury krytycznej, obowiązująca w Polsce, została szczegółowo omówiona w rozdziale 2.1., dlatego też obecnie jedynie przypomniane zostanie, iż w artykule 3 ust. 2 *Ustawy z dnia 26.04.2007 roku o zarządzaniu kryzysowym* doprecyzowano, że jako infrastrukturę krytyczną należy rozumieć „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców”[334]. Można zatem przyjąć, że trwale i niezmiennie do elementów tworzących infrastrukturę krytyczną RP zalicza się systemy:

- *zaopatrzenia w energię, surowce energetyczne i paliwa,*
- *łączności,*
- *sieci teleinformatycznych,*
- *finansowe,*
- *zaopatrzenia w żywność,*
- *zaopatrzenia w wodę,*
- *ochrony zdrowia,*
- *transportowe,*
- *ratownicze,*
- *zapewniające ciągłość działania administracji publicznej,*

późn. zm.), *ustawy z 8.03.1990 r. o samorządzie gminnym* (Dz. U. z 2001 r. Nr 142, poz. 1591, z późn. zm.), *ustawy z 6.04.1990 r. o Policji* (Dz. U. z 2002 r. Nr 7, poz. 58, z pó źn. zm. *ustawy z 12.10.1990 r. o ochronie granicy państwowej* (Dz. U. z 2005 r. Nr 226, poz. 1944), *ustawy z 24.08.1991 r. o ochronie przeciwpożarowej* (Dz. U. z 2002 r. Nr 147, poz. 1229, z późn. zm.), *ustawy z 24.08.1991 r. o Państwowej Straży Pożarnej* (Dz. U. z 2002 r. Nr 147, poz. 1230, z późn. zm.), *ustawy z 4.02.1994 r. - Prawo geologiczne i górnicze* (Dz. U. z 2005 r. Nr 228, poz. 1947, z pó źn. zm.), *ustawy z 7.07.1994 r. - Prawo budowlane* (Dz. U. z 2003 r. Nr 207, poz. 2016, z późn. zm.), *ustawy z 30.05.1996 r. o rezerwach państwowych oraz zapasach obowiązkowych paliw* (Dz. U. z 2003 r. Nr 24, poz. 197, z późn. zm.), *ustawy z 10.04.1997 r. - Prawo energetyczne* (Dz. U. z 2003 r. Nr 153, poz. 1504, z późn. zm. *ustawy z 5.06.1998 r. o administracji rządowej w województwie* (Dz. U. z 2001 r. Nr 80, poz. 872, z późn. zm.), *ustawy z 5.06.1998 r. o samorządzie województwa* (Dz. U. z 2001 r. Nr 142, poz. 159 0, z pó źn. zm.), *ustawy z 5.06.1998 r. o samorządzie powiatowym* (Dz. U. z 2001 r. Nr 142, poz. 1592, z późn. zm.), *ustawy z 9.11.2000 r. o bezpieczeństwie morskim* (Dz. U. Nr 109, poz. 1156, z późn. zm.), *ustawy z 29.11.2000 r. - Prawo atomowe* (Dz. U. z 2004 r. Nr 161, poz. 1689, z pó źn. zm.), ustawy z 21.12.2000 r. o żegludze śródlądowej (Dz. U. z 2001 r. Nr 5, poz. 43, z późn. zm.),

[334] *Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym,* Dz.U. 2007 nr 89 poz. 590), http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id= WDU20070890590 – [dostęp: 25.02.2019]

- *produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych*[335].

W celu realizacji założeń ustawy podmioty, w których posiadaniu znajduje się zasób infrastruktury krytycznej, powinny podejmować aktywne działania w celu utrzymania jej w należytym stanie, ochrony przed zniszczeniami i dostępem osób, które mogłyby zagrozić bezpieczeństwu państwa. Podmioty te powinny czynić także inwestycje w celu stałego podnoszenia poziomu infrastruktury krytycznej i jej stanu[336]. Działania właścicieli infrastruktury krytycznej powinny być centralnie koordynowane, jednak nie tylko w obliczu zagrożenia, ale także w czasie wykonywania obowiązków związanych z utrzymaniem infrastruktury krytycznej w stanie zapewniającym realizację zadań państwa w sytuacjach kryzysowych[337]. Realizacja założeń ustawy powinna wprowadzić mechanizmy pozwalające na:

- „monitorowanie i uaktualnianie listy elementów infrastruktury krytycznej;
- ustalenie wzajemnych relacji pomiędzy elementami infrastruktury krytycznej;
- ustalenie wzajemnych relacji pomiędzy dysponentami infrastruktury krytycznej;
- tworzenie inicjatyw w zakresie ochrony infrastruktury krytycznej
- przeprowadzenie akcji edukacyjnych – uświadamiających rolę infrastruktury krytycznej w bezpieczeństwie państwa,
- wspieranie podmiotów, w posiadaniu których znajduje się infrastruktury krytycznej, w ponoszeniu kosztów jej budowy, utrzymania i ochrony”[338].

Autorzy cytowanego już *Raportu Instytutu Kościuszki* oceniają intencję ustawodawcy w zakresie wytworzenia procedur ochrony infrastruktury krytycznej jako uznanie ich za jeden z priorytetów stojących przed państwem. Tym samym „brak powyższych mechanizmów może doprowadzić do niewiedzy o wadze infrastruktury krytycznej w bezpieczeństwie państwa, chaosie w działaniach koordynacyjnych, niechęci podmiotów prywatnych do ponoszenia kosztów związanych w IK. Dopiero prawidłowe wypracowanie systemu wsparcia dla podmiotów uczestniczących w utrzymaniu IK daje podstawy do stworzenia systemu skutecznych sankcji. Elementami wsparcia dla podmiotów powinny być między innymi:

- formalna platforma do wymiany doświadczeń i wiedzy na temat ochrony IK;

[335] *Ibidem.*
[336] *Ibidem.*
[337] *Ibidem.*
[338] *Ibidem.*

- partnerstwo publiczno-prywatne;
- fundusze celowe;
- ułatwienia w stosowaniu aktów prawnych np. w stosowaniu ustawy o zamówieniach publicznych;
- wspieranie samoregulacji przedsiębiorstw dysponujących IK w zakresie przepływu informacji oraz ponoszenia nakładów na jej ochronę i utrzymanie[339].

O zgodności Ustawy z 26.04.2007 r. o zarządzaniu kryzysowym z Konstytucją RP wypowiedział się Trybunał Konstytucyjny. W wyroku z dnia 21.04.2009 r. orzekł, że art. 3 pkt 2 *Ustawy z dnia 26.04.2007 r. o zarządzaniu kryzysowym*, zawierający definicję infrastruktury krytycznej, jest zgodny z art. 2 Konstytucji oraz nie jest niezgodny z art. 22 w związku z art. 31 ust. 3 Konstytucji[340]. Trybunał Konstytucyjny zaznaczył co prawda w uzasadnieniu, że definicja „infrastruktury krytycznej" oparta jest na pojęciach nie do końca precyzyjnych, ale zawiera terminy dość powszechnie stosowane, które nie wymagają bardziej szczegółowego wyjaśnienia w przepisie sformułowanym wyłącznie na użytek tej ustawy. Możliwość uzupełniającego wyjaśnienia tego pojęcia wynika bowiem z treści normatywnej całego aktu. Jak przypomina Monika Floriańczyk-Kardaś, „Trybunał Konstytucyjny zwrócił uwagę, że w pojęciu infrastruktura krytyczna mieszczą się dwa podstawowe elementy. Po pierwsze – w pojęciu tym mieszczą się enumeratywnie wymienione ,,systemy": a) zaopatrzenia w energię i paliwa, b) łączności i sieci teleinformatycznych, c) finansowe, d) zaopatrzenia w żywność i wodę, e) ochrony zdrowia, f) transportowe i komunikacyjne, g) ratownicze, h) zapewniające ciągłość działania administracji publicznej, i) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. Po drugie – <<infrastruktura krytyczna>> to także wchodzące w skład tych systemów powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców"[341]. W tym samym wyroku Trybunał wypowiedział się także o wpływie zawartej w ustawie definicji na

[339] Pyznar M., Abgarowicz G. i inni*, op. cit.*, s. 26
[340] *Wyrok Trybunału Konstytucyjnego z 21.04. 2009 r.,* sygn. akt K 50/07, http://prawo.sejm.gov.pl/isap.nsf/ DocDetails.xsp?id= WDU 20090650553 – [dostęp: 25.02.2019]
[341] Florianczyk-Kardaś M., K*ilka uwag o ochronie infrastruktury krytycznej w świetle przepisów ustawy o zarządzaniu kryzysowym i ustawy o „złotej akcji" Skarbu Państwa,* „Kwartalnik Prawa Publicznego" 1/2015, s. 6.

stosowanie przepisów zawartych w innych ustawach i rozporządzeniach w zakresie potencjalnego ograniczania możliwości ich realizacji oraz ewentualnego wpływu na swobodę prowadzenia działalności gospodarczej. Trybunał uznał, że definicja infrastruktury krytycznej nie ogranicza w sposób samoistny wolności prowadzenia działalności gospodarczej. Trybunał zaznaczył, że w ustawie o zarządzaniu kryzysowym nie wprowadzono przepisów, które zawierałyby jakiekolwiek sankcje wobec tych zarządców infrastruktury krytycznej, którzy nie zastosują się do dyspozycji zawartych w przepisach ustawy i odmówią współpracy z administracją publiczną. W rezultacie, Trybunał orzekł, że art. 3 pkt 2 ustawy o zarządzaniu kryzysowym zawierający definicję infrastruktury krytycznej nie dotyczy bezpośrednio działalności gospodarczej i nie może być oceniany w kontekście art. 22 w związku z art. 31 ust. 3 Konstytucji.

Należy odnotować, iż ta sama ustawa w art. 3 ust. 3 zawiera także definicję ochrony infrastruktury krytycznej, przez którą należy rozumieć „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie”[342]. Definicję tę – a tym samym wiążące się z nią kontrowersje – autor zamierza omówić szczegółowo w rozdziale VII.

Warto uzupełnić, iż w roku 2010 ukazały się trzy rozporządzenia Rady Ministrów wydane na podstawie zapisów omawianej ustawy (art. 5a ust. 6, art. 5b ust. 9 i art. 6 ust. 7)[9:]

a) w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego[343],
b) w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej[344]
c) w sprawie planów ochrony infrastruktury krytycznej[345].

Ad a) Rozporządzenie w sprawie *Raportu o zagrożeniach bezpieczeństwa narodowego* określa „sposób, tryb i terminy opracowania Raportu, który mają sporządzać ministrowie kierujących działami administracji rządowej, kierownicy urzędów centralnych oraz

[342] *Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz.U. 2007 nr 89 poz. 590, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id= WDU20070890590 – [dostęp: 25.02.1019]
[342] *Ibidem.*
[343] *Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego* (DzU nr 83 z 17 maja 2010 r., poz. 540). http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20100830540 – [dostęp: 25.02.1019]
[344] *Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej* (DzU nr 83 z 17 maja 2010 r., poz. 541). http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20100830541– [dostęp: 25.02.1019]
[345] *Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w spraw ie planów ochrony infrastruktury krytycznej (DzU nr 83 z 17 maja 2010 r., poz. 542).* http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20100830542/O/D20100542.pdf- dostęp: 25.02.1019]

wojewodowie na podstawie raportów cząstkowych, które będą obejmowały, między innymi: najważniejsze zagrożenia i skutki ich wystąpienia; cele strategiczne, jakie należy osiągnąć, aby zminimalizować możliwość wystąpienia zagrożeń lub ich skutków; wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych; programowanie zadań w zakresie poprawy bezpieczeństwa państwa; określenie priorytetów w reagowaniu na określone zagrożenia"[346].

Ad b) Rozporządzenie w sprawie *Narodowego Programu Ochrony Infrastruktury Krytycznej* określa „sposób realizacji obowiązków i współpracy w zakresie NPOIK przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń i usług infrastruktury krytycznej, w tym kluczowe dla programu kryteria pozwalające wyodrębnić infrastrukturę krytyczną, natomiast rozporządzenie w sprawie planów ochrony infrastruktury krytycznej określa sposób tworzenia, aktualizacji oraz strukturę planów ochrony infrastruktury krytycznej opracowywanych przez właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, a także warunki i tryb uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej"[347].

Ad c) *Rozporządzenie w sprawie planów ochrony infrastruktury krytyczne* określa natomiast „sposób tworzenia, aktualizacji oraz strukturę planów ochrony infrastruktury krytycznej opracowywanych przez właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej [a także] warunki i tryb uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej".

[346] Radziejewski R*., O infrastrukturze krytycznej krytycznie*, Warszawa 2013, s. 24
[347] *Ibidem,* s.25.

5.2.2. *Ustawa z dnia 18.03.2010 roku o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych* [348]

Kolejnym aktem prawnym o mocy ustawy zawierającym definicję infrastruktury krytycznej jest *Ustawa z dnia 18.03.2010 roku o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych.* Zapisana w niej definicja infrastruktury krytycznej jest zawężona do systemów: energetycznego oraz paliwowego, co implikowane jest oczywiście samym charakterem dokumentu – ramy ustawy obejmują bowiem tylko podmioty odpowiedzialne za ten zakres. W myśl art. 1 ust. 2 pkt. 2 ustawy w skład infrastruktury krytycznej wchodzi w sektorze energetycznym „infrastruktura służąca do wytwarzania albo przesyłania energii elektrycznej"[349] zaś zasoby kwalifikowane jako element infrastruktury krytycznej w sektorze ropy naftowej obejmują: „infrastrukturę służącą do wydobycia, rafinacji, przetwarzania ropy naftowej, a także jej magazynowanie, przesyłanie rurociągami i przeładunek w terminalach portowych"[350]. Z kolei art. 1 ust. 2 pkt 3 wskazuje, że w sektorze paliw gazowych infrastrukturę krytyczną stanowi „infrastruktura służąca do produkcji, rafinacji, przetwarzania, magazynowania, przesyłania paliw gazowych gazociągami oraz o terminale skroplonego gazu ziemnego"[351].

Choć, jak wspomniano, definicje zawarte w obu ustawach mają nieco innych charakter, to jednak są one ściśle ze sobą powiązane, gdyż wyspecyfikowanie infrastruktury krytycznej podlegającej ochronie na podstawie ustawy o szczególnych uprawnieniach jest (niestety) następcze wobec zasad przewidzianych w ustawie o zarządzaniu kryzysowym – jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej określony jest w art. 5b ust. 7 pkt 1 tejże ustawy. Zatem należy uznać, że jedynie odwołanie do przedmiotowego jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład

[348] *Ustawa z 18.03.2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych* (Dz.U.10.65.404 http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20100650404 [dostęp: 25.02.2019]
[349] *Ustawa z 18.03.2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych* (Dz.U.10.65.404 http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20100650404 [dostęp: 25.02.2019]
[350] *Ibidem.*
[351] *Ibidem.*

infrastruktury krytycznej pozwala na zastosowania ustawy o szczególnych uprawnieniach – co nie oznacza jednak, że zastosowanie to okaże się skuteczne w praktyce sytuacji kryzysowej.

5.2.3. *Narodowy Program Ochrony Infrastruktury Krytycznej*[352] *z 2013 roku*

Pierwszy[353] *Narodowy Program Ochrony Infrastruktury Krytycznej* (NPOIK) przygotowany przez Rządowe Centrum Bezpieczeństwa (RCB)[354], przyjęty uchwałą Rady Ministrów 26 marca 2013 roku, wynika bezpośrednio z zapisów ustawy o zarządzaniu kryzysowym i zawartej w niej definicji infrastruktury krytycznej. Pozwala ona ocenić, które obiekty, urządzenia, instalacje i usługi są kluczowe dla bezpieczeństwa państwa i jego obywateli, a także służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. Z kolei NPOIK określa narodowe priorytety oraz standardy w zakresie ochrony tychże, w zakresie odpowiedzialności administracji rządowej, samorządowej oraz służb powołanych do zapewnienia bezpieczeństwa narodowego, a przy ich ustalaniu kluczowym kryterium jest ich znaczenie dla niezakłóconego funkcjonowania państwa oraz bezpieczeństwa obywateli. Celem Narodowego Programu Ochrony Infrastruktury Krytycznej jest stworzenie warunków do poprawy bezpieczeństwa IK, w szczególności w zakresie:

• zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej;

• przygotowania na sytuacje kryzysowe, które mogą niekorzystnie wpłynąć na infrastrukturę krytyczną;

• reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej;

• odtwarzania infrastruktury krytycznej[355].

Program wyodrębnia pięć podstawowych metod ochrony infrastruktury krytycznej:

a) *Ochronę fizyczną* – zespół przedsięwzięć minimalizujących ryzyko zakłócenia jej funkcjonowania przez osoby, które znalazły się na terenie infrastruktury krytycznej mimo braku stosownych uprawnień. Składają się na nią ochrona osób oraz ochrona mienia, a także przeciwdziałanie powstawaniu szkód i niedopuszczające do wstępu osób nieuprawnionych na teren chroniony.

[352] *https://rcb.gov.pl/narodowy-program-ochrony-infrastruktury-krytycznej-przyjety-przez-rade-ministrow-2* [dostęp: 25.02.2019]
[353] Pierwotna wersja Programu…, przygotowana w 2011 roku, została zakwalifikowana jako niejawna.
[354] Zakres kompetencyjny oraz rolę RCB w procesie identyfikacji i ochrony infrastruktury krytycznej opisano szerzej w pkt. 4.2.4 niniejszej pracy
[355] *https://rcb.gov.pl/narodowy-program-ochrony-infrastruktury-krytycznej-przyjety-przez-rade-ministrow-2* [dostęp: 25.02.2019]

b) *Ochronę osobową* – zespół przedsięwzięć i procedur mających na celu zmniejszenie ryzyka związanego z osobami, które przez uprawniony dostęp do obiektów, urządzeń, instalacji i usług IK mogą spowodować zakłócenia w jej funkcjonowaniu. Ochronę tę należy zatem powiązać z pracownikami oraz innymi osobami czasowo przebywającymi w obrębie infrastruktury krytycznej.
c) *Ochronę techniczną*, która obejmuje sprawy związane ze zgodnością budynków, urządzeń, instalacji i usług z obowiązującymi normami (np. budowlanymi), a także innymi przepisami (np. przeciwpożarowymi), co ma zagwarantować bezpieczne użytkowanie obrębie infrastruktury krytycznej oraz zabezpieczenie techniczne obiektu, czyli wykorzystanie płotów, barier, systemów telewizji przemysłowej, systemów dostępowych i tym podobnych środków.
d) *Ochronę teleinformatyczną* systemów i sieci teleinformatycznych służących infrastrukturze krytycznej – oznacza to również ochronę przed cyberprzestępstwami i cyberterroryzmem oraz przeciwdziałanie tego typu incydentom.
e) *Ochronę prawną* – zespół przedsięwzięć mających na celu minimalizację ryzyka związanego z działalnością innych podmiotów gospodarczych, państwowych lub prywatnych, których aktywność może prowadzić do zakłócenia w funkcjonowaniu obiektów, urządzeń, instalacji i usług infrastruktury krytycznej.

W załączniku nr 3 do Programu określono także kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej[356]. Wraz z jednolitym wykazem infrastruktury krytycznej kryteria te zostały opracowane i zaktualizowane przez Rządowe Centrum Bezpieczeństwa we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnych za poszczególne systemy. Procedurę opracowania kryteriów niezbędnych do stworzenia jednolitego wykazu infrastruktury krytycznej można określić jako wieloetapową. Obejmowała ona:

Etap I polegający na opracowaniu przez Rządowe Centrum Bezpieczeństwa kryteriów wyodrębniających systemy i instalacje należące do infrastruktury krytycznej i przekazaniu ich do uzgodnień organom centralnej administracji państwowej[357].

[356] Jest to dokument zawierający informacje niejawne, zgodnie z przepisami ustawy z 5.8.2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 poz. 1167

[357] *W celu sporządzenia Narodowego Programu Ochrony Infrastruktury Krytycznej, zwanego dalej "Programem", dyrektor Rządowego Centrum Bezpieczeństwa, zwany dalej "dyrektorem Centrum", opracowuje kryteria pozwalające wyodrębnić infrastrukturę krytyczną w ramach systemów, o których mowa w art. 3 pkt 2 ustawy, zwane dalej "kryteriami", i przekazuje je do uzgodnień ministrom i kierownikom urzędów*

Etap II – organy administracji i urzędów centralnych zobowiązani są przedstawić zwrotnie propozycje infrastruktury krytycznej do zamieszczenia w wykazie, a Dyrektor Centrum po dokonaniu weryfikacji zgodności z kryteriami ma obowiązek sporządzić wykaz w postaci tabeli obejmującej: „1) nazwę i lokalizację infrastruktury krytycznej; 2) podległość organizacyjną, w tym w stosunku do ministrów i kierowników urzędów centralnych, jeśli taka występuje; 3) dane operatora infrastruktury krytycznej; 4) dane zarządzającego w imieniu operatora infrastruktury krytycznej, jeśli taki występuje”[358].

Etap III, w którym organy administracji i urzędów centralnych, w terminie 6 miesięcy od dnia otrzymania kryteriów, mają obowiązek przedłożyć dyrektorowi Centrum informacje zawierające: „1) charakterystykę obszaru zadaniowego pozostającego w ich właściwości, obejmującą identyfikację jego zasobów, podsystemów, funkcji i zależności od innych systemów infrastruktury krytycznej; 2) propozycje wymagań i standardów pozwalających zapewnić ciągłość funkcjonowania infrastruktury krytycznej; 3) ogólną ocenę ryzyka dla funkcjonowania opisywanego obszaru zadaniowego, uwzględniającą zagrożenia, podatności na zagrożenie oraz konsekwencje zakłócenia funkcjonowania infrastruktury krytycznej; 4) propozycje priorytetów w zakresie odtwarzania infrastruktury krytycznej; 5) możliwe sposoby zapobiegania zakłóceniom funkcjonowania obszaru zadaniowego będącym skutkiem zakłócenia funkcjonowania infrastruktury krytycznej; 6) propozycje programów badawczych i rozwojowych mogących przyczynić się do zwiększenia bezpieczeństwa infrastruktury krytycznej”[359].

Etap IV – obejmuje na postawie wykazu powyższych informacji opracowanie projektu Programu przez Rządowe Centrum Bezpieczeństwa, a następnie przedstawia go Radzie Ministrów (wraz z protokołem rozbieżności, powstałych na etapie konsultacji).

Etap V – zatwierdzony przez Radę Ministrów wykaz podlega opracowaniu przez Rządowe Centrum Bezpieczeństwa oraz przekazaniu wyciągu (odpowiedniego każdorazowo dla kompetencji organu odbiorczego) organom administracji rządowej oraz samorządowej (tu rozumianej jako organy wojewódzkie podporządkowane administracji państwowej). Ponadto Rządowe Centrum Bezpieczeństwa informuje na piśmie operatorów infrastruktury krytycznej o ujęciu ich systemów w wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład

centralnych, o których mowa w art. 5b ust. 3 ustawy. - Rozporządzenie Rady Ministrów z 30.04.2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U.10.83.54) https://www.prawo.pl/akty/dz-u-2010-83-541,17619033.html [dostęp: 25.02.2019]

[358] § 4 Rozporządzenie Rady Ministrów z 30.04.2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U.10.83.54) https://www.prawo.pl/akty/dz-u-2010-83-541,17619033.html [dostęp: 25.02.2019]

[359] Ibidem, § 5

infrastruktury krytycznej. Wykaz ten podlega stałej aktualizacji – przeprowadzanej na wniosek właściwego ministra lub kierownika urzędu centralnego odpowiedzialnego za dany system, wojewody lub operatora infrastruktury krytycznej[360].

Rządowe Centrum Bezpieczeństwa odgrywa zatem kluczową rolę w zakresie identyfikacji i stałej aktualizacji wykazu infrastruktury krytycznej, niemniej jednak w Programie z 2013 roku podkreśla się, że dystynktywnym kryterium skuteczności i komplementarności ochrony infrastruktury krytycznej jest współpraca sektora publicznego z sektorem prywatnym.

„Ważnym elementem [tej] współpracy jest wypracowanie przejrzystych zasad i procedur między organami i służbami państwa a właścicielami oraz posiadaczami samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej. Należy jednak z naciskiem zaznaczyć, że partnerstwo międzysektorowe w rozumieniu Programu oznacza jedynie ograniczoną formę współpracy między jednostkami administracji publicznej a podmiotami prywatnymi, poprzez na przykład wymianę wszelkich informacji mogących mieć wpływ na osiągnięcie celów NPOIK. Takie partnerstwo nie przewiduje natomiast zawarcia jakiejkolwiek umowy, na podstawie której następowałaby realizacja za wynagrodzeniem przez partnera prywatnego przedsięwzięcia na rzecz podmiotu publicznego”[361].

Warto dostrzec, że autorzy dokumentu dokonali także identyfikacji słabości procedury nakładania na operatorów infrastruktury krytycznej obowiązków w drodze ustaw czy rozporządzeń „ze względu na realny brak możliwości prowadzenia audytu i kontroli ich realizacji. Mając to na uwadze, w działania z zakresu ochrony IK w większym stopniu należy zaangażować podmioty, które nią zarządzają – jednak nie jedynie w drodze nakazów, ale świadomego udziału w przedsięwzięciach mających na celu poprawę bezpieczeństwa systemów istotnych dla funkcjonowania społeczeństwa, poprzez intensyfikację współpracy sektora prywatnego i publicznego w tym zakresie”[362].

Program z 2013 roku określił także zakres zadań i obowiązków jednostek samorządu terytorialnego w zakresie ochrony infrastruktury krytycznej (choć zostały one zdefiniowane już w *Ustawie z 26.04.2007 roku o zarządzaniu kryzysowym*, niemniej jednak nie sprecyzowano w niej zakresu obowiązku samorządu województwa). Zadaniem wojewody, starosty i wójta

---

[360] § 6 ust. 1 i 2, § 10 oraz § 11 ust. 1 i 2 *Uchwały nr r 67 Rady Ministrów z 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022”*, Monitor Polski z 16 maja 2013 r., poz. 377, s. 73

[361] Wiercińska-Krużewska A., Gajek P*., Prawne uwarunkowania ochrony infrastruktury krytycznej* [w:] *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny, Kraków 2015, s*. 32.

[362] Uchwała nr 67 Rady Ministrów z 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022”, *op. cit*., s. 73

(odpowiednio także burmistrza i prezydenta) jest między innymi organizacja wykonywania zadań z zakresu ochrony infrastruktury krytycznej: „gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej, opracowywanie i wdrażanie procedur na wypadek ich wystąpienia, odtwarzanie infrastruktury krytycznej oraz współpraca między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w celu jej ochrony. W obszarze planowania cywilnego do zadań wojewody, starosty i wójta należy przygotowanie rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej. Powinny uwzględniać zapewnienie działania i możliwości jej odtworzenia. […] Obowiązek podjęcia działań w zakresie zarządzania kryzysowego [w tym ochrony IK] spoczywa na organie właściwym w sprawach zarządzania kryzysowego, który pierwszy otrzymał informację o wystąpieniu zagrożenia. O zaistniałym zdarzeniu niezwłocznie informuje on odpowiednio organy wyższego i niższego szczebla, przedstawiając jednocześnie swoją ocenę sytuacji oraz informację o zamierzonych działaniach” [363].

5.2.4. *Narodowy Program Ochrony Infrastruktury Krytycznej*[364] *z 2018 roku*

Dokument ten, przyjęty w dniu 7 września 2018 roku, stanowi aktualizację Narodowego Programu Ochrony Infrastruktury Krytycznej przyjętego uchwałą Rady Ministrów w dniu 26 marca 2013 roku. Jak zapisano we wprowadzeniu, „działająca sprawnie i w sposób niezakłócony infrastruktura krytyczna ma coraz większy wpływ na obywateli, struktury administracji i gospodarkę. Administracja i przedsiębiorcy stają się współzależni. Powstaje wspólna infrastruktura realizująca procesy na rzecz obydwu stron. Prowadzi to do uzależnienia się w takim stopniu, że dysfunkcja tej infrastruktury może prowadzić do skutków wykraczających poza granice władającej nią organizacji. Tym samym konieczne staje się uznanie ochrony IK jako procesu ukierunkowanego na ochronę ciągłości świadczenia określonej usługi oraz odtworzenia jej w razie potrzeby.[365] Z tej właśnie przyczyny, nowa edycja Programu proponuje działania mające pomóc w ustaleniu skali współzależności i podjęciu skutecznych działań celem zredukowania ryzyka zakłócenia funkcjonowania IK”[366].

[363] Panasiuk A., Sierański S., *Bezpieczeństwo państwa i obywateli. Ochrona obiektów infrastruktury krytycznej*. [w:] „Kontrola Państwowa” Nr 1, styczeń-luty 2017, s. 781-82.
[364] *https://rcb.gov.pl/narodowy-program-ochrony-infrastruktury-krytycznej-przyjety-przez-rade-ministrow-2* [dostęp: 25.02.2019]
[365] *http://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf., s 4.* dostęp: [25.02.2019]
[366] *Ibidem*, s. 5.

Głównym celem Programu jest „stworzenie warunków do poprawy bezpieczeństwa IK. Wraz z innymi dokumentami programowymi składa się on na cel nadrzędny – podniesienie bezpieczeństwa Rzeczypospolitej Polskiej" – w tym zakresie dokument nie różni się od edycji poprzedniej. Znaczne różnice ilościowe występują jednak na etapie formułowania celów pośrednich (szczegółowych), wśród których wymieniono zaledwie pięć, podczas gdy w edycji z roku 2013 wyszczególniono ich osiem). Cele te przewidują:

- „zdobycie określonego poziomu świadomości, wiedzy i kompetencji wszystkich uczestników Programu w zakresie znaczenia IK dla sprawnego funkcjonowania państwa oraz sposobów i metod jej ochrony,
- wprowadzenie metodyki oceny ryzyka uwzględniającej pełny wachlarz zagrożeń, w tym metodyki postępowania z zagrożeniami o bardzo małym prawdopodobieństwie i katastrofalnych skutkach,
- wprowadzenie skoordynowanego i opartego na ocenie ryzyka podejścia do realizacji zadań z zakresu ochrony IK,
- budowa partnerstwa między uczestnikami procesu ochrony IK,
- wprowadzenie mechanizmów wymiany i ochrony informacji przekazywanych między uczestnikami procesu ochrony IK"[367].

Narodowy Program Ochrony Infrastruktury Krytycznej z 2018 roku podtrzymuje przyjęte w poprzedniej edycji bezsankcyjne podejście do ochrony prawnej infrastruktury krytycznej. Podstawą tego rozumienia systemu ochrony jest założenie autorów, że „zwiększenie skuteczności ochrony IK może nastąpić jedynie przez działania jej operatorów wspieranych przez możliwości i potencjał administracji publicznej"[368]. Niestety, bezsankcyjność wiąże się także z brakiem wsparcia finansowego operatorów infrastruktury krytycznej, co przedstawione jest jako czynnik równowagi pomiędzy „władczym oddziaływaniem państwa, a wydatkami niezbędnymi do poprawy bezpieczeństwa IK". Przypomniano tym samym, iż „[...] ustawa o zarządzaniu kryzysowym nie przewiduje sankcji za niedopełnienie obowiązków w niej określonych, jak również nie przewiduje wsparcia budżetowego operatorów IK"[369] oraz zaprezentowano katalog zasad ujętych jako wytyczne dla realizowania celów Programu przez jego odbiorców. Wśród nich jako najważniejsze filary wskazano:

[367] *Ibidem*, s. 6.
[368] *Ibidem*, s. 9.
[369] *Ibidem*.

- współodpowiedzialność rozumianą „[…] jako wspólne (zbiorowe) dążenie do poprawy bezpieczeństwa IK wynikające ze świadomości jej znaczenia dla funkcjonowania zarówno organów administracji publicznej, jak i operatorów IK, społeczeństwa, gospodarki i państwa. Ochrona infrastruktury krytycznej leży bowiem w interesie zarówno jej operatorów, jak i odpowiedzialnej za funkcjonowanie państwa administracji”[370];
- współpracę oznaczającą „wykonywanie razem przez uczestników ochrony IK określonych, zbieżnych i wzajemnie uzupełniających się zadań dla osiągnięcia wspólnego celu, który wynika z zasady współodpowiedzialności. Współpraca jest niezbędna w przypadku chęci uniknięcia powielania działań i ponoszonych kosztów oraz efektywniejszego wykorzystania posiadanych sił i środków”[371];
- zaufanie – trzeci filar systemu ochrony infrastruktury krytycznej – rozumiane jako „przekonanie, że motywacją działania uczestników ochrony IK (dotyczy to w szczególności administracji i operatorów IK) jest dążenie do wspólnego celu – poprawy bezpieczeństwa IK i RP. Osiągnięcie tego celu będzie zatem korzystne dla wszystkich zainteresowanych stron, w tym przede wszystkim społeczeństwa”[372].

5.3. Instytucje powołane do ochrony infrastruktury krytycznej

5.3.1. Rządowe Centrum Bezpieczeństwa

Rządowe Centrum Bezpieczeństwa rozpoczęło działalność 2 sierpnia 2008 roku, a jego powołania dokonano na podstawie *Ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym*[373] (art. 10) i *Rozporządzenia Prezesa Rady Ministrów z dnia 11 kwietnia 2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa*[374].

Rządowe Centrum Bezpieczeństwa jest centralną jednostką koordynującą system zarządzania kryzysowego, państwową jednostką budżetową podległą Prezesowi Rady Ministrów. Właściwe będzie także rozumieć RCB jako kluczowy element struktury o charakterze ponadresortowym, którego zadaniem jest zoptymalizowanie i ujednolicenie postrzegania zagrożeń przez poszczególne elementy tej struktury, a tym samym podwyższenie stopnia

[370] *Ibidem*.
[371] *Ibidem*.
[372] *Ibidem*, s.10.
[373] *Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz.U. 2007 nr 89 poz. 590, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id= WDU20070890590 – [dostęp: 28.02.1019]
[374] *http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20110860471* - [dostęp: 28.02.1019]

zdolności radzenia sobie z trudnymi sytuacjami przez właściwe służby i organy administracji publicznej.

Do podstawowych zadań Rządowego Centrum Bezpieczeństwa należy dokonywanie pełnej analizy zagrożeń w oparciu o dane uzyskiwane ze wszystkich możliwych „ośrodków kryzysowych" funkcjonujących w ramach administracji publicznej oraz w oparciu o dane od partnerów międzynarodowych. Ponadto do zadań Rządowego Centrum Bezpieczeństwa należy opracowywanie optymalnych rozwiązań pojawiających się sytuacji kryzysowych, a także koordynowanie przepływu informacj**i** o zagrożeniach.

W ramach Rządowego Centrum Bezpieczeństwa utworzono Wydział Ochrony Infrastruktury Krytycznej, a do zakresu jego obowiązków należy między innymi:

- opracowanie projektu i aktualizowanie Narodowego Programu Ochrony Infrastruktury Krytycznej;
- tworzenie i aktualizowanie kryteriów umożliwiających sporządzenie jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy;
- sporządzanie i aktualizacja jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy;
- analizowanie treści planów ochrony infrastruktury krytycznej, przedstawionych przez operatorów do zatwierdzenia dyrektorowi Centrum;
- sporządzanie analiz i prognoz dotyczących krajowej infrastruktury krytycznej, analizowanie rozwiązań międzynarodowych oraz współpraca w tym zakresie z podmiotami krajowymi i zagranicznymi, w tym z ośrodkami naukowymi i badawczymi;
- współpraca w zakresie ochrony infrastruktury krytycznej z ministerstwami, urzędami i odpowiednimi służbami;
- współpraca w zakresie ochrony infrastruktury krytycznej z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej;
- współpraca jako krajowy punkt kontaktowy, z instytucjami Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz ich krajami członkowskimi w zakresie ochrony europejskiej infrastruktury krytycznej i infrastruktury krytycznej[375].

[375] *Ibidem.*

5.3.2. Agencja Bezpieczeństwa Wewnętrznego (ABW)

Agencja Bezpieczeństwa Wewnętrznego utworzona została na mocy ustawy z dnia 24 maja 2002 roku (tekst jednolity Dz.U. z 2017 r., poz. 1920, 2405 z późn. zm.)[376], Rozporządzeniem Prezesa Rady Ministrów z dnia 01.10.2018 roku (M. P. z 2018, poz. 927)[377]. ABW nadano statut organizacyjny, w którym określono między innymi strukturę Agencji. Zgodnie z wytycznymi na czele Agencji Bezpieczeństwa Wewnętrznego stoi Szef ABW. Pełni on funkcję krajowej władzy bezpieczeństwa w stosunkach międzynarodowych, to znaczy odpowiada za wdrażanie uzgodnionych zasad i środków ochrony informacji niejawnych. Od dnia 2 stycznia 2011 roku Szef ABW pełni funkcję krajowej władzy bezpieczeństwa. W sferze wojskowej funkcję tę Szef ABW pełni za pośrednictwem Szefa SKW.

W skład Agencji wchodzą następujące jednostki organizacyjne:

1) Departament Bezpieczeństwa Teleinformatycznego (Departament I);
2) Departament Kontrwywiadu (Departament II);
3) Departament Postępowań Karnych (Departament III);
4) Departament Ochrony Informacji Niejawnych (Departament IV);
5) Departament Wsparcia Operacyjno-Technicznego (Departament V);
6) Departament Bezpieczeństwa Wewnętrznego i Audytu (Departament VI);
7) Departament Zagrożeń Strategicznych (Departament VII);
8) Departament Informacji, Analiz i Prognoz (Departament VIII);
9) Centrum Antyterrorystyczne (CAT);
10) Centrum Prewencji Terrorystycznej (CPT);
11) Biuro Prawne (Biuro A);
12) Biuro Badań Kryminalistycznych (Biuro B);
13) Gabinet Szefa (Biuro D);
14) Biuro Ewidencji i Archiwum (Biuro E);
15) Biuro Finansów (Biuro F);
16) Biuro Kadr (Biuro K);
17) Biuro Logistyki (Biuro L);
18) Centralny Ośrodek Szkolenia i Edukacji (COS);

[376] https://www.abw.gov.pl/pl/prawo/273,Prawo.html – [dostęp: 08.03.2019]
[377] https://bip.abw.gov.pl/bip/struktura/47,Struktura-organizacyjna.html – [dostęp: 08.03.2019]

19) Delegatura ABW w Białymstoku;
20) Delegatura ABW w Gdańsku;
21) Delegatura ABW w Katowicach;
22) Delegatura ABW w Lublinie;
23) Delegatura ABW w Poznaniu[378].

Agencja Bezpieczeństwa Wewnętrznego ustawowo zobowiązana jest do rozpoznawania zagrożeń terrorystycznych i zapobiegania aktom terroru. Pozyskiwanie i analizowanie informacji pozwala na ocenę źródeł i skali zjawiska, wytypowanie grup potencjalnych zamachowców, rozpoznanie ich planów i zaplecza logistycznego. Walka z terroryzmem wymaga ścisłej współpracy z innymi służbami i instytucjami państwowymi oraz organizacjami międzynarodowymi. Skuteczną koordynację działań podejmowanych przez jednostki odpowiedzialne za ochronę antyterrorystyczną Polski ma zapewnić powołane w ramach ABW Centrum Antyterrorystyczne. Naczelną funkcją Centrum Antyterrorystycznego ABW jest koordynacja – w zakresie analityczno-informacyjnym – działań służb i instytucji uczestniczących w zabezpieczeniu kraju przed zagrożeniami ze strony terroryzmu. Centrum wypełnia tę funkcję poprzez realizację następujących zadań:

- wspomaganie procesów decyzyjnych w przypadku realnego zagrożenia atakiem terrorystycznym;
- koordynację współdziałania służb odpowiedzialnych za zwalczanie terroryzmu w zakresie działań operacyjno-rozpoznawczych;
- wykonywanie czynności analityczno-informacyjnych;
- udział w opracowywaniu i nowelizowaniu procedur reagowania kryzysowego na wypadek ataku oraz sporządzanie algorytmów działań przed zamachem;
- monitoring zagranicznych mediów sympatyzujących z terrorystami;
- wspomaganie po ewentualnym zamachu terrorystycznym działań służb i instytucji uczestniczących w ochronie antyterrorystycznej Polski;
- współpracę zagraniczną [379].

Częścią Agencji Bezpieczeństwa Wewnętrznego jest również Centrum Prewencji Terrorystycznej ABW, które specjalizuje się w szeroko pojętej profilaktyce terrorystycznej, której

[378] *Ibidem*
[379] *Ibidem*

kluczowym elementem jest rozpowszechniane wiedzy na temat możliwości zapobiegania zdarzeniom, które są istotne z punktu widzenia bezpieczeństwa. W tym zakresie Centrum organizuje specjalistyczne szkolenia dla pracowników administracji publicznej i jednostek odpowiedzialnych za system bezpieczeństwa. Agencja Bezpieczeństwa Wewnętrznego odpowiada za zapewnienie właściwej ochrony informacji niejawnych, zwłaszcza oznaczonych klauzulą „tajne" i „ściśle tajne".

Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych,[380] w której określone zostały zasady, rodzaje i sposób przeprowadzania postępowań sprawdzających oraz procedury ochrony fizycznej i teleinformatycznej, zastąpiła obowiązującą od 1999 roku poprzednią regulację. System ochrony informacji niejawnych jest oparty na kilku podstawowych zasadach, które są wiążące niezależnie od zmian wprowadzanych w rozwiązaniach szczegółowych.

5.3.3. Agencja Wywiadu (AW)

Zgodnie z art. 6 ust. 2 *Ustawy z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U. z 2017 r., poz. 1920, 2405)[381] zadania prawnie przypisane Agencji Wywiadu realizowane są poza granicami Rzeczypospolitej Polskiej. Agencja Wywiadu może realizować na terytorium Polski czynności określone w odrębnych przepisach, jednak wyłącznie w związku z realizacją działań poza granicami państwa. W ich skład wchodzi także ochrona infrastruktury krytycznej.

Zgodnie z *Zarządzeniem Nr 106 Prezesa Rady Ministrów z dnia 03.07.2018 roku*, zmieniającym zarządzenie w sprawie nadania statutu Agencji Wywiadu (M.P. poz. 660)[382], na podstawie art. 20 ust.1 Ustawy z dnia 24.05.2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2017 r. poz. 1920, z późn. zm.), w skład AW wchodzą następujące jednostki organizacyjne:

1) Departament Operacyjny,
2) Departament Informacyjny,
3) Departament Techniczny,
4) Biuro Bezpieczeństwa,

[380] *http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101821228* - [dostęp: 08.03.2019]
[381] *https://aw.gov.pl/prawo/* - [dostęp: 08.03.2019]
[382] *http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WMP20180000660/O/M20180660.pdf* - [dostęp: 08.03.2019]

5) Biuro Finansowo-Administracyjne,

6) Biuro Kadr i Szkoleń,

7) Biuro Prawne,

8) Gabinet Szefa,

9) Samodzielny Wydział do Spraw Zarządzania Kryzysowego.

Do zadań Agencji Wywiadu należy:

- 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;
- rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczypospolitej Polskiej;
- ochrona zagranicznych przedstawicielstw Rzeczypospolitej Polskiej i ich pracowników przed działaniami obcych służb specjalnych i innymi działaniami mogącymi przynieść szkodę interesom Rzeczypospolitej Polskiej;
- zapewnienie ochrony kryptograficznej łączności z polskimi placówkami dyplomatycznymi i konsularnymi oraz poczty kurierskiej;
- rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej;
- 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;
- rozpoznawanie i analizowanie zagrożeń występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa, oraz podejmowanie działań mających na celu eliminowanie tych zagrożeń;
- prowadzenie wywiadu elektronicznego;
- podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych[383].

[383] *Ibidem.*

5.3.4. Służba Kontrwywiadu Wojskowego (SKW)

Służba Kontrwywiadu Wojskowego działa na podstawie *Ustawy z dnia 9 czerwca 2006 roku o służbie kontrwywiadu wojskowego oraz służbie wywiadu wojskowego*[384]. Służba Kontrwywiadu Wojskowego rozpoznaje, zapobiega oraz wykrywa popełniane przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników SZ RP i innych jednostek organizacyjnych MON przestępstwa, godzące w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność.

5.3.5. Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych

Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych utworzony został na podstawie *Zarządzenia nr 162 Prezesa Rady Ministrów z 25 października 2006 roku*[385].
Jest to organ pomocniczy Rady Ministrów, który zapewnia współdziałanie administracji rządowej w zakresie rozpoznawania, przeciwdziałania i zwalczania terroryzmu. Do podstawowych zadań Zespołu należy między innymi: monitorowanie zagrożeń o charakterze terrorystycznym, przedstawianie opinii i wniosków dla Rady Ministrów, opracowywanie projektów standardów i procedur w zakresie zwalczania terroryzmu, inicjowanie i koordynowanie działań podejmowanych przez właściwe organy administracji rządowej, organizowanie współpracy z innymi państwami w zakresie zwalczania terroryzmu *etc*. W jego skład wchodzą:

1. przewodniczący – minister właściwy do spraw wewnętrznych;
2. zastępcy – minister właściwy do spraw finansów publicznych, minister właściwy do spraw instytucji finansowych, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych, Minister Sprawiedliwości, a także Minister – Członek Rady Ministrów, Koordynator Służb Specjalnych;
3. sekretarz – osoba powołana przez przewodniczącego Zespołu spośród pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych;
4. członkowie:

a) sekretarz stanu lub podsekretarz stanu wyznaczony przez ministra właściwego do spraw wewnętrznych, sprawujący nadzór nad prowadzeniem spraw objętych działem administracji

[384] *http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040709-* [dostęp: 08.03.2019]
[385] *https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/organy-pomocnicze/organy-pomocnicze-rady/128,Miedzyresortowy-Zespol-do-Spraw-Zagrozen-Terrorystycznych.html-* [dostęp: 08.03.2019]

rządowej – sprawy wewnętrzne w zakresie ochrony bezpieczeństwa i porządku publicznego;
b) sekretarz stanu lub podsekretarz stanu wyznaczony przez ministra właściwego do spraw wewnętrznych, sprawujący nadzór nad prowadzeniem spraw objętych działem administracji rządowej – sprawy wewnętrzne w zakresie zarządzania kryzysowego, ochrony przeciwpożarowej i obrony cywilnej;
c) Sekretarz Kolegium do Spraw Służb Specjalnych lub osoba go zastępująca,
d) Szef Obrony Cywilnej Kraju lub jego zastępca,
e) Szef Agencji Bezpieczeństwa Wewnętrznego lub jego zastępca,
f) Szef Agencji Wywiadu lub jego zastępca,
g) Komendant Służby Ochrony Państwa lub jego zastępca,
h) Komendant Główny Policji lub jego zastępca,
i) Komendant Główny Straży Granicznej lub jego zastępca,
j) Komendant Główny Państwowej Straży Pożarnej lub jego zastępca,
k) Szef Sztabu Generalnego Wojska Polskiego lub jego zastępca,
l) Dowódca Operacyjny Rodzajów Sił Zbrojnych lub jego zastępca,
m) Szef Służby Wywiadu Wojskowego lub jego zastępca,
n) Szef Służby Kontrwywiadu Wojskowego lub jego zastępca,
o) Komendant Główny Żandarmerii Wojskowej lub jego zastępca,
p) Generalny Inspektor Informacji Finansowej lub osoba go zastępująca,
q) Szef Krajowej Administracji Skarbowej lub jego zastępca,
r) Dyrektor Rządowego Centrum Bezpieczeństwa lub osoba go zastępująca[386].

5.3.6. Zestawienie Dokumentów programowych Unii Europejskiej oraz polskich aktów prawnych związanych z ochroną infrastruktury krytycznej w latach 2004-2011

20.10.2004	*Communication from the Commission to the Council and the European Parliament Critical Infrastructure Protection in the fight against terrorism, Brussels, 20.10.2004, COM(2004) 702 final*.
24.02.2005	Decyzja Ramowa Rady 2005/222/WSiSW z dnia 24.02.2005 r. w sprawie ataków na systemy informatyczne.

386 *Ibidem.*

17.11.2005	Zielona Księga w sprawie europejskiego programu ochrony infrastruktury krytycznej COM(2005) 576 końcowy. Bruksela, 17.11.2005.
28.11.2005	Komunikat Komisji dla Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie wzmocnienia koordynacji w zakresie ogólnego planowania gotowości na wypadek sytuacji zagrożenia zdrowia publicznego na poziomie UE.
12.12.2006	Komunikat Komisji w sprawie europejskiego programu ochrony infrastruktury krytycznej: KOM2006) 786 wersja ostateczna, Bruksela, dnia 12.12.2006.
26.04.2007	*Ustawa z dnia 26.04.2007 roku o zarządzaniu kryzysowym*.
14.08.2008	*Zarządzenie Nr 86 Prezesa Rady Ministrów z dnia 14.08.2008 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego, określające tryb i formę zwoływania posiedzeń oraz zasady obsługi i zadania*.
08.12.2008	*Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*.
22.04.2009	Sieć ostrzegania o zagrożeniach dla infrastruktury krytycznej (CIWIN).
17.07.2009	Ustawa o zmianie ustawy o zarządzaniu kryzysowym.
15.09.2010	*Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 roku w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania*.
30.04.2010	*Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz.U. z 2010 nr 83 poz. 540)*.
30.04.2010	*Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. z 2010 nr 83 poz. 541).*
30.04.2010	*Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. z 2010 nr 83 poz. 542).*
29.10.2010	Ustawa o zmianie ustawy o zarządzaniu kryzysowym.

31.03.2011	Komunikat Komisji Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury teleinformatycznej „Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni". Bruksela, dnia 31.3.2011, KOM(2011) 163 wersja ostateczna.
11.04.2011	*Rozporządzenie Prezesa Rady Ministrów z dnia 11 kwietnia 2011 roku w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa.*
27.05.2011	Projekt konkluzji Rady Unii Europejskiej w sprawie rozwoju zewnętrznego wymiaru europejskiego programu ochrony infrastruktury krytycznej – Przyjęcie, 10662/11, Bruksela, 27 maja 2011 roku.

Rozdział VI

Infrastruktura krytyczna Rzeczypospolitej Polskiej

6.1. Infrastruktura krytyczna RP – systematyka

6.1.1. System zaopatrzenia w energię, surowce energetyczne i paliwa

Zapewnienie obywatelom energii elektrycznej oraz cieplnej, jak również zaopatrzenie struktur państwa w paliwa gwarantuje funkcjonowanie gospodarki oraz społeczeństwa. Zapotrzebowanie gospodarki i społeczeństwa na energię sprawia, że system zaopatrzenia w energię, surowce energetyczne i paliwa jest systemem o szczególnym znaczeniu dla funkcjonowania państwa. Infrastruktura systemu zapewnia wydobycie węgla na potrzeby elektroenergetyki, wytwarzanie energii elektrycznej wraz z dostarczaniem jej odbiorcom indywidualnym i przemysłowi, umożliwia wydobycie, import i przetwarzanie surowej ropy naftowej oraz produkcję i dostarczanie paliw płynnych dla sfer działalności państwa je wykorzystujących, jak również wydobycie, import i dostarczanie odbiorcom gazu ziemnego gwarantującego użytkowanie urządzeń grzewczych w gospodarstwach domowych oraz wytwarzanie dóbr materialnych opartych o gaz ziemny.

6.1.2. Sektor energii elektrycznej – system elektroenergetyczny

Sektor energii elektrycznej to dziedzina przemysłu grupująca podmioty wytwarzające energię elektryczną, operatora sieci przesyłowej, operatorów sieci dystrybucyjnej i podmioty sprzedające energię elektryczną. Dostęp i korzystanie z zalet energii elektrycznej wymaga sprawnego działania rozbudowanego układu urządzeń do jej wytwarzania, przesyłania i rozdziału.

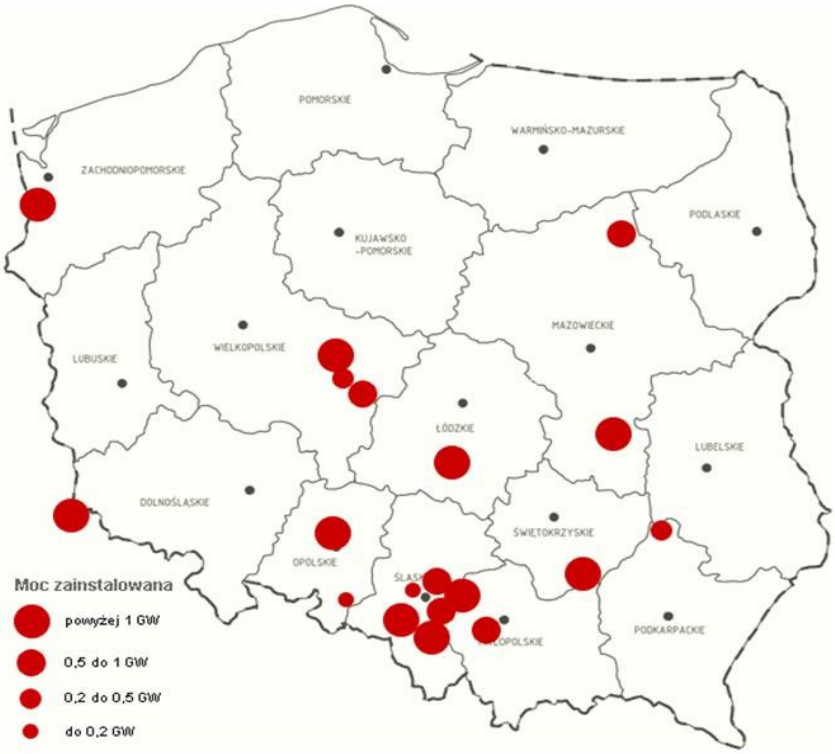
Łączna moc zainstalowana w polskim systemie elektroenergetycznym przekracza 40 tys. MW. Systematykę z uwagi na rodzaj elektrowni przedstawia poniższa tabela:

Tabela 4. **System elektroenergetyczny w Polsce - Moc zainstalowana (dane na koniec III kwartału 2017 r.)**

Wyszczególnienie	Moc elektryczna zainstalowana [MW]
OGÓŁEM	40.059,1
Elektrownie zawodowe cieplne	31461,9
z tego: - na węglu brunatnym	9603,8
- na węglu kamiennym	21819,4
- gazowe	886,0
Elektrownie zawodowe wodne	2189,0
- w tym: szczytowo-pompowe	1330,0
Elektrociepłownie przemysłowe	1900,2
Elektrownie niezależne OZE	2508,0
- w tym: elektrownie wiatrowe	2291,7

Źródło: Kwartalnik ARE „Sytuacja w elektroenergetyce”.

Mapa 1. **Schemat lokalizacji elektrowni w Polsce**



Źródło: cire.pl [dostęp: 08.03.2019].

Przesył energii z elektrowni do odbiorcy możliwy jest dzięki rozległej sieci linii i stacji elektroenergetycznych. Wiąże się on jednak ze stratami. Zasadniczy sposób ich zmniejszenia

polega na podwyższaniu napięcia elektroenergetycznych linii przesyłowych. W zależności od odległości, na jakie ma być przesyłana energia, stosowane są różne wartości napięć:

- od 220 do 400 kV (tzw. najwyższe napięcia) w przypadku przesyłania na duże odległości;
- 110 kV (tzw. wysokie napięcie) w przypadku przesyłania na odległości nieprzekraczające kilkudziesięciu kilometrów;
- od 10 do 30 kV (tzw. średnie napięcia) stosowane w lokalnych liniach rozdzielczych.

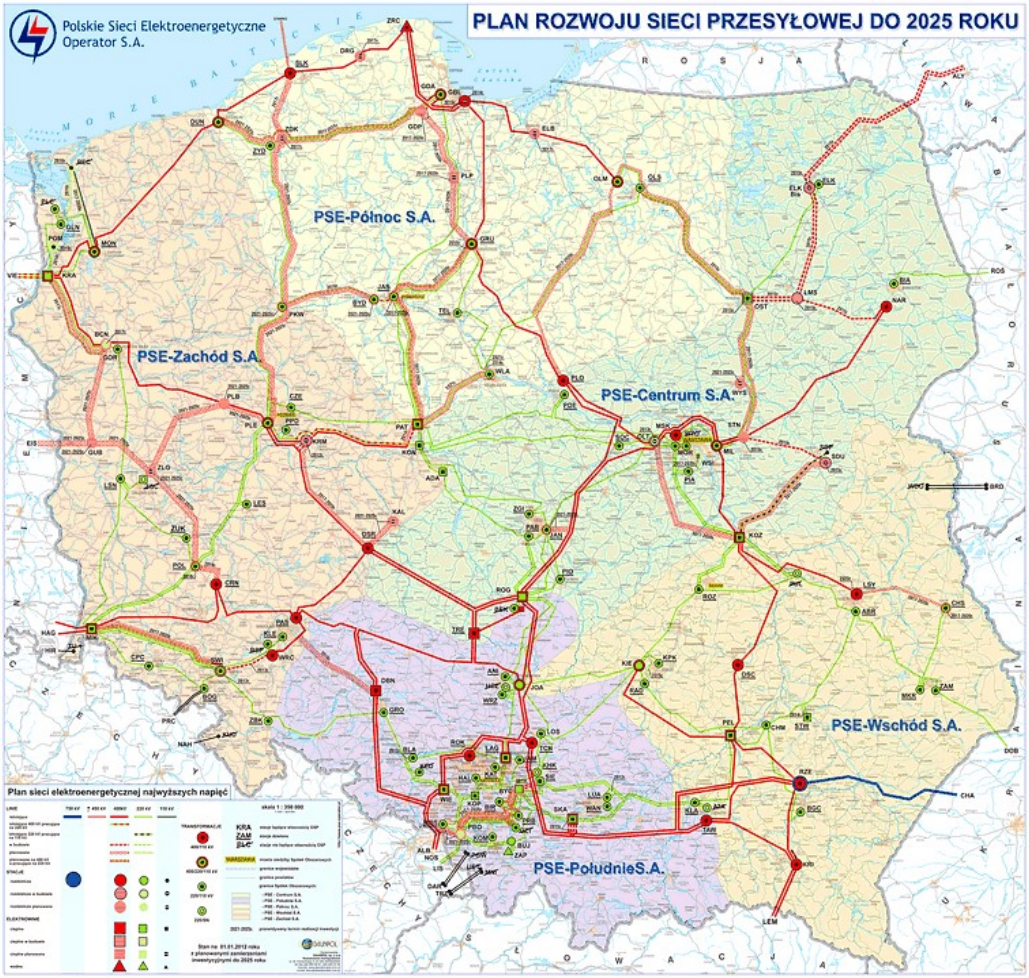
Podnoszenie napięcia dla celów przesyłu, a następnie obniżania do poziomu, na którym możliwe jest stosowanie elektrycznych urządzeń powszechnego użytku zbudowanego na napięcie 220/230 lub 380/400 V, wymaga korzystania z systemowych stacji elektroenergetycznych najwyższych napięć, wielu stacji rozdzielczych wysokiego napięcia oraz rozlicznych stacji transformatorowych zamieniających średnie napięcie (rozdzielcze) na powszechnie stosowane w instalacjach odbiorczych (230/400 V). Wszystkie te obiekty – linie i stacje elektroenergetyczne – składają się na system elektroenergetyczny.

Nie ma obecnie możliwości magazynowania energii elektrycznej, co oznacza, że w każdym momencie ilość energii wytwarzanej w elektrowniach musi być równa energii zużywanej przez odbiorców. Od systemu elektroenergetycznego wymaga się zatem, by był zdolny do zmiany kierunków i ilości przesyłanej energii. Jest to możliwe dzięki licznym połączeniom między elektrowniami, stacjami elektroenergetycznymi oraz grupami odbiorców energii. Połączenia takie zapewnia sieć linii elektroenergetycznych, które pracują na różnych poziomach napięć. Im sieć ta jest bardziej rozbudowana, a linie nowoczesne, tym większa szansa na niezawodną dostawę energii do każdego odbiorcy. Właścicielem i gospodarzem sieci przesyłowej najwyższych napięć jest w Polsce PSE Operator S.A.[387]. Spółka ta pełni rolę operatora systemu przesyłowego (OSP). OSP energii elektrycznej to przedsiębiorstwo energetyczne zajmujące się przesyłaniem energii elektrycznej, będące odpowiedzialne za ruch sieciowy w systemie przesyłowym elektroenergetycznym, bieżące i długookresowe bezpieczeństwo funkcjonowania tego systemu, eksploatację, konserwację, remonty oraz niezbędną rozbudowę sieci przesyłowej, w tym budowę połączeń z innymi systemami elektroenergetycznymi.

[387] Podstawowe informacje o krajowym systemie elektroenergetycznym za stroną: *PSE Operator S.A. http://www.pse-operator.pl/index.php?dzid=79&did=22* [dostęp: 08.03.2019]

Do obowiązków OSP należy również bilansowanie systemu polegające na równoważeniu zapotrzebowania na energię elektryczną z dostawami energii oraz zarządzanie ograniczeniami systemowymi w celu zapewnienia niezakłóconego i bezpiecznego funkcjonowania systemu elektroenergetycznego. W przypadku wystąpienia ograniczeń technicznych w przepustowości tych systemów zarządzanie ograniczeniami systemowymi odbywa się w zakresie wymaganych parametrów technicznych energii elektrycznej.

Mapa 2. **Schemat sieci przesyłowej w Polsce**[388]



Źródło: PSE Operator S.A.

[388] Liniami przerywanymi zaznaczono linie w budowie oraz planowane. Mapa w większym rozmiarze dostępna na stronie *http://www.pse-operator.pl/index.php?dzid=80&did=23* - [dostęp: 08.03.2019]

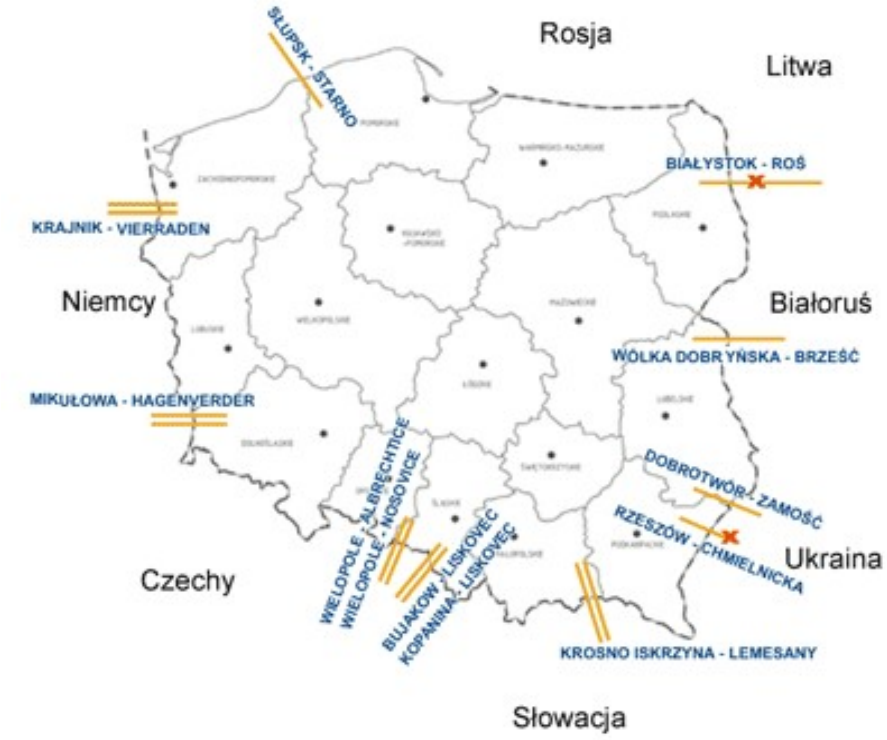
PSE Operator S.A. realizuje zadania operatora systemu przesyłowego w oparciu o posiadaną sieć przesyłową najwyższych napięć, którą tworzą[389]:

- 242 linie o łącznej długości 13 396 km, w tym:
- 1 linia o napięciu 750 kV o długości 114 km,
- 74 linie o napięciu 400 kV o łącznej długości 5 340 km,
- 167 linii o napięciu 220 kV o łącznej długości 7 942 km,
- 100 stacji najwyższych napięć (NN) oraz podmorskie połączenie 450 kV DC Polska – Szwecja o całkowitej długości 254 km.

Całkowita zdolność przepustowa połączeń polskiego systemu elektroenergetycznego z krajami Unii Europejskiej wynosi 2000-3000 MW (oczywiście w zależności od konfiguracji pracy systemu) i jest ograniczona zdolnościami przesyłowymi wewnątrz krajowego systemu. Obecna moc połączeń transgranicznych spełnia cel uznany przez Radę Europy mówiący o minimum 10% zdolności przesyłowej połączeń transgranicznych w stosunku do mocy zainstalowanej w krajowym systemie elektroenergetycznym[390].

[389] http://www.pse-operator.pl/index.php?dzid=79&did=22 - [dostęp: 08.03.2019]
[390] *http://www.cire.pl/rynekenergii/import.php?smid=205* - [dostęp: 08.03.2019]

Mapa 3. **Międzynarodowe połączenia elektroenergetyczne**



*Źródło: cire.pl***.**

Kolejnym ważnym elementem systemu elektroenergetycznego są operatorzy systemów dystrybucyjnych (OSD). OSD energii elektrycznej to przedsiębiorstwa energetyczne zajmujące się dystrybucją energii elektrycznej, odpowiedzialne za ruch sieciowy w systemie dystrybucyjnym elektroenergetycznym, bieżące i długookresowe bezpieczeństwo funkcjonowania tego systemu, eksploatację, konserwację, remonty oraz niezbędną rozbudowę sieci dystrybucyjnej, w tym połączeń z innymi systemami elektroenergetycznymi. W chwili obecnej na polskim rynku energii działa 149 OSD[391].

Największymi podmiotami na polskim rynku energii są:

Grupa Kapitałowa Polska Grupa Energetyczna największy koncern energetyczny w Polsce[392]:

- produkuje 56,52 TWh energii elektrycznej,
- dostarcza energię elektryczną dla ok. 5,1 mln odbiorców,
- eksploatuje 274,7 tys. km linii energetycznych,

[391] *http://bip.ure.gov.pl/portal/bip/75/787/Operatorzy_systemow_elektroenergetycznych__dane_adresowe_i_obszary_dzialania.html* - [dostęp: 08.03.2019]

[392] *http://www.gkpge.pl/relacje-inwestorskie/grupa/kim-jestesmy* - [dostęp: 08.03.2019]

- moce zainstalowane jednostek wytwórczych Grupy PGE wynoszą 13,1 GW.

Grupa Kapitałowa ENERGA[393]:

- produkuje ponad 4,5 TWh energii elektrycznej,
- dostarcza energię elektryczną dla 2,5 mln gospodarstw domowych oraz do ponad 300 tys. firm,
- eksploatuje ponad 193 tys. km linii energetycznych,
- moce zainstalowane jednostek wytwórczych Grupy ENERGA wynoszą około 1,2 GW.

Grupa Kapitałowa TAURON[394]:

- produkuje 21,4 TWh energii elektrycznej,
- dostarcza energię elektryczna dla ponad 5,2 mln odbiorców,
- eksploatuje 223,7 tys. km linii elektroenergetycznych,
- moce zainstalowane jednostek wytwórczych Grupy TAURON wynoszą 5,6 GW,
- produkuje 4,58 mln ton węgla handlowego.

Grupa Kapitałowa ENEA[395]:

- dostarcza energię elektryczna dla 2,4 mln odbiorców,
- eksploatuje 129 tys. km linii elektroenergetycznych,
- moce zainstalowane jednostek wytwórczych Grupy ENEA wynoszą 3,2 GW.

[393] *http://www.energa.pl/dla-domu/grupa-energa/grupaenerga* - [dostęp: 08.03.2019]

[394] *http://www.tauron-pe.pl/tauron/grupa-tauron/Strony/o-grupie-tauron.aspx.* Natomiast dane o produkcji energii elektrycznej za: *raport roczny TAURON Polska Energia 2017 http://www.tauronpe.pl/tauron/o-tauronie/Documents/raport-roczny-tauron-2016.pdf* - [dostęp: 08.03.2019]

[395] *http://www.firma.enea.pl/47/grupa-enea/wszystko-o-enea/przedmiot-dzialalnosci-162.html* - [dostęp: 08.03.2019]

Mapa 4. **Zasięg działania największych podmiotów na rynku energii w Polsce**

Źródło: ARE S.A.

Głównym odbiorcą energii elektrycznej w Polsce są klienci kupujący energię na potrzeby prowadzonej przez siebie działalności gospodarczej. Gospodarstwa domowe, do których należą wszyscy klienci kupujący energię na cele komunalno-bytowe, stanowią 25% odbiorców.

Rysunek 1. **Podział energii kupowanej przez klientów na polskim rynku energii elektrycznej**

Źródło: ARE S.A.

Posiadane zasoby węgla kamiennego i brunatnego stanowią naturalne źródło energii pierwotnej. Dostępność tych zasobów oraz historycznie rozwinięty sektor ich wydobycia decydują o wysokim udziale tych paliw w produkcji energii elektrycznej w Polsce (stanowią jednocześnie o wysokiej niezależności energetycznej kraju). Ich wysoki udział w produkcji energii elektrycznej sprawia również, że sektor wydobycia węgla stanowi ważny element systemu zaopatrywania w energię elektryczną. Udział mocy zainstalowanej elektrowni i elektrociepłowni spalających węgiel wynosi ponad 85% mocy w Krajowym Systemie Elektroenergetycznym. Obok węgla swój udział w bilansie mają także gaz ziemny i energetyka odnawialna.

Tabela 5. **Struktura produkcji energii elektryczne w Polsce w 2016 roku**

Segment	Produkcja energii [GWh]
Produkcja w kraju ogółem	**163 153**
Węgiel kamienny	90 811
Węgiel brunatny	53 623
Gaz ziemny	4 355
Elektrownie przemysłowe	9 000
Elektrownie wodne	2 529
Elektrownie wiatrowe i inne odnawialne	2 833

Źródło: Sprawozdanie z działalności Prezesa Urzędu Regulacji Energetyki w 2016 roku.

Wykorzystywany w energetyce węgiel kamienny jest wydobywany metodą głębinową. Miejsca wydobycia znajdują się w województwach: małopolskim, śląskim i lubelskim.
Główne podmioty prowadzące działalność w sektorze wydobycia węgla kamiennego, to:

- Jastrzębska Spółka Węglowa S.A.,
- Katowicki Holding Węglowy S.A.,
- Kompania Węglowa S.A.,
- Lubelski Węgiel „Bogdanka" S.A.,
- Południowy Koncern Węglowy S.A.

Wydobycie węgla brunatnego w Polsce prowadzone jest głównie metodą odkrywkową. Miejscami jego wydobycia w Polsce są:

- Zagłębie Konińskie,

- Zagłębie Turoszowskie,
- Zagłębie Bełchatowskie,
- Sieniawa na Ziemi Lubuskiej.

Wydobycie węgla brunatnego prowadzone jest obecnie w czterech[396] kopalniach, przy czym trzy z nich są kopalniami wieloodkrywkowymi (Adamów, Bełchatów, Konin), a jedna (Turów) jest kopalnią jednoodkrywkową. Głównymi podmiotami prowadzącymi działalność w sektorze wydobycia węgla brunatnego są:

- PGE Górnictwo i Energetyka Konwencjonalna S.A.,
- PAK Kopalnia Węgla Brunatnego Adamów S.A.,
- AK Kopalnia Węgla Brunatnego Konin S.A.

6.1.3. Sektor gazu ziemnego – wydobycie i przesył

Sektor gazu ziemnego to dziedzina przemysłu grupująca podmioty wydobywające gaz ziemny oraz zajmujące się jego przesyłem, magazynowaniem i dostarczaniem do odbiorców końcowych. W Polsce gaz ziemny wydobywa się głównie na Podkarpaciu i Zapadlisku Przedkarpackim, a także w Wielkopolsce w rejonie Drezdenka i Międzychodu (w Polsce wydobywany jest głównie gaz zaazotowany (L)).

W gospodarce wykorzystywany jest głównie gaz wysokometanowy (E), stąd też większość tego surowca, bo około 75%, pochodzi z importu [397]. Głównym eksporterem jest Rosja, skąd przesyłany jest on do Polski:

- gazociągiem orenburskim, z południowej części Uralu,
- gazociągiem Zorza Polarna (z okolic Wuktyłu, przez Brześć do Warszawy),
- gazociągiem jamalskim (z Półwyspu Jamał w zachodniej Syberii).

W 2016 roku całkowite zużycie gazu ziemnego w Polsce wyniosło, według danych pozyskanych w toku przeprowadzonych przez Urząd Regulacji Energetyki cyklicznych badań monitorujących, 14 380,99 mln m^3. Dostawy gazu z zagranicy w ilości 10 915,28 mln m^3 uzupełniane były gazem pochodzącym ze źródeł krajowych w ilości 4 329,42 mln m^3, co

[396] Piąta Kopalnia Węgla Brunatnego „Sieniawa" Spółka z o.o. eksploatuje znikome ilości węgla na potrzeby lokalnych odbiorców. „Cała produkcja z Sieniawy dostarczana jest do lokalnych ciepłowni, kotłowni osiedlowych, indywidualnych odbiorców oraz do zakładów wykorzystujących węgiel brunatny do celów nieenergetycznych" – *„Kopalnia Sieniawa: ekonomiczna i ekologiczna" Węgiel Brunatny nr 3/60 z 2007 r.*

[397] W Polsce w regionie Wielkopolski wykorzystywany jest również gaz zaazotowany, wydobywany z krajowych źródeł, jednakże w bardzo znikomych ilościach.

stanowiło blisko 30% całkowitego zaopatrzenia kraju w gaz ziemny. Całkowite dostawy gazu z zagranicy w 2016 roku obejmowały import z kierunku wschodniego oraz dostawy wewnątrzwspólnotowe z Niemiec i Czech, przy czym istotną ich część stanowił import z kierunku wschodniego realizowany w ramach długoterminowego kontraktu zawartego w 1996 roku między Polskim Górnictwem Naftowym i Gazownictwem S.A. (dalej PGNiG SA) a OOO „Gazprom eksport". Na podstawie tego kontraktu zakupiono 9 335,54 mln m^3 gazu ziemnego, co stanowiło około 85% całkowitego importu tego surowca na terytorium Polski. Import ten uzupełniany był dostawami z Niemiec i Czech. Wielkość sumaryczna tych dostaw, realizowanych w ramach umów, wyniosła 1 579,74 mln m^3, co stanowiło około 14% całkowitego przywozu gazu na terytorium Polski[398].

Tabela 6. Struktura dostaw i wydobycia gazu w 2016 roku

Wyszczególnienie	Ilość [mln m^3]
Import, w tym	10 915,28
Kontrakt „jamalski"	9 335,54
Nabycie wewnątrzwspólnotowe/kraj pochodzenia	1 579,74
a) Niemcy	1 579,52
b) Czechy	0,22
Wydobycie własne	4 329,42
Magazyny gazu – zmiana stanu zapasów ***in minus***	-761,30
Zakup ze źródeł krajowych (dostawy do PGNiG SA od krajowych dostawców)	110,67
a) EWE Energia Sp. z o.o.	4,41
b) FX Energy Poland Sp. z o.o.	84,70
c) CalEnergy Resources Poland Sp. z o.o.	16,63
d) DPV Service Sp. z o.o.	0,34
e) inne (usługa magazynowania w sieci, rozliczenie z tytułu przekazania paliwa gazowego)	4,59

Źródło: Sprawozdanie z działalności Prezesa Urzędu Regulacji Energetyki w 2016 roku

[398] *Sprawozdanie z działalności Prezesa Urzędu Regulacji Energetyki w 2016* r.- [dostęp: 08.03.2019]

Tabela 7. Zużycie gazu w Polsce w 2016 roku

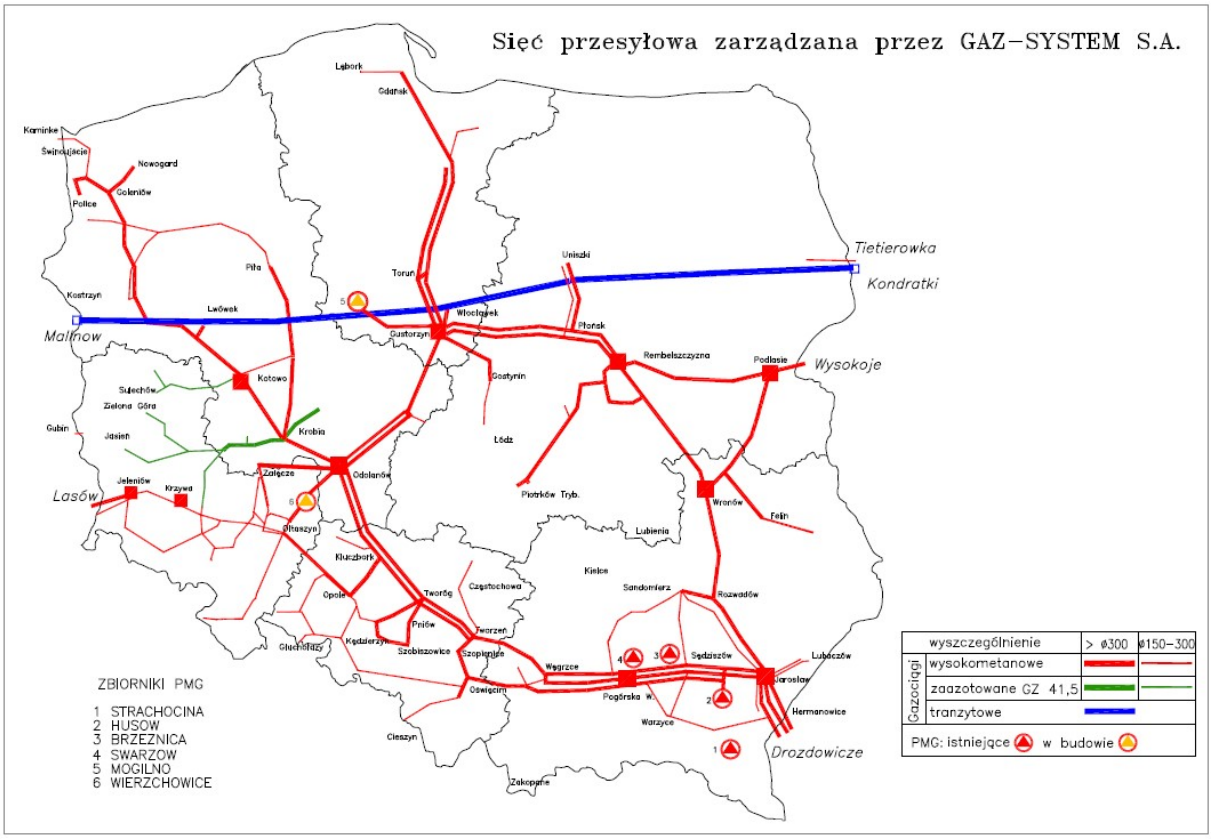
Wyszczególnienie	Gaz ziemny wysokometanowy [w hm^3]	Gaz ziemny zaazotowany [w hm^3]
krajowe	13 836	3 957
przetwarzanie na inne nośniki energii	1 484	2 874
zużycie bezpośrednie	12 352	1 083
w tym gospodarstwa domowe	3 590	259

Źródło: Rocznik Statystyczny Rzeczypospolitej Polskiej 2012.

Istotną rolę w bezpiecznym funkcjonowaniu systemu gazowego pełni operator systemu przesyłowego (OSP) gazu. OSP gazu to przedsiębiorstwo energetyczne zajmujące się przesyłaniem paliw gazowych odpowiedzialne za ruch sieciowy w systemie przesyłowym gazowym, bieżące i długookresowe bezpieczeństwo funkcjonowania tego systemu, eksploatację, konserwację, remonty oraz niezbędną rozbudowę sieci przesyłowej, w tym budowę połączeń z innymi systemami gazowymi. Do pełnienia roli OSP gazu na terenie Polski, decyzją Prezesa URE, został wyznaczony Operator Gazociągów Przesyłowych GAZ-SYSTEM S.A. Działalność OGP GAZ-SYSTEM S.A. obejmowała zarządzanie krajowym systemem przesyłowym, zgodnie z decyzją Prezesa URE z 13 października 2010 r., na mocy której spółka została wyznaczona operatorem systemu przesyłowego gazowego do 31 grudnia 2030 roku. Na jej podstawie spółka zarządzała sieciami wysokiego ciśnienia o łącznej długości 9 850 km. GAZ-SYSTEM S.A. od 17 listopada 2010 roku na okres do 31 grudnia 2025 roku pełni również rolę OSP na obszarze określonym w koncesji udzielonej przedsiębiorcy System Gazociągów Tranzytowych EuRoPol Gaz S.A.[399].

[399] Spółka akcyjna System Gazociągów Tranzytowych EuRoPol GAZ powstała 23 września 1993 r. System Gazociągów Tranzytowych [SGT] na terytorium Rzeczypospolitej Polskiej jest częścią mierzącego około 4000 km gazociągu biegnącego z Rosji przez Białoruś i Polskę do Europy Zachodniej (Jamał-Europa). Trasa gazociągu w kraju przebiega przez 5 województw (podlaskie, mazowieckie, kujawsko-pomorskie, wielkopolskie i lubuskie), 27 powiatów i 69 gmin.

Mapa 5. **Schemat sieci przesyłowej gazu ziemnego w Polsce**



Źródło: GAZ-SYSTEM S.A.

Operatorzy systemów dystrybucyjnych (OSD) gazu to przedsiębiorstwa energetyczne zajmujące się dystrybucją paliw gazowych, odpowiedzialne za ruch sieciowy w systemie dystrybucyjnym gazowym, bieżące i długookresowe bezpieczeństwo funkcjonowania tego systemu, eksploatację, konserwację, remonty oraz niezbędną rozbudowę sieci dystrybucyjnej, w tym połączeń z innymi systemami gazowymi. Zgodnie z decyzjami Prezesa URE na polskim rynku funkcjonuje 40 OSD gazu[400].

W Polsce występują znaczne sezonowe wahania w zapotrzebowaniu na gaz ziemny wysokometanowy. Sposobem na wyrównanie tych wahań oraz ewentualnych wahań w dostawach są magazyny gazu stanowiące jeden z najważniejszych elementów sektora gazu ziemnego. W Polsce aktualnie eksploatowanych jest jedenaście takich zbiorników. Operatorem systemu magazynowania paliw gazowych (OSM), zgodnie z decyzją Prezesa URE, jest Operator Systemu Magazynowania Sp. z o.o. Szczegółowe dane na temat ilości magazynowanego gazu

[400] http://bip.ure.gov.pl/portal/bip/76/786/Operatorzy_systemow_gazowych__dane_adresowy_i_obszary _dzialania.html

należą do informacji niejawnych, ostatnie publicznie dostępne dane pochodzą z kolei z roku 2011 –nie są one jednak niezbędne dla prowadzonego wywodu, stąd autor rezygnuje z ich przytoczenia.

6.1.4. Sektor ropy naftowej – wydobycie i przesył[401]

Sektor ropy naftowej to dziedzina przemysłu grupująca podmioty wydobywające oraz dostarczające i magazynujące ropę naftową, jak również zajmujące się jej przetwarzaniem oraz wytwarzaniem, dostarczaniem i magazynowaniem paliw płynnych.

Polski przemysł petrochemiczny zużywa rocznie ponad 24 mln ton ropy naftowej. Głównym źródłem dostaw surowca do przerobu jest import. Według danych GUS, w 2011 roku import ropy naftowej wyniósł 23 792 tys. ton. Ropa naftowa transportowana jest do Polski odcinkiem rurociągu „Przyjaźń"[402]. Eksploatacją sieci rurociągów służących do transportu ropy naftowej i paliw płynnych zajmuje się spółka Przedsiębiorstwo Eksploatacji Rurociągów Naftowych „Przyjaźń" S.A. Spółka dysponuje także pojemnościami zbiornikowymi, świadcząc usługi magazynowania ropy naftowej.

Infrastruktura PERN „Przyjaźń" S.A. do transportu ropy naftowej składa się z trzech zasadniczych odcinków rurociągów:

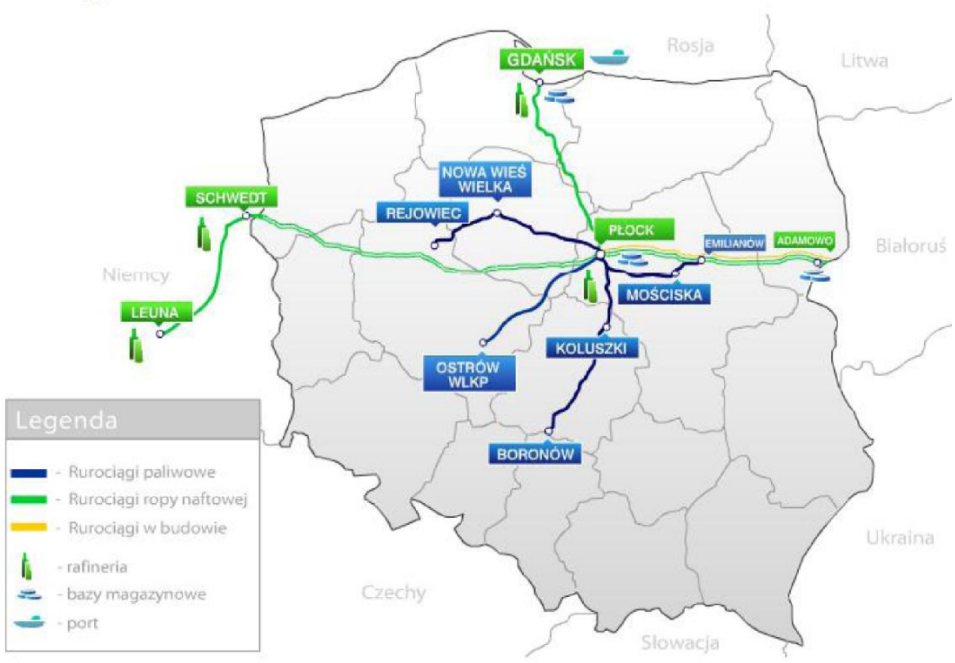
- Odcinek Wschodni rurociągu „Przyjaźń" – łączy Bazę Zbiornikową w Adamowie zlokalizowaną przy granicy z Białorusią z Bazą Surowcową w Płocku. Odcinek ten osiąga przepustowość 50 mln ton ropy naftowej rocznie.
- Odcinek Zachodni rurociągu „Przyjaźń" – łączy Bazę Surowcową w Płocku z bazą ropy naftowej zlokalizowaną w Schwedt. Tą częścią magistrali płynie surowiec dla dwóch niemieckich rafinerii: PCK Raffinerie GmbH Schwedt oraz TOTAL Raffinerie Mitteldeutschland GmbH w Spergau. Odcinek Zachodni rurociągu „Przyjaźń" osiąga wydajność 27 mln ton ropy naftowej rocznie.
- Rurociąg Pomorski – łączy Bazę Surowcową w Płocku z Bazą Manipulacyjną w Gdańsku. Tędy płynie rosyjska ropa naftowa przeznaczona dla rafinerii w Gdańsku należącej do Grupy LOTOS S.A. oraz na eksport przez Naftoport. Rurociągiem Pomorskim można transportować surowiec w dwóch kierunkach. Na trasie Gdańsk-Płock

[401] Wszystkie dane i statystyki dotyczące przemysłu naftowego pochodzą z lat 2011-2012.
[402] System rurociągów dalekosiężnych „Przyjaźń" to system łączący syberyjskie złoża ropy naftowej z Europą. Informacje o infrastrukturze PERN „Przyjaźń" S.A. za *http://www.pern.com.pl/?q=node/45* [dostęp: 08.03.2019]

jego przepustowość wynosi około 30 mln ton ropy naftowej rocznie, zaś w przeciwnym kierunku rurociąg osiąga wydajność około 27 mln ton na rok.

W 2011 roku w użytkowaniu było 2 444 km rurociągów magistralnych do przetłaczania ropy naftowej i produktów naftowych.

Mapa 6. **Schemat rurociągów ropy naftowej w Polsce**



Źródło: PERN S.A.

Obecnie w użytkowaniu są następujące rurociągi paliw płynnych:[403]

- Płock – Nowa Wieś Wielka – Rejowiec (kierunek: Bydgoszcz – Poznań). Na trasie z Płocka do Nowej Wsi Wielkiej można transportować rocznie 2,1 mln ton paliw.
- Płock – Mościska – Emilianów (kierunek: Warszawa). Rurociągiem tym można transportować 1 mln ton paliw rocznie.
- Płock – Koluszki – Boronów (kierunek: Łódź – Częstochowa). Płock – Koluszki osiąga on roczną przepustowość 3,8 mln ton paliw, zaś jego przedłużenie z Koluszek do Boronowa 1 mln ton paliw rocznie.
- Płock – Ostrów Wielkopolski oraz 40-kilometrowy rurociąg będący odgałęzieniem Odcinka Zachodniego, a którym doprowadzany jest surowiec do podziemnych

[403] *http://www.pern.com.pl/?q=node/59* - [dostęp: 08.03.2019]

magazynów w Inowrocławskich Kopalniach Soli SOLINO S.A. oraz rurociąg produktowy łączący kawerny po wyrobiskach solnych z rurociągiem PERN „Przyjaźń" S.A., który biegnie z Płocka do Nowej Wsi Wielkiej.

Drugą drogą importu ropy naftowej jest droga morska. Największym w Polsce operatorem przeładunków importowanej lub eksportowanej drogą morską ropy naftowej jest Przedsiębiorstwo Przeładunku Paliw Płynnych „Naftoport" Sp. z o.o. Infrastruktura terminalu Naftoportu obejmuje cztery stanowiska przeładunkowe (piąte – w budowie) o potencjale przekraczającym 40 mln ton paliw płynnych rocznie. W roku 2012 na terenie Bazy Paliw Naftoportu obsłużono ponad 220 zbiornikowców, w tym ponad 70 jednostek o tonażu przekraczającym 80 tys. ton i ponad 40 – z ładunkiem 15-80 tys. ton. Przeładowano 10,3 mln ton paliw płynnych, z czego 74% stanowiła ropa naftowa, reszta – to przeładunki produktów naftowych[19].

Przerób importowanej oraz wydobytej ropy naftowej dokonywany jest w rafineriach należących do dwóch wiodących podmiotów: Polskiego Koncernu Naftowego „Orlen" S.A. oraz Grupy LOTOS S.A.

Tabela 8. Przerób naftowej w Polsce w 2011 roku

Wielkość przerobu ropy naftowej w polskich rafineriach[20] w 2011 r. [tys. ton]	
Rafineria w Płocku	14 547
Rafineria w Gdańsku	9 170
Rafineria w Trzebini	234
Rafineria w Jedliczu	55
Razem	24 033

Źródło: Sprawozdanie zarządu z działalności Grupy Kapitałowej Lotos za 2011 r. oraz Orlen w liczbach 2011.

Istotnym ogniwem systemu logistycznego sektora naftowego w Polsce są bazy magazynowe ropy naftowej i paliw. Zbiorniki ropy naftowej są uzupełnieniem infrastruktury rurociągowej – spełniają one funkcje stabilizatora przepływu surowca. Oprócz spełnianych funkcji technologicznych wykorzystywane są one również do magazynowania surowca. PERN „Przyjaźń" S.A. posiada trzy bazy naftowe, w których w sumie może zmagazynować niemal 3 mln m^3 ropy naftowej. Największa z nich zlokalizowana jest pod Płockiem. Dwie pozostałe mieszczą się w Adamowie przy granicy z Białorusią oraz Gdańsku, w pobliżu Naftoportu.

Największym w Polsce przedsiębiorstwem specjalizującym się w magazynowaniu i przeładunku paliw płynnych jest Operator Logistyczny Paliw Płynnych (OLPP) Sp. z o.o. OLPP

Sp. z o.o. posiada dwadzieścia Baz Paliw, w których przechowywana jest benzyna, olej napędowy, lekki olej opałowy oraz paliwo lotnicze. Ich łączna pojemność to 1,8 mln m^3. Pięć największych Baz: w Koluszkach, Nowej Wsi Wielkiej, Boronowie, Rejowcu Poznańskim i Emilianowie znajduje się na końcówkach dalekosiężnych rurociągów paliwowych. Cztery Bazy zlokalizowane przy wschodniej granicy naszego kraju posiadają terminale przeładunkowe z torów szerokich na znormalizowane, które pozwalają na przeładunek rocznie 2,7 mln ton paliw i gazu. Z kolei dzięki Bazie w Dębogórzu i terminalowi morskiemu możliwe jest sprowadzenie do Polski lub wysłanie 1,2 mln ton paliw rocznie[404].

6.1.5. Sektor energii cieplnej

Sektor energii cieplnej to dziedzina przemysłu grupująca podmioty wytwarzające energię cieplną i operatorów cieplnych sieci dystrybucyjnych. Zgodnie z obowiązującym prawem energetycznym, działalność w zakresie:

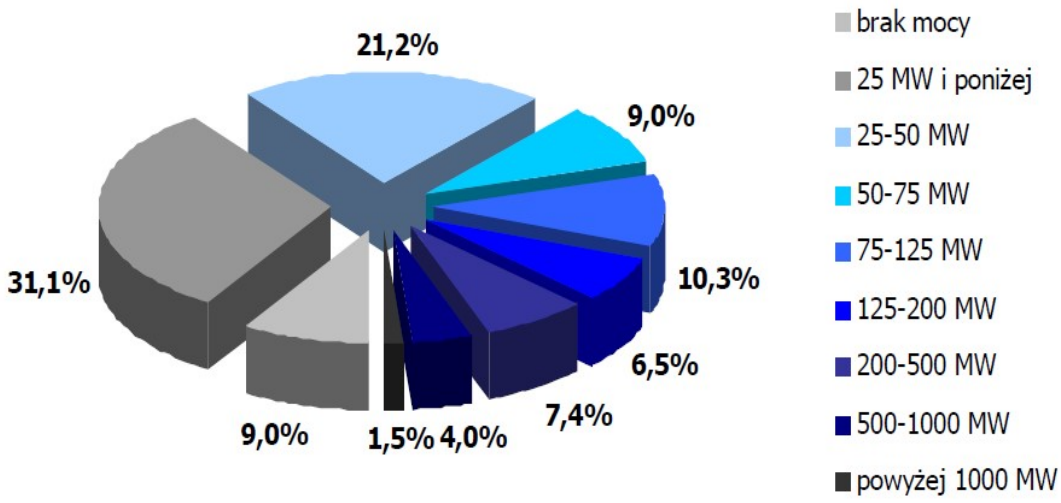
- wytwarzania ciepła w źródłach o mocy powyżej 5 MWt,
- przesyłania i dystrybucji ciepła, jeżeli moc zamówiona przez odbiorców przekracza 5 MWt,

podlega koncesjonowaniu przez Prezesa Urzędu Regulacji Energetyki. W 2016 roku na regulowanym rynku ciepła funkcjonowało 512 przedsiębiorstw posiadających koncesje Prezesa URE na działalność związaną z zaopatrzeniem w ciepło. Całkowita moc cieplna zainstalowana u koncesjonowanych wytwórców ciepła i w przedsiębiorstwach ciepłowniczych w Polsce wynosi prawie 60 tys. MW, na co składają się:

- elektrownie i elektrociepłownie zawodowe,
- elektrociepłownie i ciepłownie niezawodowe,
- przedsiębiorstwa produkcyjno-dystrybucyjne i ciepłownie zawodowe.

[404] *http://www.olpp.pl/uslugi* - [dostęp: 08.03.2019]

Rysunek 2. Struktura przedsiębiorstw ciepłowniczych mocy zainstalowanej w źródłach ciepła w 2016 roku

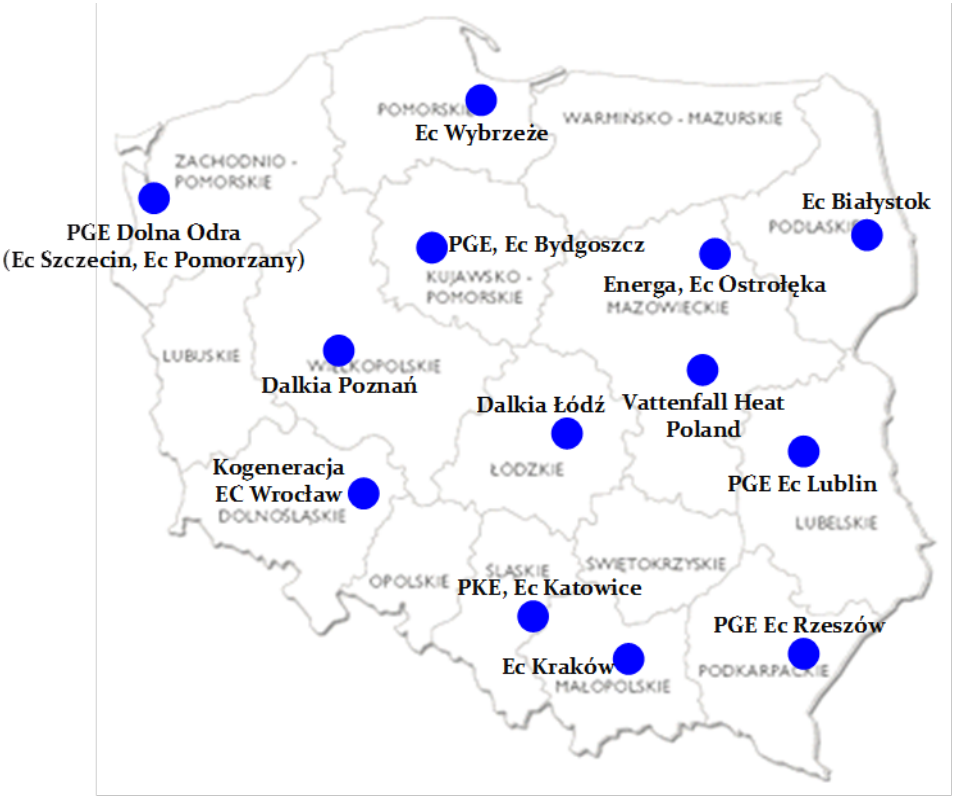


Źródło: Urząd Regulacji Energetyki.

Koncesjonowane przedsiębiorstwa ciepłownicze dysponują sieciami ciepłowniczymi o długości przekraczającej 19,5 tys. km. Scentralizowane systemy ciepłownicze funkcjonują we wszystkich większych miastach w Polsce. W dużych aglomeracjach miejskich, takich jak: Warszawa, Kraków, Łódź, Poznań, Trójmiasto dostawy ciepła i energii elektrycznej są realizowane z lokalnych elektrociepłowni zawodowych, które pokrywają całość lub większość zapotrzebowania na ciepło w ciągu roku oraz mają znaczący udział w pokryciu średniorocznego zapotrzebowania na energię elektryczną.

Podstawowym paliwem wykorzystywanym do produkcji ciepła jest węgiel kamienny, którego udział w produkcji ciepła stanowi 74,1%. Obok węgla swój udział mają olej opałowy, gaz ziemny i energetyka odnawialna.

Mapa 7. **Największe elektrociepłownie zawodowe w Polsce**



Źródło: Urząd Regulacji Energetyki.

6.2. System łączności[405]

Systemy łączności zapewniają przekazywanie informacji i obejmują pocztę oraz telekomunikację, jak również radiofonię i telewizję.

Przez telekomunikację rozumie się nadawanie, odbiór lub transmisję informacji, niezależnie od ich rodzaju, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną. Łączność ma decydujące znaczenie w gospodarce dla procesów biznesowych, zarządzania czy w relacjach administracja-obywatel obywatel-administracja, a także między samymi obywatelami. Współcześnie trudno sobie wyobrazić społeczeństwo informacyjne bez skutecznego przekazu informacji.

Wartość polskiego rynku usług telekomunikacyjnych mierzona wielkością przychodów ze sprzedaży usług trzech głównych segmentów (telefonii stacjonarnej, telefonii ruchomej i dostępu do Internetu) w 2011 roku wyniosła ponad 40 mld zł (wraz z transmisją danych i poczty

[405] Wszystkie dane w podrozdziale 2.2.2. podane za : http://www.stat.gov.pl/cps/rde/xbcr/gus, podają stan na koniec roku 2011. [dostęp: 08.03.2019]

elektronicznej). Do rejestru przedsiębiorców telekomunikacyjnych wpisanych było ponad 6,5 tys. podmiotów gospodarczych. Zdecydowana większość z nich faktycznie prowadziła działalność gospodarczą w dziedzinie telekomunikacji.

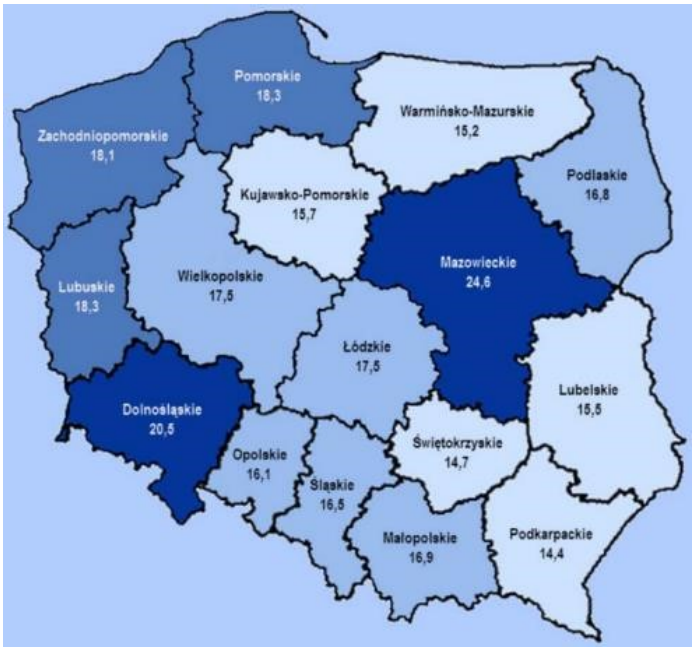
6.2.1. Łączność telefoniczna

Łączność telefoniczna jest powszechnie rozpowszechnioną formą komunikacji między abonentami. W 2011 roku wykonano w obrocie krajowym około 3275 mln połączeń telefonicznych wychodzących. Ze względu na umiejscowienie urządzeń abonenckich w przestrzeni można podzielić na telefonię stacjonarną i telefonię ruchomą.

- Telefonia stacjonarna

Usługi w zakresie telefonii stacjonarnej świadczyło w 2011 roku 115 operatorów, którzy prowadzili usługi w ramach połączeń lokalnych, międzystrefowych i międzynarodowych. Liczba telefonicznych łączy głównych sieci publicznej (tj. standardowych łączy głównych powiększonych o liczbę łączy w dostępach ISDN) według stanu na dzień 31 grudnia 2011 roku wyniosła około 6,9 mln – na 1000 mieszkańców przypadało średnio 181 łączy (w miastach – 239,7, a na wsi – 90).

Mapa 8. **Telefoniczne łącza główne przypadające na 100 mieszkańców (stan na 31 XII 2011 r.)**



Źródło: Główny Urząd Statystyczny.

- Telefonia mobilna – komórkowa

W sektorze telefonii komórkowej na polskim rynku konkurują sieci:

a) T-Mobile (operator: Polska Telefonia Cyfrowa S.A.) – liczba użytkowników 14,141 mln,
b) Orange Polska (operator: PTK Centertel Sp. z o.o.) – liczba użytkowników 16,658 mln,
c) Play (operator: P4 Sp. z o.o.) – liczba użytkowników 7,08 mln,
d) Plus (operator: Polkomtel S.A.) –liczba użytkowników 13,993 mln.

Na koniec 2011 roku na krajowym rynku telefonii ruchomej działalność prowadziło 23 przedsiębiorców telekomunikacyjnych (operatorzy udostępniają zarówno telefony na abonament, jak i w systemie przedpłaconym *pre-paid*). Liczba abonentów (łącznie z użytkownikami) telefonii ruchomej wynosiła 50,7 mln i była o 6,8% większa niż w końcu 2010 roku. Na 100 mieszkańców przypadało 132,7 abonentów (w 2010 r. – 124,3). Trendem zaczyna być zatem posiadanie więcej niż jednego aktywnego numeru na użytkownika.

6.2.2. Transmisja programów radiofonicznych i telewizyjnych

Usługi oferowane na tym rynku obejmują cyfrową transmisję treści radiofonicznych i telewizyjnych z wykorzystaniem naziemnej infrastruktury sieciowej.

W ramach usługi transmisji programów realizowane są:

- emisja sygnałów z obiektów nadawczych przedsiębiorców telekomunikacyjnych do odbiorców końcowych programów radiowych i telewizyjnych;
- dosył sygnałów – transmisja przeznaczonych do emisji programów ze studiów radiowych i telewizyjnych (umiejscowionych zazwyczaj w większych aglomeracjach) do obiektów nadawczych rozlokowanych na terenie całego kraju;
- usługi do celów kontrybucyjnych – dostarczanie do studia sygnałów radiowych lub wizyjnych z wozów transmisyjnych i stałych obiektów do studiów radiowych i telewizyjnych w celu ich montażu w gotowe programy – są to usługi świadczone producentom programów.

Klienci tworzący stronę popytową rynku to dwa rodzaje podmiotów. Pierwszy z nich to nadawcy radiofoniczni i telewizyjni zainteresowani, aby ich oferta programowa docierała do użytkowników końcowych za pośrednictwem naziemnych sieci transmisyjnych. Muszą oni korzystać z usług naziemnych sieci transmisyjnych. Drugi rodzaj to operatorzy sieci transmisyjnej.

6.2.3. Radiofonia[406] i telewizja[407]

Na polskim rynku radiowym i telewizyjnym funkcjonują obok siebie zarówno nadawcy publiczni, jak i prywatni (koncesjonowani).

- Radiofonia publiczna
  - **a)** Polskie Radio S.A. –nadaje cztery programy ogólnokrajowe (Program 1, Program 2, Program 3 i Program 4) oraz program skierowany do słuchaczy za granicą (Polskie Radio dla Zagranicy).
  - **b)** Rozgłośnie regionalne radia publicznego – w 2010 roku program nadawało 17 rozgłośni regionalnych radia publicznego. Pięć spośród nich, oprócz programu regionalnego, rozpowszechniało sześć programów miejskich: w Koszalinie (Radio Słupsk), w Poznaniu (MC Radio), w Szczecinie (Radio Szczecin FM), we Wrocławiu (Radio RAM) i w Zielonej Górze (dwa programy: Radio Zielona Góra i Radio Miejskie Gorzowa 95,6 FM).
  - **c)** Program lokalny dla mniejszości ukraińskiej przygotowywany i nadawany przez Radio Olsztyn S.A.
- Telewizja publiczna

W III kwartale 2012 roku do sektora publicznego łącznie (TVP1, TVP2, TV Polonia, TVP INFO, TVP Kultura, TVP Seriale, TVP Sport, TVP HD, TVP Historia) należało 33,9%. Było to mniej o 0,8 punktu procentowego niż rok temu. Z analizy danych wynika, że tempo spadku udziałów telewizji publicznej ogółem było mniejsze niż w I i II kwartale roku, przede wszystkim dzięki mniejszym spadkom programów ogólnopolskich. Podobnie jak w I i II kwartale 2012 roku zyskiwały publiczne programy tematyczne. Spośród nich największe udziały w widowni odnotowały programy: TVP Seriale (0,8%) i TVP Sport (0,4%).

6.2.4. Telewizja kablowa

Polska jest trzecim co do wielkości rynkiem telewizji kablowych w Europie i bez wątpienia najbardziej dynamicznym, a działa na nim ponad 600 operatorów sieci kablowych. Rynek został zdominowany przez kilku największych operatorów: UPC Polska, Vectra, Multimedia Polska, Aster City Cable, TOYA, które łącznie obejmują ponad 50% rynku. Oprócz

[406] *http://www.krrit.gov.pl/Data/Files/_public/Portals/0/kontrola/program/radio/kwartalne/rynek_3_kw12.pdf* -[dostęp: 08.03.2019]
[407] *http://www.krrit.gov.pl/Data/Files/_public/Portals/0/publikacje/analizy/rynek-tv-iii-kw2012.pdf* -[dostęp: 08.03.2019]

rozprowadzania programów telewizyjnych i radiowych (w tym programów płatnych), operatorzy kablowi działający w Polsce świadczą usługi dostępu do Internetu, telewizji cyfrowej oraz usługi telefoniczne. W 2011 roku w Polsce było 4 915 225 abonamentów telewizji kablowej.

6.2.5. Szerokopasmowy dostęp do Internetu[408]

Na koniec 2011 roku z dostępu do Internetu korzystało ponad 10 mln użytkowników, blisko o 12% więcej niż w roku 2010. Przełożyło się to na penetrację na poziomie 74,4% w odniesieniu do gospodarstw domowych oraz 26% w przeliczeniu na 100 mieszkańców Polski. Obecnie – grudzień 2018 – wskaźniki te sięgają odpowiednio 91,5 % oraz 41%. Usługi dostępu do Internetu realizowane są przede wszystkim przez modemy 3G, LTE, łącza xDSL, modemy kablowe operatorów TVK, przewodowe sieci LAN-Ethernet oraz bezprzewodowe WLAN.

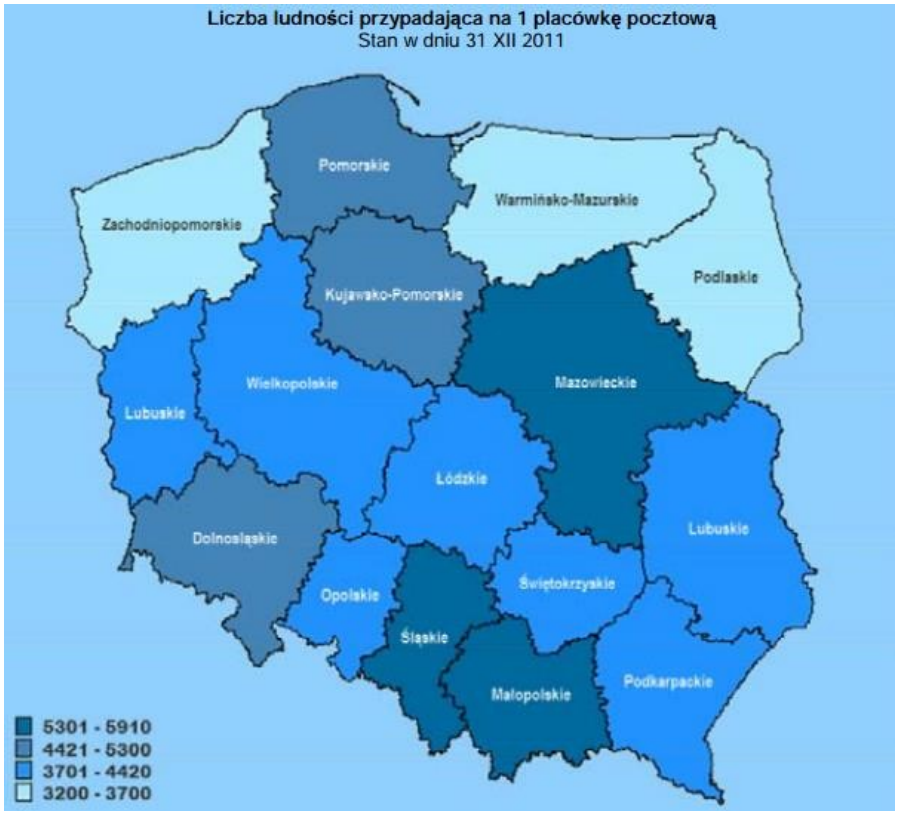
6.2.6. Łączność pocztowa[409]

Polski rynek pocztowy od kilku lat funkcjonuje w warunkach stopniowej liberalizacji. Z jednej strony zmniejsza się obszar usług zastrzeżonych dla operatora publicznego, a z drugiej systematycznie zwiększa się liczba podmiotów, które prowadzą działalność w zakresie świadczenia usług pocztowych. W 2011 roku, poza Pocztą Polską, do rejestru operatorów pocztowych były wpisane 154 podmioty (wg stanu na koniec 2011 r.). Jednak nie wszyscy operatorzy, którzy uzyskali wpis, faktycznie prowadzą działalność.

W 2011 roku zaobserwowano, podobnie jak w latach poprzednich, zmniejszenie się wielkości podstawowych usług pocztowych świadczonych przez operatora publicznego, z wyjątkiem przesyłek listowych poleconych nadanych (wzrost o 4,4%) i liczby przekazów pocztowych zrealizowanych (wzrost o 14,9%). W porównaniu z rokiem 2010 zmniejszyła się liczba paczek nadanych o 2,8%, wpłat na rachunki bankowe – o 10,9%, a także przesyłek listowych zwykłych nadanych – o 11,4%.

[408] *http://www.uke.gov.pl/_gAllery/56/31/56314/Raport_o_stanie_rynku_telekomunikacyjnego_za_2011_zm02.pdf* -[dostęp: 08.03.2019]
[409] *http://www.stat.gov.pl/cps/rde/xbcr/gus/tl_lacznosc_wyniki_dzialalnosci_2011.pdf* - [dostęp: 08.03.2019]

Mapa 9. **Liczba mieszkańców przypadająca na 1 placówkę pocztową (stan na 31 XII 2011 r.)**



Źródło: http://www.krrit.gov.pl

6.2.7. System sieci teleinformatycznych

Zgodnie z definicją zawartą w *Ustawie z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.)* system teleinformatyczny to „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego".
Z kolei pod pojęciem 'sieć telekomunikacyjna', zgodnie z definicją zawartą w art. 2 pkt 35 *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)*, należy rozumieć „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju".

Operacyjna zdolność systemów teleinformatycznych rozumianych zatem jako zespół urządzeń i oprogramowania, zdolnych do współpracy w celu przetwarzania zgromadzonych

danych, osiągana jest dopiero wówczas, gdy urządzenia te połączone zostaną za pomocą sieci telekomunikacyjnej. Ich rola polega na przekazywaniu informacji, zapewniając efektywną realizację dwóch pozostałych cech systemów teleinformatycznych, a mianowicie wysyłanie i odbieranie danych.

Organy administracji publicznej do wykonywania swoich ustawowych obowiązków wykorzystują:

- systemy teleinformatyczne dedykowane do przetwarzania i gromadzenia różnorodnych danych,
- wydzielone fizycznie lub logicznie będące własnością organów administracji publicznej lub też dzierżawione od operatorów sieci telekomunikacyjnych sieci telekomunikacyjne. Administracja publiczna korzysta w tym względzie z usług dzierżawy sieci przedsiębiorstw telekomunikacyjnych.

Ogół istniejących i eksploatowanych przez administrację publiczną systemów teleinformatycznych połączonych wewnętrznie za pomocą sieci telekomunikacyjnych został ujęty w ustawie o zarządzaniu kryzysowym pod pojęciem systemów sieci teleinformatycznych stanowiących jeden ze składników infrastruktury krytycznej państwa

6.3. System finansowy

System finansowy to ogół norm prawnych oraz zespół instytucji finansowych, których zadaniem jest gromadzenie, dzielenie i wydatkowanie zasobów pieniężnych państwa. Sprawnie funkcjonujący system finansowy ma decydujące znaczenie dla sprawnego funkcjonowania państwa i społeczeństwa. Organem administracji publicznej sprawującym państwowy nadzór nad rynkiem finansowym w Polsce jest Komisja Nadzoru Finansowego[410] (KNF).

6.3.1. Struktura systemu finansowego

System finansowy składa się z kilku segmentów:

a) budżetowego – na który składa się ogół norm prawnych oraz struktur organizacyjnych regulujących funkcjonowanie budżetu państwa i jednostek samorządu terytorialnego.

[410] KNF sprawuje nadzór nad sektorem bankowym, rynkiem kapitałowym, ubezpieczeniowym i emerytalnym oraz nad instytucjami pieniądza elektronicznego. Celem nadzoru nad rynkiem finansowym jest zapewnienie prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnienie ochrony interesów uczestników tego rynku. Nadzór nad działalnością KNF sprawuje Prezes Rady Ministrów. W związku z występowaniem różnych podziałów systemu finansowego skupiono się na segmentach mających potencjalnie największy wpływ na funkcjonowanie systemu w wypadku powstania zakłóceń.

Z budżetu państwa finansowane są wszystkie działania mające na celu wypełnienie ustawowych obowiązków państwa wobec obywatela;

b) bankowego – który stanowi ogół norm prawnych regulujących zady prowadzenia działalności bankowej, tworzenia i organizacji banków, oddziałów i przedstawicielstw banków zagranicznych, a także oddziałów instytucji kredytowych oraz norm ostrożnościowych ustalanych przez Komisję Nadzoru Finansowego. Zasadniczą rolę w podsystemie bankowym odgrywa bank centralny Rzeczypospolitej Polskiej – Narodowy Bank Polski (NBP). NBP pełni trzy podstawowe funkcje:

- banku emisyjnego – NBP ma wyłączne prawo emitowania znaków pieniężnych będących prawnym środkiem płatniczym w Polsce. Narodowy Bank Polski określa wielkość ich emisji oraz moment wprowadzenia do obiegu, za którego płynność odpowiada. Ponadto organizuje obieg pieniężny i reguluje ilość pieniądza w obiegu;
- „banku banków" – NBP pełni w stosunku do banków funkcje regulacyjne, które mają na celu zapewnienie sprawnego i efektywnego systemu płatniczego oraz stabilności sektora bankowego. Organizuje system rozliczeń pieniężnych, prowadzi bieżące rozrachunki międzybankowe i aktywnie uczestniczy w międzybankowym rynku pieniężnym. NBP jest odpowiedzialny za stabilność i bezpieczeństwo całego systemu bankowego, ponadto nadzoruje systemy płatności w Polsce;
- centralnego banku państwa – NBP prowadzi obsługę bankową budżetu państwa, prowadzi rachunki bankowe rządu i centralnych instytucji państwowych, państwowych funduszy celowych i państwowych jednostek budżetowych oraz realizuje ich zlecenia płatnicze;

c) ubezpieczeniowego – reguluje tworzenie, podział i organizację rynku ubezpieczeniowego. Ubezpieczenia dzielą się na dwie kategorie:

- ubezpieczenia społeczne – mają na celu prewencyjną i ubezpieczeniową ochronę zdrowia, zdolności do wykonywania pracy oraz życia ludności, są przymusowe i powszechne. Najistotniejszymi ogniwami podsystemu ubezpieczeń społecznych są:

  - Zakład Ubezpieczeń Społecznych (ZUS). ZUS to państwowa instytucja publicznoprawna realizująca zadania z zakresu ubezpieczeń społecznych w Polsce. Obecnie z usług ZUS korzysta około 25 mln klientów. Środki Funduszu

Ubezpieczeń Społecznych, których dysponentem jest ZUS, stanowią blisko 60% zasobów pieniężnych państwa;

- Otwarte Fundusze Emerytalne (OFE) – osoby prawne, których przedmiotem działalności jest gromadzenie środków pieniężnych, ich lokowanie, z przeznaczeniem na wypłatę członkom funduszu po osiągnięciu przez nich wieku emerytalnego i wypłata okresowych emerytur kapitałowych. OFE są zarządzane i reprezentowane przez Powszechne Towarzystwa Emerytalne[411] (PTE);

- Kasa Rolniczego Ubezpieczenia Społecznego (KRUS) – instytucja powołana do realizacji zadań związanych z pełną obsługą ubezpieczenia społecznego rolników. Kasa prowadzi działalność prewencyjną, rehabilitację leczniczą i wydzielone orzecznictwo lekarskie, zasiłki rodzinne, pielęgnacyjne, świadczenia kombatanckie dla inwalidów wojennych, pełni funkcję płatnika składek na ubezpieczenie zdrowotne;

- ubezpieczenia na życie, osobowe i majątkowe – ten rodzaj działalności ubezpieczeniowej wykonują zakłady ubezpieczeń w oparciu o zezwolenia organu nadzoru. Zakład ubezpieczeń może wykonywać działalność ubezpieczeniową wyłącznie w formie spółki akcyjnej albo towarzystwa ubezpieczeń wzajemnych;

- ubezpieczenie emerytalno-rentowe, finansowane w przeważającej części z dotacji budżetowej, uzupełnionej dochodami ze składek ubezpieczonych rolników;
- ubezpieczenie wypadkowe, chorobowe i macierzyńskie – realizację świadczeń z tego ubezpieczenia gwarantują jedynie składki od rolników gromadzone w Funduszu Składkowym Ubezpieczenia Społecznego Rolników. Fundusz ten jest osobą prawną, funkcje zarządu pełni z urzędu Prezes KRUS, pod nadzorem Rady Rolników;

d) kapitałowego – gdzie dokonywany jest obrót średnio i długoterminowych instrumentów finansowych (np. akcje i obligacje). Obrót dokonuje się głównie na Giełdzie Papierów Wartościowych (GPW). Giełda Papierów Wartościowych w Warszawie jest spółką akcyjną powołaną przez Skarb Państwa. Skarb Państwa posiada 35% udział w kapitale zakładowym Spółki, co stanowi 51,40% udział w

[411] Powszechne Towarzystwo Emerytalne to spółka akcyjna celowa, powołana do zarządzania Otwartym Funduszem Emerytalnym.

ogólnej liczbie głosów akcjonariuszy. Skarb Państwa jest jedynym akcjonariuszem posiadającym powyżej 5% ogólnej liczby głosów.

Oprócz GPW istotnymi uczestnikami segmentu kapitałowego są:

- Krajowy Depozyt Papierów Wartościowych SA – centralna instytucja odpowiedzialna za prowadzenie i nadzorowanie systemu depozytowo-rozliczeniowego w zakresie obrotu instrumentami finansowymi w Polsce;
- BondSpot S.A.[412] – instytucja dysponująca licencją na prowadzenie rynku regulowanego pozagiełdowego oraz alternatywnego systemu obrotu i jednocześnie mogąca tworzyć inne platformy elektronicznego obrotu instrumentami finansowymi;
- domy i biura maklerskie – instytucje finansowe świadczące usługi maklerskie za pośrednictwem maklerów oraz doradców inwestycyjnych. Podstawową funkcją działalności maklerskiej jest pośrednictwo w obrocie maklerskimi instrumentami finansowymi;
- towarzystwa funduszy inwestycyjnych – instytucje finansowe działające w formie spółek akcyjnych (z siedzibą na terytorium RP, po uzyskaniu zgody KNF), których przedmiot działalności jest ograniczony wyłącznie do tworzenia i zarządzania funduszami inwestycyjnymi, reprezentowania ich wobec osób trzecich oraz zarządzania zbiorczym portfelem papierów wartościowych.

6.4. System zaopatrzenia w żywność

System zaopatrzenia w żywność to dziedzina gospodarki, na którą składa się wytworzenie środków produkcyjnych (np. nawozy, pasze) i usług dla rolnictwa, produkcja i pozyskiwanie surowców żywnościowych (w rolnictwie, rybactwie, leśnictwie, łowiectwie), skup surowców żywnościowych, ich przechowywanie i transport, przetwórstwo surowców żywnościowych, obrót towarowy produktami żywnościowymi (magazynowanie i przechowywanie żywności, handel hurtowy i detaliczny, eksport i import) oraz system bezpieczeństwa żywności obejmujący wszystkie składowe łańcucha zaopatrzenia w żywność.

System zaopatrzenia w żywność jest jednym z podstawowych filarów gospodarki narodowej, który ma bezpośrednio przełożenie na bezpieczeństwo ekonomiczne państwa. Celem

[412] Od maja 2009 r. wiodącym akcjonariuszem BondSpot S.A. jest właśnie GPW S.A., zwiększając swoje zaangażowanie kapitałowe w spółce do 92,47% udziałów w kapitale zakładowym. Pozostałe akcje należą do banków (3,56%), domów maklerskich (3,88%) oraz innych podmiotów (0,09%) w tym Skarbu Państwa, reprezentowanego przez Ministra Finansów.

strategicznym tego systemu jest zapewnienie wyżywienia narodu przez utrzymanie możliwości produkcyjnych gospodarki żywnościowej zapewniających bezpieczeństwo żywnościowe, bezpieczeństwo żywności i pasz.

Bezpieczeństwo żywnościowe jest jedną z podstawowych potrzeb społeczeństwa. Składa się na nie szereg czynników i jest to zagadnienie znacznie bardziej skomplikowane niż wyprodukowanie wystarczającego wolumenu żywności. Istotne są również: dostęp do pożywienia ubogiej ludności, systemy rolnictwa, polityka rolna, międzynarodowa polityka handlowa, koszty żywności, różnorodność i bezpieczeństwo żywności, łańcuchy żywnościowe, dystrybucja, walory żywieniowe i kwestie zdrowotności. Ważnym elementem bezpieczeństwa żywnościowego jest zapewnienie społeczeństwu dostępu do dostatecznej ilości żywności.

Bezpieczeństwo żywnościowe powinno być traktowane na równi z innymi strategicznymi funkcjami państwa, takimi jak zapewnienie bezpieczeństwa energetycznego, bezpieczeństwa środowiskowego, bezpieczeństwa zasobów wody, czego niezbędnym warunkiem jest utrzymanie produkcji rolnej na odpowiednim poziomie (również gotowość do prowadzenia produkcji przez utrzymanie gruntów w dobrej kulturze rolnej), a także tworzenie odpowiednich warunków do tej produkcji (przez mechanizmy wsparcia i inne instrumenty polityki rolnej).

6.4.1. Rolnictwo

Rolnictwo jest jednym z najważniejszych elementów systemu zaopatrzenia w żywność i w sposób oczywisty wpływa na bezpieczeństwo ekonomiczne kraju w wymiarze produkcyjnym (wielkość produkcji i przetwórstwa), co stanowi o możliwości zapewnienia bezpieczeństwa żywnościowego kraju oraz wsparcia Sił Zbrojnych. Celami rolnictwa w kontekście bezpieczeństwa żywnościowego są: utrzymanie i zwiększenie w przyszłości produktywności, zachowanie bazy produkcyjnej, czyli ziemi rolnej będącej w gotowości do produkcji oraz ograniczenie obciążenia dla środowiska. Duże znaczenie dla bezpieczeństwa żywnościowego ma polityka rolna. Rynki rolne charakteryzuje nieunikniona niestabilność. Spowodowana jest ona szeregiem czynników, z których najważniejsze to czynniki pogodowe oraz występowanie chorób i szkodników. W efekcie mają miejsce wahania wolumenu produkcji i cen, co z kolei stwarza dla rolników problem z dochodowością produkcji, w warunkach skrajnej niepewności rynkowej:

a) system zaopatrywania w żywności a bezpieczeństwo żywnościowe

Bezpieczeństwo żywnościowe, ze względu na swój ponadnarodowy charakter, jest celem zarówno krajowej, jak i wspólnotowej polityki rolnej. Najważniejszymi instrumentami mającymi wpływ na utrzymanie produkcji na użytkach rolnych są płatności bezpośrednie oraz wsparcie dla obszarów o niekorzystnych warunkach gospodarowania. Instrumenty krajowe usprawniają funkcjonowanie rynku ziemi między innymi przez stosowanie kredytów preferencyjnych na jej zakup.

Głównym elementem systemu zaopatrzenia w żywność jest produkcja i pozyskiwanie surowców żywnościowych. Obejmuje ona przede wszystkim sprawy dotyczące:

- produkcji roślinnej i ochrony roślin uprawnych,
- nasiennictwa, z wyłączeniem leśnego materiału rozmnożeniowego,
- produkcji zwierzęcej i hodowli zwierząt.

Produkcja i pozyskiwanie surowców żywnościowych to nie tylko produkcja żywności, lecz także kwestie związane z:

- ochroną zdrowia zwierząt, weterynaryjną ochroną zdrowia publicznego oraz ochroną zwierząt,
- nadzorem nad zdrowotną jakością środków spożywczych pochodzenia zwierzęcego w miejscach ich pozyskiwania, wytwarzania, przetwarzania i składowania,
- nadzorem nad obrotem produktami leczniczymi weterynaryjnymi i wyrobami medycznymi stosowanymi w weterynarii,
- nadzorem nad zdrowotną jakością pasz oraz sprawy organizmów genetycznie zmodyfikowanych przeznaczonych do użytku paszowego i pasz genetycznie zmodyfikowanych w zakresie niektórych zadań lub czynności określonych właściwymi przepisami.

Zasadniczym celem działania w tym obszarze powinno być utrzymanie produkcji rolnej, przetwórstwa i zdolności dystrybucji na poziomie zapewniającym zaopatrzenie społeczeństwa, w co najmniej podstawowe artykuły rolno-spożywcze (produkty mięsne, mleczarskie, zbożowe i cukier). Niezbędne jest stworzenie warunków do odtworzenia i utrzymania produkcji rolno-hodowlanej (roślinnej i zwierzęcej) w przypadku zdarzeń powodujących ograniczenie tej produkcji (katastrofy naturalne i przemysłowe, akty terroru, działania wojenne). Należy podkreślić, iż to produkcja rolna i sposób jej dystrybucji decyduje o właściwym (zapewnienie odpowiedniej kaloryczności i ilości składników pokarmowych) wyżywieniu ludności, a

stanowiąc podstawowe ogniwo produkcyjne w całym cyklu produkcyjnym, jest jednocześnie istotnym elementem gospodarki narodowej.

System zaopatrzenia w żywność obejmuje również zakres:

- przetwórstwa i przechowalnictwa rolno-spożywczego,
- jakości handlowej artykułów rolno-spożywczych,
- mechanizmów regulacji rynków rolnych.

Przemysł rolno-spożywczy ze względu na zatrudnienie, wielkość produkcji, wymianę handlową na rynku wewnętrznym Unii Europejskiej i na rynkach krajów trzecich stanowi istotny element gospodarki narodowej oraz składową bezpieczeństwa ekonomicznego. Produkcja tego przemysłu stanowi około 16% sprzedaży całego przemysłu, zaś zatrudnienie wynosi około 15% pracujących ogółem w przemyśle. Działalność w sektorze rolno-spożywczym oraz w tak zwanej pozarolniczej sferze działalności zawodowej i gospodarczej ze względu na procent, jaki stanowią obszary wiejskie (93,2% – dane GUS za rok 2017 r.), ma duże znaczenie gospodarcze. W sposób istotny wpływa ona na sytuację społeczno-ekonomiczną (np. zróżnicowanie dochodów ludności wiejskiej i pozarolniczej), stan środowiska przyrodniczego (np. poziom jego skażenia środkami chemicznymi) oraz różnorodność biologiczną kraju (odmienność i wielość ekosystemów).

b) Rynki żywnościowe

Ze względu na specyfikę zagadnienia bezpieczeństwo ekonomiczne na rynkach rolnych należy rozpatrywać w rozbiciu na poszczególne rynki:

- rynek zbóż,
- owoców i warzyw,
- cukru,
- rynek wołowiny i cielęciny,
- mięsa wieprzowego,
- drobiu,
- mleka,
- rynek alkoholu etylowego.

Na każdym z tych rynków mogą pojawiać się specyficzne zagrożenia, zaś bezpieczeństwo ekonomiczne w tym obszarze związane jest ściśle z unijnymi rynkami w ramach Wspólnej Polityki Rolnej. W kategoriach wewnętrznych obszar ten ściśle powiązany jest z rolnictwem.

Po wejściu Polski do struktur Unii Europejskiej istotnego znaczenia dla polskiego rolnictwa nabrała budowa nowoczesnej infrastruktury rynku rolnego, tj. rynków hurtowych, giełd, systemów informacji rynkowej (dot. szczególnie cen i rozmiarów obrotu).

Działalność rynków hurtowych została rozpoczęta w 1992 roku, kiedy została otwarta Wielkopolska Gildia Rolno-Ogrodnicza S.A. w Poznaniu. Następnie w wyniku realizacji programów rządowych budowy i rozwoju rynków hurtowych powstały kolejne: o charakterze ponadregionalnym zlokalizowane w Warszawie, Gdańsku, Wrocławiu i Lublinie oraz lokalne w Białymstoku, Elblągu, Legnicy, Radomiu, Rzeszowie, Tarnowie, Wałbrzychu oraz Zielonej Górze. Celem programów rządowych było stworzenie nowoczesnych, spełniających wysokie standardy miejsc handlu, które gwarantują, że obrót artykułami spożywczymi dokonywany jest w sposób bezpieczny dla konsumenta. Głównymi akcjonariuszami tych spółek jest Agencja Restrukturyzacji i Modernizacji Rolnictwa, Minister Skarbu Państwa, a ponadto samorządy, producenci rolni oraz indywidualni operatorzy – hurtownicy.

Równolegle do rynków hurtowych powstałych z inicjatywy rządu, funkcjonują rynki o kapitale prywatnym i samorządowym. Do największych należy zaliczyć rynki usytuowane w: Łodzi, Ząbkach k/Warszawy, Katowicach, Sandomierzu, Wrocławiu, Bielsku-Białej, Gorzowie Wielkopolskim i Tychach. Przedmiotem obrotu towarowego na rynkach hurtowych są przede wszystkim świeże owoce i warzywa, kwiaty, przetworzone produkty spożywcze, w tym produkty mleczarskie i zbożowe, mięso i jego przetwory, jaja, napoje, wyroby cukiernicze. Rynki hurtowe stanowią miejsce zaopatrzenia dla sklepów detalicznych, targowisk, punktów zbiorowego żywienia. Rynki hurtowe są znaczącym ogniwem dystrybucji artykułów rolno-spożywczych, przede wszystkim świeżych towarów, które cechuje wysoka jakość. Szacuje się, że udział rynków hurtowych w globalnej podaży na rynku owoców i warzyw wynosi 30-40%.

6.4.2. Rybołówstwo

Rybołówstwo jako część systemu zaopatrzenia w żywność obejmuje następujące zagadnienia:

- rybactwo śródlądowe i rybołówstwo morskie,
- racjonalne gospodarowanie żywymi zasobami morza,
- gospodarka rybna i organizacji rynku rybnego,

- organizacja producentów rybnych, związków organizacji producentów rybnych i organizacji międzybranżowych.

a) Strefa przybrzeżna Morza Bałtyckiego – obejmuje 36 gmin na terenie 18 powiatów w trzech województwach: pomorskim, zachodniopomorskim, a także częściowo warmińsko-mazurskim (część Zalewu Wiślanego). Długość polskiego wybrzeża wynosi 528 km. Na polskim wybrzeżu znajdują się 74 porty i przystanie rybackie. Powierzchnia morza terytorialnego wynosi 8 682 km^2. Morze Bałtyckie jest akwenem mało zasolonym, w którym średnie zasolenie zmniejsza się w miarę oddalania od cieśnin duńskich. Większość polskich rzek należy do zlewni Morza Bałtyckiego. W głównej mierze należą one do dorzecza Wisły i Odry (89,9%). Pozostałe to dorzecza uchodzących bezpośrednio do Morza Bałtyckiego rzek przepływających przez pojezierza: Pomorskie i Mazurskie (9,8%).

b) Powierzchnia wód śródlądowych w Polsce – (naturalnych i sztucznych, ale z wyłączeniem stawów) wynosi około 550 tys. ha, w tym około 300 tys. ha jezior, 139 tys. ha rzek i potoków, 55 tys. ha zbiorników zaporowych (o powierzchni powyżej 20 ha), 40 tys. ha zalewisk i starorzeczy. Większość tej powierzchni stanowi własność publiczną. System wodny w Polsce charakteryzuje się niewielką liczbą zbiorników zaporowych. Łączna pojemność 140 większych zbiorników wynosi około 2,8 km^3, stanowiąc zaledwie 5% objętości wody rocznie odpływającej z obszaru kraju. Większość zbiorników zaporowych znajduje się na południu kraju. Polska jest krajem o stosunkowo dużej liczbie jezior. Jezior większych niż 1 ha jest 7 081, a ich znaczna powierzchnia wynosi około 281 tys. ha, stanowiąc w przybliżeniu 1% obszaru kraju.

c) Porty morskie, przystanie i miejsca wyładunku – Polska posiada 74 wyznaczone porty, przystanie i miejsca wyładunku. Blisko połowa z nich to miejsca wyładunku położone na plażach. Zwykle są one niespecjalnie wyposażone i wymagają znaczących usprawnień i modernizacji. Spośród polskich portów jedenaście zostało wyznaczonych do wyładunku dorsza: Gdańsk, Władysławowo, Jastarnia, Hel, Łeba, Ustka, Darłowo, Mrzeżyno, Kołobrzeg, Dziwnów i Świnoujście. Korzystają z nich statki, na których pokładzie znajdują się dorsze w ilości większej niż 750 kg żywej wagi.

Dla statków rybackich szczególne znaczenie ma dziecięć portów rybackich. Są to:

- wybrzeże zachodnie: Świnoujście, Dziwnów,
- wybrzeże środkowe: Kołobrzeg, Darłowo, Ustka, Łeba,

- wybrzeże wschodnie: Władysławowo, Jastarnia, Hel, Gdynia.

Pięcioma najważniejszymi portami, jeżeli chodzi o ilość wyładowywanej ryby, ilość obsługiwanych kutrów rybackich i posiadającymi odpowiednie wyposażenie są: Kołobrzeg, Darłowo, Ustka, Władysławowo i Hel.

d) Chów i hodowla ryb – w Polsce chów i hodowla ryb obejmuje przede wszystkim gatunki ryb słodkowodnych. Chów i hodowla ryb morskich dotychczas nie była przedmiotem działalności komercyjnej prowadzonej na dużą skalę. Istnieją dwa główne typy działalności: produkcja słodkowodnych ryb ciepłolubnych (karp) oraz słodkowodnych ryb zimnolubnych (głównie pstrąg tęczowy). Z szacowanej powierzchni stawów wielkości 70 tys. ha eksploatowanych jest tylko 50 tys. (70%). Według danych z powszechnego spisu rolnego z 2002 roku ponad 10 000 gospodarstw deklarowało chów i hodowlę ryb jako jeden z rodzajów działalności rolniczej, przy czym nie była to ich główna dziedzina działalności. Gospodarstwa hodowlane zlokalizowane są w różnych regionach całego kraju. W większości przypadków ryby hodowane są w stawach, których ilość i rodzaj determinuje sposób i wielkość produkcji ryb. Około 600 gospodarstw prowadzi chów i hodowlę ryb w celu wprowadzenia ich na rynek, z czego 400 specjalizuje się w produkcji karpia. Pozostałe gospodarstwa prowadzą hodowlę pstrąga tęczowego. Wiele gospodarstw dążąc do dywersyfikacji działalności, prowadzi chów i hodowlę więcej niż jednego gatunku ryb (np. lina, tołpygi białej i pstrej, amura, jesiotra, pstrąga potokowego, pstrąga źródlanego, troci jeziorowej i wędrownej, łososia atlantyckiego). Co roku na rynek krajowy dostarczane jest około 31 tys. ton hodowlanych ryb słodkowodnych. W miarę opanowywania technologii produkcji zwiększa się liczba gatunków ryb produkowanych w specjalnych zbiornikach, w których woda znajduje się w obiegu zamkniętym. Dotyczy to głównie takich gatunków, jak sum afrykański czy barramundi.

e) Przetwórstwo produktów rybactwa – na koniec października 2012 roku w rejestrze Głównego Inspektoratu Weterynarii (GIW) znajdowało się 245 zakładów przetwórczych uprawnionych do handlu produktami rybnymi. Uprawnienia do eksportu do krajów trzecich posiadało 76 zakładów przetwórczych. Liczba zakładów dopuszczonych do sprzedaży bezpośredniej tylko na rynki lokalne wyniosła 482, z czego około 50 zajmuje się przetwórstwem.

f) Spożycie ryb – Polska należy do krajów o stosunkowo niskim spożyciu ryb. Ocenia się, że w 2015 roku spożycie ryb, przetworów rybnych i owoców morza wyniosło około 11,48 kg (w

przeliczeniu na masę żywej ryby). Jest to spadek o około 3,8% w stosunku do roku poprzedniego i o około 7% w stosunku do roku 2012. Wzrost spożycia odnotowano w przypadku łososia i szprota, natomiast w przypadku pozostałych gatunków nastąpił delikatny spadek konsumpcji. W strukturze spożycia dominują ryby morskie, z których kolejno najpopularniejsze są: mintaj, śledź, makrela, łosoś, dorsz, szprot oraz tuńczyk, a spośród ryb słodkowodnych najpopularniejsze gatunki to karp i pstrąg. Duże znaczenie ma także konsumpcja importowanych ryb słodkowodnych, takich jak panga i tilapia. W odróżnieniu od świątecznej sprzedaży karpi, sprzedaż pstrągów tęczowych nie ma charakteru sezonowego. Zgodnie z oczekiwaniami konsumentów coraz większe znaczenie w wynikach sprzedaży mają produkty przetworzone o dużej wartości dodanej. Roczna produkcja pstrąga tęczowego oscyluje w granicach 13,2 tys. ton i są przesłanki, aby sądzić, że istnieje potencjał dla dalszego rozwoju produkcji i rynku.

g) Eksport i import ryb – polski sektor rybacki stanowi 0,07% PKB, jednak ma ogromny wpływ na życie społeczno-gospodarcze trzech nadmorskich województw. Udział produktów rybnych w eksporcie stanowi 10% całego eksportu żywności. Szacuje się, że w 2012 roku import wyniósł 442,4 tys. ton, a wielkość eksportu to 355 tys. ton. Wartość sprzedaży eksportu ryb i produktów rybnych wyniosła około 1160,5 mln euro, jednak koszt importowanych ryb i produktów rybnych wyniósł 1165,2 mln euro, co pozostawiło ujemny bilans handlowy w wysokości około 5 mln euro (w porównaniu z 11 mln euro w 2011 r.). Polska importuje głównie surowiec rybny dla przetwórstwa, a eksportuje przede wszystkim produkty przetworzone: konserwy rybne, ryby wędzone, filety rybne i mięso ryb, które stanowią 92% łącznej wartości wszystkich produktów rybnych sprzedawanych za granicą. Głównymi importerami ryb i produktów rybnych z Polski są kraje Unii Europejskiej. Główne surowce wykorzystywane w przetwórstwie to śledź, makrela, łosoś, ryby białe (dorsz). Polskie rybołówstwo nie jest jednak w stanie sprostać potrzebom sektora przetwórstwa ryb, który uzależniony jest od importowanego surowca rybnego. Surowiec ten importowany jest główne z krajów Europejskiego Stowarzyszenia Wolnego Handlu (EFTA), a w następnej kolejności z państw Unii Europejskiej i krajów rozwijających się. Najważniejszymi gatunkami dla polskich importerów i przetwórców są łosoś, śledź, makrela i dorsz. W przypadku łososia i makreli importujemy praktycznie cały surowiec potrzebny do przetwórstwa, natomiast w przypadku śledzia i dorsza import uzupełnia krajowe połowy.

Wśród krajów należących do UE, Polska jest jednym z liderów w produkcji karpia. Roczna produkcja karpia handlowego waha się w granicach 15 tys. ton i praktycznie w całości przeznaczona jest na rynek krajowy.

6.4.3. Udział obszarów wiejskich w sektorze żywnościowym w Polsce

a) Obszary wiejskie w Polsce – zgodnie z metodologią ich wyodrębniania przez Główny Urząd Statystyczny, opartą na podziale administracyjnym, definiowane są jako tereny położone poza granicami administracyjnymi miast. Są to zatem obszary gmin wiejskich oraz części wiejskie gmin miejsko-wiejskich (wg Narodowego Spisu Powszechnego Ludności i Mieszkań 2011 GUS obszary wiejskie w Polsce stanowiły w 2011 r. ponad 93% powierzchni kraju i były zamieszkiwane przez około 39,8% ogółu ludności).

Obszary wiejskie są nierozerwalnie związane z rolniczym użytkowaniem gruntów, a tym mym prowadzeniem rolniczej działalności. Użytki rolne stanowią ponad 50% powierzchni ogólnej kraju. Możliwości produkcyjne rolnictwa zależą od czynników przyrodniczych, agrotechnicznych i społeczno-ekonomicznych, w tym od uwarunkowań związanych ze zmianami klimatycznymi. Miernikiem odnoszącym się do warunków przyrodniczych jest opracowany w Instytucie Uprawy Nawożenia i Gleboznawstwa w Puławach wskaźnik waloryzacji rolniczej przestrzeni produkcyjnej ujmujący warunki glebowe, klimatyczne, wodne i rzeźbę terenu. W Polsce mamy do czynienia z gorszymi warunkami glebowo-wodnymi niż ma to miejsce w większości krajów Unii Europejskiej. Na proces glebotwórczy miały wpływ kolejne zlodowacenia powodujące w efekcie pokrycie większości kraju glebami lekkimi, na przepuszczalnym piaszczystym podłożu. Gleby te nie dają możliwości uprawy takiego zestawu roślin, jaki mogą uprawiać rolnicy w UE, jak też nie umożliwiają uzyskania porównywalnych plonów, zwłaszcza wśród gatunków wymagających, takich jak pszenica czy warzywa. Na wysokość plonów mają wpływ również warunki klimatyczne charakteryzujące się niższą temperaturą, krótszym okresem wegetacyjnym i mniejszymi opadami niż w wielu rejonach Europy o korzystniejszych dla rolnictwa warunkach klimatycznych.

b) Infrastruktura terenów wiejskich – ma duży wpływ na poprawne funkcjonowanie systemu zaopatrzenia w żywność. W odniesieniu do terenów wiejskich infrastrukturę dzielimy na podstawowe grupy[413]:

- gospodarczą – usługi ułatwiające procesy produkcyjne w tym związane ze sprzedażą wytworzonych produktów (np. punkty zaopatrzenia w nawozy sztuczne, lecznice weterynaryjne, giełdy towarowe);
- techniczną – systemy transportowe, energetyczne, łączności, wodno-sanitarne (np. drogi, przystanki kolejowe, porty morskie, urzędy pocztowe);
- społeczną – obiekty zaspokajające potrzeby ludności wiejskiej w zakresie oświaty, wychowania, pomocy społecznej, ochrony zdrowia, kultury (np. szkoły, przedszkola, ośrodki zdrowia, obiekty kultu religijnego, organizacje społeczne);
- organizacyjną – systemy zarządzania na przykład gminami.

Mówiąc o infrastrukturze polskiej wsi, należy zwrócić uwagę na ogromne zróżnicowanie wielkości i struktury jednostek osadniczych na terenach wiejskich.
Wsi o liczbie mieszkańców powyżej 1 000 jest tylko 6%, podczas gdy wsi o liczbie mieszkańców od 500 do 1 000 jest 13%, a od 100 do 500 – 60%, z kolei poniżej 100 mieszkańców – 15%. Kolejnym czynnikiem jest rozproszenie zabudowy. Wsi o zabudowie rozproszonej, tj. o odległościach między gospodarstwami powyżej 200 m, jest 15 350, co stanowi 27%. Wsi o zabudowie zwartej o odległościach między gospodarstwami do 45 m jest 18 200, co stanowi 32%. Największą grupę, w liczbie 23 300, tj. 41%, stanowią wsie o zabudowie pośredniej.

Infrastruktura techniczna odgrywa szczególną rolę w kształtowaniu osadnictwa i rozwoju wsi, jest ważnym czynnikiem stymulującym aktywizację społeczno-gospodarczą otoczenia. Takie elementy infrastruktury, jak drogi, wodociągi i zaopatrzenie w wodę, kanalizacja, usuwanie i oczyszczanie ścieków komunalnych, wysypiska i unieszkodliwianie odpadów komunalnych, zaopatrzenia w energię elektryczną i cieplną oraz gaz, łączność – poprawiają nie tylko standard życia mieszkańców, ale przyczyniają się również do zwiększenia atrakcyjności inwestycyjnej i zapobiegają skutecznie odpływowi wykwalifikowanej siły roboczej do miast.

Do prawidłowego funkcjonowania systemu zaopatrzenia w żywność niezbędne jest między innymi prawidłowe funkcjonowanie obszarów dotyczących:

[413] Rutkowska G. *Analiza porównawcza infrastruktury technicznej w wybranej gminie z wymogami UE* http://iks_pn.sggw.pl/z38/art7.pdf *(*dr inż. Gabriela Rutkowska – Wydział Inżynierii i Kształtowania Środowiska, Szkoła Główna Gospodarstwa Wiejskiego Warszawa). - [dostęp: 08.03.2019]

- kształtowania ustroju rolnego państwa,
- ochrony gruntów przeznaczonych na cele rolne,
- scalania i wymiany gruntów, gleboznawczej klasyfikacji gruntów oraz podziału i rozgraniczenia nieruchomości na obszarze wsi,
- infrastruktury wsi (w szczególności: melioracji, w zakresie spraw nieobjętych działem gospodarka wodna, zaopatrzenia wsi i rolnictwa w wodę oraz oczyszczania ścieków i gospodarki odpadami, elektryfikacji i gazyfikacji w zakresie spraw nieobjętych działem gospodarka oraz telefonizacji wsi w zakresie spraw nieobjętych działem łączność),
- prac urządzeniowo-rolnych na gruntach Skarbu Państwa,
- rozwoju przedsiębiorczości (w tym w szczególności podnoszenia kwalifikacji zawodowych, wspomagania pozarolniczych form aktywności zawodowej i gospodarczej mieszkańców wsi),
- ubezpieczenia społecznego rolników (w zakresie ubezpieczenia społecznego rolników minister właściwy do spraw rozwoju wsi współdziała z ministrem właściwym do spraw zabezpieczenia społecznego).

6.4.4. Zagrożenia dla systemu zaopatrzenia w żywność

Najważniejsze zagrożenia systemu zaopatrzenia w żywność mogą wynikać z niestabilnego funkcjonowania takich systemów infrastruktury krytycznej, jak: zaopatrzenie w energię, surowce energetyczne i paliwa, łączności, finansowy, zaopatrzenia w wodę, transportowy. Należy jednak zaznaczyć, że powyższe systemy inaczej będą wpływać na rolnictwo tradycyjne, tak zwane drobnotowarowe, a inaczej na rolnictwo intensywne, zwane wysokotowarowym lub uprzemysłowionym. Dla gospodarstw tradycyjnych, najczęściej rodzinnych, krótkotrwałe zawirowania w zakresie funkcjonowania któregoś z systemu IK nie stanowią poważniejszego zagrożenia. Inaczej jest w przypadku gospodarstw towarowych w sensie ekonomiczno-rynkowym, gdzie już najmniejsze zachwianie na przykład w dostawach energii elektrycznej może spowodować katastrofalne skutki. Dlatego też oczekuje się:

a) poprawy bezpieczeństwa zaopatrzenia w energię elektryczną na obszarach wiejskich między innymi w wyniku rozwoju odnawialnych źródeł energii, a w tym biogazowni rolniczych. Duże towarowe gospodarstwa rolne dysponują największym potencjałem sprzyjającym takim inwestycjom. Biogazownie zwłaszcza wykorzystujące pozostałości oraz produkty

uboczne rolnictwa poza funkcją utylizacyjną umożliwią wytwarzanie energii elektrycznej z biogazu, podnosząc tym samym bezpieczeństwo energetyczne. Pod tym kątem przygotowywane są między innymi zmiany w przepisach prawnych w obszarze energetyki, a przede wszystkim projektowana ustawa o odnawialnych źródłach energii;

b) budowy rynku surowcowego dla produkcji biopaliw ciekłych. Biopaliwa pierwszej generacji wykorzystujące technologie fermentacji alkoholowej na obecnym etapie nie stanowią zagrożenia rynku surowców spożywczych, ponieważ w Polsce dla tego celu wykorzystuje się około 3% produkcji zbożowej. W przypadku produkcji surowców oleistych głównie rzepaku, z którego wytwarzane są estry wpływ popytu na rynku biopaliwowym jest już wyraźnie zauważalny. W 2011 roku w kraju wytworzono około 364 tys. ton estrów co odpowiada zapotrzebowaniu na rzepak w ilości około 1 mln ton. Potrzeby przemysłu spożywczego na rzepak wynoszą również około 1 mln ton tego surowca. Dotychczas osiągane zdolności produkcyjne rzepaku w Polsce, w zależności od warunków pogodowych, wynosiły około 2 mln ton. Potrzeby przemysłu paliwowego w 2011 roku wyniosły 946 tys. ton estrów rzepakowych, do których wytworzenia niezbędne są dostawy rzepaku wynoszące około 3 mln ton. Bez istotnego wzrostu plonowania rzepaku ustabilizowanego na poziomie 3 ton/ha oraz importu zaspokojenie tego popytu nie będzie możliwe (w latach 2006-2010 przeciętny plon wynosił około 2,77 t/ha). Należy mieć na uwadze, że dostępna w Polsce powierzchnia gleb nadająca się pod tę uprawę wynosi około 1,2 mln ha i tereny o korzystnych warunkach do uprawy tego gatunku uległy już wyczerpaniu;

c) ochrony gruntów o większej przydatności rolniczej. W celu zapewnienia bezpieczeństwa żywnościowego kraju grunty orne o większej przydatności rolniczej, obejmujące takie kompleksy, jak: pszenny bardzo dobry, pszenny dobry, żytni bardzo dobry i żytni dobry, których łączna powierzchnia w Polsce wynosi około 9,4 mln ha, nie powinny być przeznaczane pod wieloletnie plantacje roślin energetycznych. Dynamika wzrostu powierzchni zajmowanej przez rośliny energetyczne będzie miała tendencję malejącą wskutek sukcesywnego zastępowania w przyszłości biopaliw pierwszej generacji biopaliwami płynnymi drugiej generacji, wytwarzanymi z biomasy lignocelulozowej, efektywniej wykorzystującej energię biomasy i mniej konkurencyjnej w stosunku do produkcji żywności.

Nie należy uwzględniać przy szacowaniu zasobów dostępnych pod uprawy energetyczne gleb najsłabszych o niskim potencjale produkcyjnym, na których plony roślin są silnie uzależnione od ilości i rozkładu opadów w sezonie wegetacyjnym. Niedopuszczalna jest także zmiana trwałych użytków zielonych na użytki rolne przeznaczone pod intensywne uprawy energetyczne. Ze względu na oddziaływanie na przestrzeń produkcyjną rynku żywnościowego wpływ popytu na biomasę ze strony przemysłu paliwowego i energetycznego powinien być stale monitorowany.

6.5. System zaopatrzenia w wodę

System zaopatrzenia w wodę to ściśle powiązane ze sobą przedsiębiorstwa i urządzenia pobierające, uszlachetniające, dostarczające i oczyszczające wodę dla ludności i przemysłu. W wyniku postępującej koncentracji ludności w ośrodkach miejskich zaopatrzenie w wodę i odbiór ścieków stało się jedną z najistotniejszych usług zapewniających sprawne i stabilne funkcjonowanie społeczności. Znaczenie zaopatrzenia w wodę nie ogranicza się jedynie do obszarów miejskich, również obszary wiejskie wykorzystują znaczne jej ilości w produkcji roślinnej i zwierzęcej.

Tabela 9. Zasoby wód powierzchniowych w 2016 roku [hm^3]

Regionalny Zarząd Gospodarki Wodnej	
Gdańsk	35 466,1
Gliwice	7 775,7
Kraków	43 768,8
Poznań	54 528,7
Szczecin	20 473,9
Warszawa	111 113,2
Wrocław	39 551,0
OGÓŁEM	**312 677,4**

Źródło: GUS

Tabela 10. Zasoby eksploatacyjne wód podziemnych w 2016 roku [$hm^{3/rok}$]

Ogółem	**17 276,7**
Czwartorzędowych	11 436,3
Trzeciorzędowych	1 799,6
Kredowych	2 361,5
Starszych	1 679,4

Źródło: GUS

Tabela 11. **Pobór wody na potrzeby gospodarki narodowej i ludności według źródeł poboru w 2016 roku** [hm^3]

O G Ó Ł E M	11 152,2
Wody powierzchniowe	9 461,6
Wody podziemne	1 628,5
Wody z odwadniania zakładów górniczych oraz obiektów budowlanych (użyte do produkcji)	62,1
Cele produkcyjne	8 008,1
Wody powierzchniowe	7 740,0
Wody podziemne	206,0
Wody z odwadniania zakładów górniczych oraz obiektów budowlanych (użyte do produkcji)	62,1
Nawodnienia w rolnictwie i leśnictwie oraz napełnianie i uzupełnianie stawów rybnych	1 111,2
Wody powierzchniowe	1 111,2
Eksploatacja sieci wodociągowej	2 033,0
Wody powierzchniowe	610,5
Wody podziemne	1 422,5

Źródło: GUS

W 2016 roku długość sieci kanalizacyjnej wyniosła około 128 tys. km. W układzie przestrzennym największe zagęszczenie sieci [w km na 100 km^2] występuje w województwach: śląskim (99,3), podkarpackim (77,2), małopolskim (70,1) oraz pomorskim (45,3). W Polsce funkcjonowało 3 143 oczyszczalni ścieków komunalnych, w tym 55 mechanicznych, 2 261 biologicznych i 821 z podwyższonym usuwaniem biogenów. Z kolei w zakładach przemysłowych funkcjonowało 1 110 oczyszczalni. Sieć wodociągowa rozdzielcza w 2011 roku wynosiła ponad 278 tys. km. W układzie przestrzennym największe zagęszczenie sieci [w km na 100 km^2] występuje na terenach województw: śląskiego (162,9), kujawsko-pomorskiego (123,2), łódzkiego (120,7) i małopolskiego (116,6); najmniejsze na terenach województw zachodniopomorskiego (45,2) i lubuskiego (46,8).

6.6. System ochrony zdrowia

System ochrony zdrowia to zespół osób i instytucji mający za zadanie zapewnienie opieki zdrowotnej ludności, a jego sprawne funkcjonowanie (wraz z systemem ratowniczym) jest gwarantem praw obywatela zapisanych w Konstytucji.

Uczestników systemu można podzielić na następujące kategorie:

- świadczeniobiorców – czyli pacjentów,

- instytucję ubezpieczenia zdrowotnego pełniącą funkcję płatnika – czyli Narodowy Fundusz Zdrowia (NFZ),
- świadczeniodawców – czyli podmioty wykonujące działalność leczniczą, zgodnie z art. 4 i 5 *Ustawy z dnia 15 kwietnia 2011 roku o działalności leczniczej (Dz. U. z 2013 r. poz. 217)*,
- organy kontroli i nadzoru:
    - Państwową Inspekcję Sanitarną,
    - Państwową Inspekcję Farmaceutyczną,
    - Rzecznika Praw Pacjenta,
    - wojewodów i działające przy nich wojewódzkie centra zdrowia publicznego oraz konsultantów wojewódzkich w poszczególnych specjalnościach medycznych,
    - Ministerstwo Zdrowia, które wytycza kierunki polityki zdrowotnej kraju oraz posiada uprawnienia kontrolne, a także działających przy nim konsultantów krajowych w poszczególnych specjalnościach medycznych.

Najważniejszymi elementami ze względu na dostępność systemu są podmioty lecznicze oraz Narodowy Fundusz Zdrowia (NFZ).

Podmiotami leczniczymi w zakresie, w jakim wykonują działalność leczniczą, są:

- przedsiębiorcy w rozumieniu przepisów *Ustawy z dnia 2 lipca 2004 roku o swobodzie działalności gospodarczej (Dz. U. z 2010 r. Nr 220, poz. 1447, z późn. zm.)* we wszelkich formach przewidzianych dla wykonywania działalności gospodarczej, jeżeli ustawa nie stanowi inaczej;
- samodzielne publiczne zakłady opieki zdrowotnej;
- jednostki budżetowe, w tym państwowe jednostki budżetowe tworzone i nadzorowane przez Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, Ministra Sprawiedliwości lub Szefa Agencji Bezpieczeństwa Wewnętrznego, posiadające w strukturze organizacyjnej ambulatorium, ambulatorium z izbą chorych lub lekarza podstawowej opieki zdrowotnej;
- instytuty badawcze, o których mowa w art. 3 *Ustawy z dnia 30 kwietnia 2010 roku o instytutach badawczych (Dz. U. Nr 96, poz. 618, z późn. zm.)*;
- fundacje i stowarzyszenia, których celem statutowym jest wykonywanie zadań w zakresie ochrony zdrowia, i których statut dopuszcza prowadzenie działalności

leczniczej oraz posiadające osobowość prawną jednostki organizacyjne stowarzyszeń, o których mowa w pkt 5;

- osoby prawne i jednostki organizacyjne działające na podstawie przepisów o stosunku Państwa do Kościoła katolickiego w Rzeczypospolitej Polskiej, o stosunku Państwa do innych kościołów i związków wyznaniowych oraz o gwarancjach wolności sumienia i wyznania.

Opieka zdrowotna o charakterze stacjonarnym świadczona jest w szpitalach ogólnych oraz w innych podmiotach leczniczych. W 2016[414] roku funkcjonowało:

- 861 szpitali ogólnych, w tym 540 szpitali publicznych, tj.63,3%, oraz 321 szpitali niepublicznych,
- łącznie 505 stacjonarnych zakładów długoterminowej opieki zdrowotnej (zakłady opiekuńczo-lecznicze i pielęgnacyjno-opiekuńcze o charakterze ogólnym i psychiatrycznym) o 8,1% (38) więcej niż w 2010 roku oraz 79 hospicjów,
- 19,1 tys. ambulatoryjnych zakładów opieki zdrowotnej z czego 14,4% stanowiły zakłady publiczne a 85,6% niepubliczne,
- 6 675 jednostki podstawowej służby medycyny pracy,
- 23 regionalne centra krwiodawstwa oraz 164 oddziały terenowe, łącznie z resortowymi.

W 2016 roku w Polsce działało 11,7 tys. aptek ogólnodostępnych, 1,2 tys. punktów aptecznych oraz 40 aptek zakładowych. Niemal wszystkie apteki ogólnodostępne należały do prywatnych właścicieli (99,6%). W omawianym roku tylko niecałe 6% aptek ogólnodostępnych pełniło stałe dyżury nocne, a 23,8% miało je okresowo.

Narodowy Fundusz Zdrowia (NFZ) to państwowa jednostka organizacyjna posiadająca osobowość prawną. Fundusz zarządza środkami finansowymi pochodzącymi głównie z obowiązkowych składek ubezpieczenia zdrowotnego.

6.7. System transportowy

Przez transport należy rozumieć przemieszczanie ludzi, ładunków (przedmiot transportu) w przestrzeni przy wykorzystaniu odpowiednich środków transportu. Przemieszczanie dóbr,

[414] http://www.stat.gov.pl/cps/rde/xbcr/gus/zo_zdrowie_i_ochrona_zdrowia_w_2016.pdf

ludzi i usług stanowi jedną z podstawowych cech charakterystycznych dla współczesnej gospodarki i społeczeństwa, dlatego sprawnie funkcjonujący system transportowy stanowi jeden z filarów nowoczesnego państwa.

Ogólnie transport można podzielić na transport pasażerski (komunikację) i transport towarowy (ładunków). Z kolei ze względu na rodzaj, transport dzieli się na:

- transport kolejowy,
- transport samochodowy,
- transport lotniczy,
- transport rurociągowy,
- żegluga śródlądowa,
- żegluga morska.

Podstawowe informacje o transporcie w 2016 roku. (za GUS), pokazujące znaczenie tego systemu dla gospodarki i społeczeństwa, przedstawiają poniższa tabela oraz wykresy.

Tabela 12. Statystyka efektywności systemu transportowego w 2016 roku

Praca przewozowa w mln tonokilometrów	**317 807**
w tym: transport kolejowy	53 746
transport samochodowy	218 888
transport rurociągowy	22 794
żegluga śródlądowa	909
żegluga morska	21 341
Obroty ładunkowe w portach morskich w tys. ton	**57 738**
Statki wchodzące do morskich portów handlowych	
liczba	18 864
pojemność NT w tys.	71 903
Przewozy pasażerów w tys. pasażerów	**807 141**
w tym: transport kolejowy	263 609
transport samochodowy	534 885
transport lotniczy	6 491
Praca przewozowa w mln pasażerokilometrów	**50 073**
w tym: transport kolejowy	18 177
transport samochodowy	20 651
transport lotniczy	11 065

Ruch pasażerów:	
W portach lotniczych	
przyjazdy do kraju	9 689 842
wyjazdy z kraju	9 803 830
W morskich portach handlowych	
przyjazdy do kraju	781 353
wyjazdy z kraju	802 785

Źródło: GUS.

6.8. System ratowniczy

Przez ratownictwo należy rozumieć ogół środków i przedsięwzięć organizacyjnych podejmowanych w celu ratowania zdrowia i życia, mienia i środowiska znajdujących się w niebezpieczeństwie oraz przewidywania, rozpoznawania i likwidacji skutków zdarzeń. Razem z systemami ochrony zdrowia razem stanowią podstawę realizacji konstytucyjnych praw obywateli do ochrony ich życia i zdrowia.

W ramach Systemu Ratowniczego w Polsce funkcjonują:

- Krajowy System Ratowniczo-Gaśniczy – celem jego funkcjonowania jest ratowanie życia, zdrowia, mienia i środowiska. System ten skupia jednostki ochrony przeciwpożarowej, inne służby, inspekcje, straże, instytucje oraz podmioty, które dobrowolnie, w drodze umowy cywilnoprawnej, zgodziły się współdziałać w akcjach ratowniczych. W 2016 roku odnotowano 457 988 zdarzeń, w tym 171 839 pożarów, 268 280 miejscowych zagrożeń oraz 17 869 fałszywych alarmów;
- Państwowe Ratownictwo Medyczne – system powołany w celu ratowania życia i zdrowia ludzkiego. Jednostkami systemu są:
    - szpitalne oddziały ratunkowe,
    - zespoły ratownictwa medycznego, w tym lotnicze zespoły ratownictwa medycznego.

W 2016 roku w ramach ratownictwa medycznego pomoc medyczną w razie nagłego wypadku świadczyło 1 537 zespołów ratownictwa medycznego, w tym zespoły podstawowe i specjalistyczne, a ponadto zespoły wypadkowe oraz zespoły reanimacyjne. Funkcjonowały również 222 szpitalne oddziały ratunkowe. W ramach ratownictwa medycznego w 2016 roku zrealizowano około 2,8 mln wyjazdów na miejsce zdarzenia.

- System Powiadamiania Ratunkowego – stworzony w 2012 roku w celu integracji Krajowego Systemu Ratowniczo-Gaśniczego i Państwowego Ratownictwa Medycznego.
- Ratownictwo górskie – działania związane z prowadzeniem akcji ratowniczych w terenie górskim, poszukiwanie zaginionych osób, udzielanie pomocy medycznej ofiarom wypadków, transport poszkodowanych do miejsc, gdzie można im udzielić pełnej pomocy medycznej; również działania prewencyjne związane z informowaniem o zagrożeniach, niebezpieczeństwie lawin i spodziewanych załamaniach pogody. Ratownictwo górskie zorganizowane jest w oparciu o struktury organizacyjne Górskiego Ochotniczego Pogotowia Ratunkowego i Tatrzańskiego Ochotniczego Pogotowia Ratunkowego. GOPR i TOPR w 2016 roku podjęły 8 540 działań (interwencji, akcji ratunkowych oraz wypraw ratunkowych).
- Ratownictwo morskie – działalność polegająca na ratowaniu życia i mienia na morzu. W Polsce ratownictwem morskim zajmują się przede wszystkim dwie instytucje państwowe:
  - Morska Służba Poszukiwania i Ratownictwa (zwana Służbą SAR),
  - Marynarka Wojenna.

  Morska Służba Poszukiwania i Ratownictwa zrealizowała w 2016 roku 246 działań ratowniczych.
- Ratownictwo górnicze – zajmujące się udzielaniem pomocy zagrożonym górnikom i kopalniom oraz usuwaniem skutków i przywracaniem bezpiecznych warunków pracy po zaistnieniu tych zagrożeń oraz działalnością prewencyjną i szkoleniową w kopalniach. Każda kopalnia ma własny zastęp ratowniczy, jednak główną bazą ratowników górniczych w Polsce jest Centralna Stacja Ratownictwa Górniczego z siedzibą w Bytomiu wraz z Okręgowymi Stacjami Ratownictwa.
- Ratownictwo wodne – prowadzenie działań ratowniczych polegających w szczególności na organizowaniu i udzielaniu pomocy osobom, które uległy wypadkowi lub są narażone na niebezpieczeństwo utraty życia lub zdrowia na obszarze wodnym, przez uprawnione do tego podmioty.
- Krajowy System Wykrywania Skażeń i Alarmowania (KSWSiA) – stanowi wyspecjalizowany podsystem do przeciwdziałania i likwidacji skażeń chemicznych, biologicznych, promieniotwórczych i nuklearnych. Elementami składowymi systemu KSWSiA są:

- System Wykrywania Skażeń Sił Zbrojnych RP,
- sieci i systemy nadzoru epidemiologicznego i kontroli chorób zakaźnych,
- system stacji wczesnego wykrywania skażeń promieniotwórczych (koordynowany przez Prezesa Państwowej Agencji Atomistyki),
- wojewódzkie systemy wykrywania i alarmowania oraz wojewódzkie systemy wczesnego ostrzegania o zagrożeniach,
- system alarmowania o zagrożeniach i skażeniach, określony w Krajowym Planie Zwalczania Zagrożeń i Zanieczyszczeń Środowiska Morskiego,
- jednostki organizacyjne prowadzące działania interwencyjne nadzorowane przez ministra właściwego do spraw wewnętrznych.

6.9. System zapewniający ciągłość działania administracji publicznej

Administracja publiczna to prawo władcze wykonywania zadań przypisywanych przez porządek prawny państwu i jego organom lub innym podmiotom wykonującym funkcje władcze. Administrację publiczną w Polsce tworzą między innymi:

- administracja rządowa,
- administracja samorządowa.

6.9.1. Administracja rządowa

Administrację rządową ze względu na zakres jej działania można podzielić na administrację rządową na szczeblu centralnym (Prezes Rady Ministrów, Rada Ministrów, ministrowie oraz centralne organy administracji rządowej) oraz na administrację rządową na szczeblu wojewódzkim (przedstawicielem Rady Ministrów w województwie jest wojewoda, administracja rządowa na tym szczeblu obejmuje organy rządowej administracji zespolonej oraz organy niezespolonej administracji rządowej).

a) Administracja rządowa centralna to:

- Ministerstwo Cyfryzacji,
- Ministerstwo Edukacji Narodowej,
- Ministerstwo Energii,
- Ministerstwo Finansów,
- Ministerstwo Gospodarki Morskiej i Żeglugi Śródlądowej,

- Ministerstwo Infrastruktury,
- Ministerstwo Inwestycji i Rozwoju,
- Ministerstwo Kultury i Dziedzictwa Narodowego,
- Ministerstwo Nauki i Szkolnictwa Wyższego,
- Ministerstwo Obrony Narodowej,
- Ministerstwo Przedsiębiorczości i Technologii,
- Ministerstwo Rodziny, Pracy i Polityki Społecznej,
- Ministerstwo Rolnictwa i Rozwoju Wsi,
- Ministerstwo Sportu i Turystyki,
- Ministerstwo Spraw Wewnętrznych i Administracji,
- Ministerstwo Spraw Zagranicznych,
- Ministerstwo Sprawiedliwości,
- Ministerstwo Środowiska,
- Ministerstwo Zdrowia.

b) Centralne organy administracji rządowej to:

- Generalny Dyrektor Dróg Krajowych i Autostrad,
- Generalny Dyrektor Ochrony Środowiska,
- Główny Geodeta Kraju,
- Główny Inspektor Farmaceutyczny,
- Główny Inspektor Jakości Handlowej Artykułów Rolno-Spożywczych,
- Główny Inspektor Nadzoru Budowlanego,
- Główny Inspektor Ochrony Roślin i Nasiennictwa,
- Główny Inspektor Ochrony Środowiska,
- Główny Inspektor Sanitarny,
- Główny Inspektor Transportu Drogowego,
- Główny Lekarz Weterynarii,
- Inspektor do spraw Substancji Chemicznych,
- Komendant Główny Państwowej Straży Pożarnej,
- Komendant Główny Policji,
- Komendant Główny Straży Granicznej,
- Naczelny Dyrektor Archiwów Państwowych,

- Prezes Głównego Urzędu Miar,
- Prezes Głównego Urzędu Statystycznego,
- Prezes Kasy Rolniczego Ubezpieczenia Społecznego,
- Prezes Krajowego Zarządu Gospodarki Wodnej,
- Prezes Państwowej Agencji Atomistyki,
- Prezes Urzędu Lotnictwa Cywilnego,
- Prezes Urzędu Ochrony Konkurencji i Konsumentów,
- Prezes Urzędu Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych,
- Prezes Urzędu Regulacji Energetyki,
- Prezes Urzędu Komunikacji Elektronicznej,
- Prezes Urzędu Transportu Kolejowego,
- Prezes Urzędu Zamówień Publicznych,
- Prezes Wyższego Urzędu Górniczego,
- Rzecznik Praw Pacjenta,
- Szef Agencji Bezpieczeństwa Wewnętrznego,
- Szef Agencji Wywiadu,
- Szef Centralnego Biura Antykorupcyjnego,
- Szef Obrony Cywilnej Kraju,
- Szef Służby Kontrwywiadu Wojskowego,
- Szef Służby Wywiadu Wojskowego,
- Szef Urzędu do Spraw Cudzoziemców,
- Urząd do Spraw Kombatantów i Osób Represjonowanych,
- Urząd Patentowy Rzeczypospolitej Polskiej.

c) Rządowa administracja zespolona

Rządową administrację zespoloną tworzą działający pod zwierzchnictwem wojewody kierownicy zespolonych służb, inspekcji i straży wykonujący zadania i kompetencje określone w ustawach. Do tej kategorii należą na przykład:

- Komendant Wojewódzki Policji,
- Komendant Wojewódzki Państwowej Straży Pożarnej,
- Kurator Oświaty,

- Państwowy Wojewódzki Inspektor Sanitarny,
- Wojewódzki Inspektor Farmaceutyczny,
- Wojewódzki Inspektor Inspekcji Handlowej,
- Wojewódzki Inspektor Nadzoru Budowlanego,
- Wojewódzki Inspektor Ochrony Roślin i Nasiennictwa,
- Wojewódzki Inspektor Ochrony Środowiska,
- Wojewódzki Inspektor Jakości Handlowej Artykułów Rolno-Spożywczych,
- Wojewódzki Inspektor Transportu Drogowego,
- Wojewódzki Inspektor Nadzoru Geodezyjnego i Kartograficznego,
- Wojewódzki Konserwator Zabytków,
- Wojewódzki Lekarz Weterynarii.

d) Niezespolona administracja rządowa

Organami niezespolonej administracji rządowej (niekiedy zwanej również administracją specjalną) są podmioty podporządkowane właściwym ministrom oraz kierownikom państwowych osób prawnych i kierownikom innych państwowych jednostek organizacyjnych wykonujące zadania z zakresu administracji rządowej na obszarze województwa. *Ustawa z dnia 23 stycznia 2009 roku o wojewodzie i administracji rządowej w województwie (Dz. U. Nr 31, poz. 206, z późn. zm.)* wymienia następujące organy niezespolonej administracji rządowej:

- szefowie wojewódzkich sztabów wojskowych i wojskowi komendanci uzupełnień,
- dyrektorzy izb celnych i naczelnicy urzędów celnych,
- dyrektorzy izb skarbowych, naczelnicy urzędów skarbowych, dyrektorzy urzędów kontroli skarbowej,
- dyrektorzy okręgowych urzędów górniczych i dyrektor Specjalistycznego Urzędu Górniczego,
- dyrektorzy okręgowych urzędów miar i naczelnicy obwodowych urzędów miar,
- dyrektorzy okręgowych urzędów probierczych,
- dyrektorzy regionalnych zarządów gospodarki wodnej,
- dyrektorzy urzędów morskich,
- dyrektorzy urzędów statystycznych,
- dyrektorzy urzędów żeglugi śródlądowej,
- graniczni i powiatowi lekarze weterynarii,

- komendanci oddziałów Straży Granicznej, komendanci placówek i dywizjonów Straży Granicznej,
- okręgowi inspektorzy rybołówstwa morskiego,
- państwowi graniczni inspektorzy sanitarni,
- regionalni dyrektorzy ochrony środowiska[415].

6.9.2. Administracja samorządowa

Administrację samorządową ukształtowano w Polsce na trzech szczeblach: gminnym, powiatowym i wojewódzkim. Do organów samorządu terytorialnego należą:

a) organy stanowiące:
   - sejmik województwa (16 województw),
   - rada powiatu (308 powiatów ziemskich i 65 grodzkich – miast na prawach powiatu),
   - rada gminy (2 489 – gminy);

b) organy wykonawcze:
   - zarząd województwa,
   - zarząd powiatu,
   - wójt (burmistrz, prezydent miasta).

6.10. System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych

6.10.1. Sektor przemysłu chemicznego (łącznie z farmaceutycznym) w Polsce[416]

Znaczenie sektora chemicznego warunkowany jest jego specyfiką – jest bazą surowcową wszystkich sektorów gospodarki. Produkcja chemiczna wypiera wyroby z metalu, drewna, szkła i włókna naturalnego. Największymi odbiorcami wyrobów przemysłu chemicznego są sektory: maszynowy i metalowy, motoryzacyjny, elektrotechniczny i elektroniczny, budowlany, papierniczy i poligraficzny, tekstylny i odzieżowy, rolniczy.

Wśród działów przemysłu chemicznego wyróżnia się:

a) wielką chemię – produkty tanie i masowo stosowane w wielkich ilościach:

[415] *Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie* (Dz. U. Nr 31, poz. 206, z późn. zm.
[416] Systematykę polskiego sektora chemicznego oparto na danych Ministerstwa Gospodarki – *Polska 2016, Raport o Stanie Gospodarki* – Warszawa 2016.

- przemysł petrochemiczny – oparty na przetwórstwie ropy naftowej,
- przemysł sodowy – opiera się na soli kamiennej i wapieniach,
- przemysł kwasu siarkowego – wytwórnie kwasu siarkowego,
- przemysł nawozów sztucznych,
- zakłady nawozów fosforowych, produkcja nawozów azotowych,
- przemysł tworzyw sztucznych,
- przemysł włókien sztucznych;

b) chemię niskotonażową – produkty kosztowne i stosowane w niewielkich ilościach:

- przemysł farmaceutyczny,
- przemysł kosmetyczny,
- przemysł środków pomocniczych – środki czystości, higieniczne, pielęgnacji roślin itp. ;

c) przetwórstwo chemiczne – które na bazie produktów wielkotonażowych wytwarza produkty końcowe:

- przemysł gumowy,
- przemysł przetwórstwa tworzyw sztucznych,
- przemysł farb i lakierów,
- dystrybucja i handel odczynnikami.

Według stanu na koniec III kwartału 2016 roku na terenie Polski funkcjonowało 1 311 zakładów (dane Głównego Inspektora Ochrony Środowiska), w których w trakcie procesu przemysłowego, magazynowania lub transportu, może powstać z udziałem substancji niebezpiecznych emisja, pożar lub eksplozja mogące spowodować natychmiastowe powstanie zagrożenia życia lub zdrowia ludzi lub środowiska, zwane poważnymi awariami przemysłowymi, w tym: 173 zakłady o dużym ryzyku powstania poważnej awarii przemysłowej, 194 zakłady o zwiększonym ryzyku powstania poważnej awarii przemysłowej oraz 853 pozostałe zakłady, w których stosuje się substancje niebezpieczne, oraz w których mogą powstać poważne awarie przemysłowe.

6.10.2. Obiekty jądrowe i źródła promieniowania jonizującego

W Polsce nie istnieje żaden obiekt jądrowy wykorzystywany do produkcji energii elektrycznej ani żaden obiekt funkcjonalnie powiązany z produkcją energii elektrycznej z wykorzystaniem technologii jądrowej[417].

Istniejący reaktor badawczy „Maria" ma zastosowanie do celów naukowych, medycznych i szkoleniowych. Oprócz reaktora „Maria"[418] w Polsce istnieją także inne obiekty jądrowe (likwidowany reaktor badawczy „Ewa" oraz dwa przechowalniki wypalonego paliwa jądrowego), jednak, podobnie jak ma to miejsce w przypadku reaktora „Maria", ich funkcjonowanie nie wiązało się i nie wiąże z produkcją energii elektrycznej.

Odbiorem, transportem, przetwarzaniem i składowaniem odpadów powstających u wszystkich użytkowników materiałów promieniotwórczych w kraju zajmuje się Zakład Unieszkodliwiania Odpadów Promieniotwórczych. Miejscem składowania powstających w Polsce odpadów promieniotwórczych jest Krajowe Składowisko Odpadów Promieniotwórczych (ZUOP). Składowisko w Różanie istnieje od 1961 roku i jest jedynym tego typu obiektem w naszym kraju.

Państwowa Agencja Atomistyki prowadzi i weryfikuje rejestr zamkniętych źródeł promieniotwórczych. Obejmuje on informacje o ponad 16 tys. źródeł, w tym także zużytych źródłach promieniotwórczych, tj. źródłach wycofanych z eksploatacji i przekazanych do ZUOP, jak również informacje dotyczące ruchu źródła, czyli terminy otrzymania i przekazania źródła oraz dokumenty z tym związane. Krajowy system ewidencji materiałów jądrowych spełnia funkcję kontroli nad tymi materiałami w Polsce.

6.10.3. Rurociągi substancji niebezpiecznych

Na terenie Polski, poza rurociągami naftowymi (ropa surowa, produkty finalne) oraz gazu ziemnego, które zostały opisane w rozdziałach 6.1.3-6.1.4., brak jest rurociągów transportujących substancje niebezpieczne.

6.11. Infrastruktura a zagrożenie cyberterroryzmem – podsumowanie

Ataki na systemy wchodzące w skład tak zwanej infrastruktury krytycznej państwa, czyli między innymi bankowo-finansowe, energetyczne, telekomunikacyjne, dostarczania wody,

[417] Dane Ministerstwa Gospodarki – *Polska 2016 Raport o Stanie Gospodarki* – Warszawa, 2016.

[418] Reaktor badawczy „Maria", obecnie jedyny czynny reaktor jądrowy w Polsce, to wysokostrumieniowy reaktor badawczy typu basenowego, o projektowej nominalnej mocy termicznej 30 MW i gęstości strumienia neutronów termicznych w rdzeniu wynoszącej 1014 n/cm 2. s.

transportu, służb do działań w sytuacjach wyjątkowych, które przechowują informacje ważne dla bezpieczeństwa państwa, to stanowczo największe pole zagrożenia cyberterroryzmem[419]. Systemy przedsiębiorstw kluczowych sektorów, które przechowują oraz przetwarzają informacje, są niebywale istotne nie tylko z punktu widzenia działalności firmy, ale i całego systemu gospodarczego i bezpieczeństwa państwa. Warto przywołać tu zestawienie wskazujące przewidywane miejsca występowania zagrożeń bezpośrednich infrastruktury krytycznej – w każdym przypadku są to miejsca lokalizacji kluczowych elementów systemów teleinformatycznych, takich jak:

- centra zarządzania i utrzymania infrastruktury teleinformatycznej: własnych zasobów administracji, w szczególności urzędów, wydziałów i biur bezpieczeństwa i zarządzania kryzysowego oraz przedsiębiorców dostarczających usługi telekomunikacyjne;
- centrale telekomunikacyjne obsługujące instytucje państwowe, urzędy oraz organizacje przewidywane do likwidacji zagrożeń;
- miejsca przebiegu telekomunikacyjnych linii międzycentralowych i podstawowych linii telekomunikacyjnych;
- stacje bazowe i satelitarne,
- inne ważne obiekty telekomunikacyjne (np. wyniesione koncentratory, stacje czołowe, węzły dostępowe itp.), serwery zarządzające systemami i bazami danych i kluczowe bazy danych (rejestry państwowe), wykorzystywane przez administrację publiczną (np. PESEL, Regon, CEPIK, rejestry sądowe i inne systemy)[420]

Infrastruktura krytyczna ze względu na swoje znaczenie i rolę w bezpieczeństwie państwa jest częstym przedmiotem działania terrorystów. Starają się oni podejmować wszelkie działania, które zakłócą jej sprawne funkcjonowanie, a tym samym doprowadzą do dezorganizacji w danym państwie. Coraz większym zagrożeniem staje się cyberterroryzm, co należy wiązać z postępem technologicznym i informatyzacją życia ludzkiego. Obecnie trudno bowiem mówić o elementach infrastruktury krytycznej, która nie korzysta ze wsparcia technologicznego. Stąd też należy powiedzieć, że podatność na zagrożenia cyberterroryzmem stale wzrasta i będzie wzrastać. W celu zrozumienia tej zależności koniecznym jest przedstawienie powiązań, jakie występują pomiędzy elementami infrastruktury krytycznej, rozwiązaniami z zakresu technologii

[68] Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa we współczesnym świecie,* Warszawa 2003.
[420] Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne", 1-2/ 2014, s. 26.

informacyjnych, z których korzystają, potencjalnymi zagrożeniami terrorystycznymi oraz ich ewentualnymi skutkami[421].

Jednym z podstawowych elementów infrastruktury krytycznej w przypadku, którego obserwuje się wysoką podatność na cyberterroryzm, jest system zaopatrzenia w surowce energetyczne, energię oraz paliwa. Wynika to głównie z dużego zaawansowania technologicznego w tym zakresie, ale także specyficznych cech surowców energetycznych i paliw. Są to bowiem zasoby wyczerpywalne i trudno dostępne. Tylko niewielka ilość państw posiada bezpośredni dostęp do surowców i jest w stanie je wydobywać, stad też pozostałe państwa dążą do wdrażania nowoczesnych rozwiązań, za sprawą których możliwe będzie efektywne pozyskiwanie surowców energetycznych czy energii. Mowa tutaj o zachowaniu korzystnych proporcji pomiędzy nakładami pracy, jej kosztami oraz osiąganymi efektami[422]. Przykładowe rozwiązania z zakresu technologii informacyjnych stosowane w systemie zaopatrzenia w surowce energetyczne, energię oraz paliwa, to chociażby:

- systemy nadzorowania oraz monitorowania miejsc w których składowane są surowce oraz paliwa;
- systemy odpowiadające za dystrybucję energii elektrycznej;
- systemy pozwalające na zarządzanie krajową bądź regionalną siecią energetyczną;
- systemy zabezpieczenia elektroenergetycznego[423].

W przypadku wymienionych systemów zaopatrzenia w surowce energetyczne, energię oraz paliwa cyberterroryści mogą zaatakować elektroniczne części tworzące system monitorowania i nadzorowania miejsc, w których składowane są surowce. Elementy te odpowiadają zazwyczaj za kontrolę ciśnienia paliwa oraz ilości wydobywających się oparów. Ich uszkodzenie prowadzi do wyładowań elektrycznych, które są niezwykle szkodliwe dla całego środowiska naturalnego. Wyładowania te w skrajnym przypadku są w stanie doprowadzić do cierpienia fizycznego – spowodować śmierć lub poważne obrażenia ciała. Cyberterroryści mogą również dążyć do odłączenia linii wysokiego napięcia, co pozbawi dostęp do energii elektrycznej obiekty infrastruktury krytycznej. W zależności od rozmiaru działań terrorystów może dojść do znacznego chaosu i zakłóceń w zakresie świadczenia usług lub też wykonywania czynności

[421] Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki informacyjne", nr 1-2, 2014, s. 28.
[422] Szewczyk T., Pyznar M., *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne*, www.abw.gov.pl/download/1/1886/Szewczyk.pdf, [dostęp: 16.11.2018].
[423] Lidwa W., Krzeszowski W., Więcek W., Kamiński P., *Ochrona infrastruktury krytycznej*, AON, Warszawa 2012, s. 123.

codziennego życia. Przedmiotem ataków mogą być połączenia systemów elektroenergetycznych i gazowych. Cyberterroryści poprzez ich rozregulowanie przyczynią się do wywołania znacznych strat ekonomicznych bądź skażenia określonego terenu. Przykładowo do ataku na system sieci energetycznej doszło w Stanach Zjednoczonych w kwietniu 2009 roku, wówczas to hakerzy z Rosji oraz Chin złamali zabezpieczenie systemu obsługującego sieć i zostawili w nim szkodliwe oprogramowanie. Jego uruchomienie miało skutkować zakłóceniem pracy całego systemu zaopatrzenia w surowce energetyczne, energię oraz paliwa. Dodatkowo hakerzy byli również zainteresowani możliwościami dostania się do pozostałych elementów infrastruktury krytycznej Stanów Zjednoczonych. Działanie te dowiodły, że Stany Zjednoczone muszą podjąć liczne inicjatywy w zakresie zwiększenia ochrony infrastruktury krytycznej, ponieważ obecne działania są niewystarczające i narażają państwo na zbyt duży poziom zagrożenia dla jego bezpieczeństwa[424].

Te same parametry zagrożenia tyczą się energetycznych sieci dystrybucyjnych – zwłaszcza zagrożenia dla tych ostatnich wiążą się bezpośrednio z pojęciem bezpieczeństwa energetycznego. Nader często jest ono terminem rozumianym bardzo wąsko – tylko i wyłącznie jako stan, „w którym gospodarka danego państwa ma zapewniona niezbędną dla jej funkcjonowania i rozwoju podaż czynników produkcji, w tym wystarczalność energetyczną”[425]. Takie definiowanie (czysto gospodarcze, w którym najistotniejsze jest bezpieczeństwo surowcowe, a także finansowe) ogranicza znaczenie tego terminu i sprowadza je głównie do kosztów uzyskania energii oraz zapewnienia ciągłości dostaw.[426] Warto jednak zauważyć, iż energia jest produktem bardzo specyficznym, ponieważ musi być dostępna w sposób ciągły, bez wyjątku, także w sytuacji kryzysów politycznych, ekonomicznych czy nawet militarnych. Brak płynności w dostawach energii wiąże się z zagrożeniami dla całej gospodarki państwa czy wręcz grup państw i to nie tylko w zakresie ich stabilności gospodarczej, ale przede wszystkim zdrowia i życia obywateli. Sektor energetyczny odgrywa więc zasadniczą rolę nie tylko w kształtowaniu efektywności i konkurencyjności gospodarki, ale wpływa też (bezpośrednio i pośrednio) na kompleksowe funkcjonowanie społeczeństwa oraz systemu państwowego. Stąd też każdy atak cyberterrorystyczny, wymierzony w energetyczną infrastrukturę krytyczną, prowadzi nie tylko do

[424] Kowalewski J., Kowalewski M., *op. cit.*, s. 29.
[70.] Haliżak E., *Ekonomiczny wymiar bezpieczeństwa narodowego i międzynarodowego*, [w:] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, Warszawa 1997, s. 78 – 82.
[71.] Gradziuk A., Lach W., Poseł – Częścik E., Sochacka K., *Co to jest bezpieczeństwo energetyczne państwa?*, [w:] Dębski S., Górka –Winter B., [red.], *Kryteria bezpieczeństwa międzynarodowego państwa*, Warszawa 2003, s. 76.

zaburzenia bezpieczeństwa energetycznego w klasycznym, ekonomicznym rozumieniu tego terminu, ale pociąga za sobą realne, fizyczne zagrożenie dla państwa i jego obywateli.

Liczba ataków o charakterze cyberterrorystycznym, wymierzonych w bezpieczeństwo i stabilność sektora energetycznego, gwałtownie rośnie. Można by odnieść się do prostej korelacji, że ponieważ rośnie w ogóle liczba wszystkich cyberataków kwalifikowanych jako terrorystyczne, tendencja ta tyczy się również sektora energetycznego. Jednakże ataki na systemy i przedsiębiorstwa energetyczne, z uwagi na skalę i charakter potencjalnych szkód, które mogą wyrządzić, mają znaczenie szczególne i tak właśnie powinny być traktowane przez rządy, organizacje międzynarodowe i grupy państw. Według zespołu ICS-CERT (*Industrial Control System-Cyber Emergency Response Team*) Departamentu Bezpieczeństwa Wewnętrznego USA, odpowiedzialnego za reagowanie na incydenty komputerowe przeciwko energetycznej infrastrukturze krytycznej, w 2011 roku zanotowano 198 cyberataków, gdy tymczasem w roku poprzednim było ich zaledwie 49. Czterokrotny wzrost w skali zaledwie jednego roku musi dawać do myślenia. Co prawda w raporcie za rok 2014 odnotowano „tylko" 245 ataków skierowanych na urządzenia klasy ICS w sektorze energetyki i kluczowej produkcji (*Critical Manufacturing*), co wskazywałoby, że wzrost nie jest wprawdzie już tak dynamiczny, ale z pewnością nadal wyraźny. Warto też zwrócić uwagę na badania ICS-CERT przeprowadzone w roku 2013 wśród 150 przedsiębiorstw sektora energetycznego USA – aż 9% z nich poinformowało, że do prób atakowania ich systemów dochodzi niemal codziennie[427].

Duża podatność na cyberterroryzm występuje również w systemach łączności oraz sieci teleinformatycznych. W tym elemencie infrastruktury krytycznej wykorzystywane są systemy łączności ruchomej, które posiadają różnorodne zastosowania (zarówno publiczne jak i społeczne). Istotną rolę odgrywają również powszechne systemy komunikacyjne oraz systemy teletransmisyjne. Działania cyberterrorystów mogą doprowadzić do niedozwolonych i niepożądanych modyfikacji w ramach istniejących łączy telekomunikacyjnych, a także do przejęcia kontroli nad zarządzaniem aktywnymi sieciami. Efektem tego niszczącego zachowania mogą być różnorodne zjawiska o charakterze społecznym. Jednak najbardziej widocznym z nich będzie chaos oraz dezorganizacja[428].

[427] http://geopolityka.org/analizy/andrzej-kozlowski-cyberbezpieczenstwo-infrastruktury-energetycznej [dostęp: 03.06.2018]
[428] *Ibidem*, s. 30.

Bardzo dużym zainteresowaniem wśród terrorystów cieszą się systemy finansowe oraz bankowe. Sprawny przepływ pieniądza w dzisiejszych czasach jest bowiem elementem zapewniającym funkcjonowanie całej gospodarki i ciągłość określonych procesów ekonomicznych. Stąd też wielu cyberterrorystów rozważa zaatakowanie takich systemów, jak:

- systemy zarządzania papierami wartościowymi;
- system realizowania działań na rynku pieniężnym;
- systemy umożliwiające dokonywanie operacji na giełdzie papierów wartościowych;
- systemy nadzorowania pracy sieci bankomatów itp.[429].

Wspomniane systemy są szczególnie podatne na działalność cyberterrorystyczną, ponieważ istnieje możliwość zakłócenia ich pracy poprzez instalację szkodliwego oprogramowania. Omawiając podatność systemów finansowych i bankowych na zagrożenia ze strony cyberterroryzmów, należy wskazać na możliwość blokowania witryn internetowych banków oraz instytucji finansowych, a zatem blokować możliwość przyjmowania oraz realizacji zleceń o charakterze *online* czy korzystania z rachunków bankowych i/lub maklerskich. Efektem przedstawionych działań jest przede wszystkim brak dostępu do środków płatniczych, czyli w pewnym stopniu paraliż finansowy, którego długie trwanie może przyczynić się do konfliktów bądź kradzieży. Wynika to przede wszystkim z przypisywania szczególnej wartości i znaczenia społecznego pieniądzom, które – zdaniem jednostek ludzkich – są niezbędnym elementem życia codziennego. Trudno nie zgodzić się z tym twierdzeniem, ponieważ blokada pieniądza elektronicznego prowadzi do dezinformacji, paniki oraz niekorzystnych zmian o charakterze ekonomicznym[430].

Celem cyberterrorystów mogą stać się również systemy zaopatrzenia w żywność i w wodę, ponieważ w ich przypadku również można dostrzec znaczne zaawansowanie technologiczne, a skutki ataków będą odczuwalne przez ogromną ilość osób. Terroryści interesują się przede wszystkim:

- systemami produkcji żywności;
- systemami kontrolowania jakości żywności;
- systemami uzdatniania wody;
- systemami nadzorowania zaporami wodnymi itp.[431].

[429] *Ibidem*, s. 30.
[430] Świątkowska J. (red*.), op. cit.*, s. 18.
[431] *Ibidem*, s. 18.

Wysokiej jakości, nieskażona żywność oraz woda są niezbędne do przeżycia i utrzymania ciągłości gatunku ludzkiego. Skutki negatywnych transformacji w tym obszarze można dostrzec w najbiedniejszych państwach świata, gdzie głód i susza połączone z ogromną biedą przyczyniają się do powstawania licznych patologii, które od wewnątrz niszczą państwo. Patologie te stanowią realne zagrożenie także w przypadku państw rozwiniętych, gdzie dojdzie do niekontrolowanych zdarzeń uderzających w systemy zaopatrzenia w żywność i w wodę. Mowa tutaj o przejęciu kontroli nad sterowaniem zaporami wodnymi przez cyberterrorystów lub też wprowadzeniu pewnych przekłamań do systemów nadzorujących jakość żywności oraz zdatność wody do picia. Efektem takich działań mogą być zniszczenia infrastruktury, cierpienie ludzkie, ale także epidemie wywołane spożyciem skażonej wody lub żywności[432].

Kolejnym z wymienionych systemów, które są podatne na działania cyberterrorystów, jest system ratowniczy oraz ochrony zdrowia. Współczesne ratownictwo oraz medycyna korzystają z licznych technologii informacyjnych pozwalających na realizację określonych usług zdrowotnych, ale także przyjmowanie zgłoszeń o nagłych zdarzeniach czy komunikację pomiędzy ratownikami i/lub lekarzami. Mowa tu przede wszystkim o systemach informatycznych wspierających obsługę numerów alarmowych, na przykład, numeru 112, oraz o systemach komunikacji pomiędzy pracownikami służb medycznych. Umożliwiają one szybką reakcję i tym samym przyczyniają się do ochrony zdrowia ludzkiego. Nawet niewielka dezorientacja w ich przypadku może doprowadzić do licznych, negatywnych konsekwencji. Jako przykład można podać zakłócenie pracy centrów telekomunikacyjnych ratownictwa medycznego czy częstotliwości kanałów, za pośrednictwem których porozumieją się pracownicy medyczni w trakcie zamachu terrorystycznego na obiekt użyteczności publicznej na przykład stację metra. Ogrom zniszczeń w postaci ofiar ludzkich czy osób rannych byłby wówczas znacznie wyższy niż w przypadku natychmiastowej, sprawnie koordynowanej akcji ratunkowej. Dodatkowo zakłócenia wspomnianych systemów za sprawą działań cyberterrorystów mogą zmniejszyć poziom zaufania opinii publicznej do służby zdrowia[433].

System transportowy to kolejny, ważny element infrastruktury krytycznej, gdzie ataki cyberterrorystów mogą wpłynąć na poziom bezpieczeństwa całego państwa. Wśród obszarów,

[432] Mosadeghi R., *op. cit*., s. 196.
[433] *Ibidem*, s. 196.

które mogą stać się przedmiotem zainteresowania działań organizacji cyberterrorystycznych należy wymienić:

- systemy nadzorowania ruchu kolejowego,
- systemy kontrolowania sygnalizacji świetlnej,
- systemy kontrolowania ruchem drogowym[434].

Cyberterroryści mogą naruszyć sprawność funkcjonowania systemu transportowego poprzez manipulowanie komputerami, które odpowiadają za kontrolę szybkości lokomotyw czy innych środków transportu masowego. Przekroczenie obowiązujących limitów drogowych może doprowadzić do tragedii w ruchu lądowym. Dodatkowo przejęcie dostępu lub zakłócenie funkcjonowania systemu kontrolowania ruchem drogowym, na przykła poprzez zmianę świateł na skrzyżowaniach, przejściach dla pieszych, generowanie nieprawidłowych danych odnośnie natężenia ruchu drogowego, może zablokować komunikację w danym mieście. Chaos komunikacyjny sprzyja natomiast realizacji innych, bardziej drastycznych działań terrorystycznych, na przykład podkładaniu bomb w miejscach użyteczności publicznej, pojmowaniu zakładników czy szturmowaniu obiektów użyteczności publicznej[435].

Analizując podatność infrastruktury krytycznej na wpływ cyberterroryzmu, nie można zapomnieć o systemach zapewniających sprawność systemu funkcjonowania administracji publicznej. Bazują bowiem na rozbudowanych rejestrach publicznych, na przykład PESEL, REGON, KRS itp., sieciach teletransmisyjnych oraz systemach telekomunikacyjnych, które pozwalają na łączność bezprzewodową. Cyberterroryści mogą zaatakować ten element poprzez przerwanie integralności przetrzymywanych danych, wprowadzanie danych nieprawdziwych oraz za sprawą zakłóceń łączności przewodowej w ramach systemu telekomunikacyjnego. Oprócz strat w postaci danych może dojść do zmniejszenia poziomu zaufania wobec administracji publicznej, a także do wzrostu poziomu przestępczości. Utrudniony dostęp do baz danych wpłynie na sprawne weryfikowanie oraz wykrywanie sprawców przestępców[436].

Ostatnimi z elementów infrastruktury krytycznej, o których należy wspomnieć w kontekście działań cyberterrorystów, są systemy tworzenia, przechowywania oraz składowania substancji szkodliwych, na przyklad chemicznych, łatwopalnych, toksycznych itp. W tym obszarze cyberterroryści interesują się głównie systemami pomiarowymi oraz informującymi o

[434] *Ibidem,* s. 196.
[435] Świątkowska J. (red.), *op. cit*., s. 21.
[436] *Ibidem*, s. 21.

wystąpieniu potencjalnych zagrożeń, systemami rurociągów czy systemów nadzorujących przechowywanie, składowanie czy wykorzystanie substancji szkodzących. Mogą bowiem dokonywać przesterowań przy wykorzystaniu hakerskich oprogramowań lub też przejąć całkowitą kontrolę nad rurociągami, w których przesyłane są substancje niebezpieczne. Jeżeli dojdzie do wspomnianych zdarzeń, wówczas państwo narażone jest na skażenie ekologiczne, niszczące faunę i florę znajdujące się w pobliżu[437].

Wymienione przykłady zwracają uwagę na szczególną podatność infrastruktury krytycznej państwa na działania cyberterrorystów. Pomimo tego, że dotychczas większość z osób obawiało się tradycyjnych działań terrorystów, które sprowadzały się do wykorzystywania przemocy wobec jak największej liczby niewinnych jednostek, współcześnie coraz większym zagrożeniem jest dezorganizacja życia ludzkiego i ataki na infrastrukturę krytyczną poprzez działania wymierzone wobec technologii informacyjnej. Współczesne systemy bezpieczeństwa państw opierają się bowiem na zaawansowanych rozwiązaniach technologicznie, które często wywodzą się z powiązanych ze sobą systemów infrastruktury krytycznej.

[437] *Ibidem,* s. 22.

Rozdział VII
Problemy ochrony infrastruktury krytycznej RP przed zagrożeniami cyberterrorystycznymi

7.1. Problemy definicyjne pojęcia infrastruktury krytycznej

W Polsce zagadnienie infrastruktury krytycznej definiuje *Ustawa z dnia 27 kwietnia 2007 roku o zarządzaniu kryzysowym*, gdzie w artykule 3 ust. 2 określono, iż jako infrastrukturę krytyczną należy „rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców”[438].

W regulacjach prawnych Rzeczpospolitej Polskiej termin „ochrona infrastruktury krytycznej” to zespół przedsięwzięć organizacyjnych realizowanych w celu zapewnienia funkcjonowania lub szybkiego odtworzenia infrastruktury krytycznej w przypadku zagrożeń, w tym awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

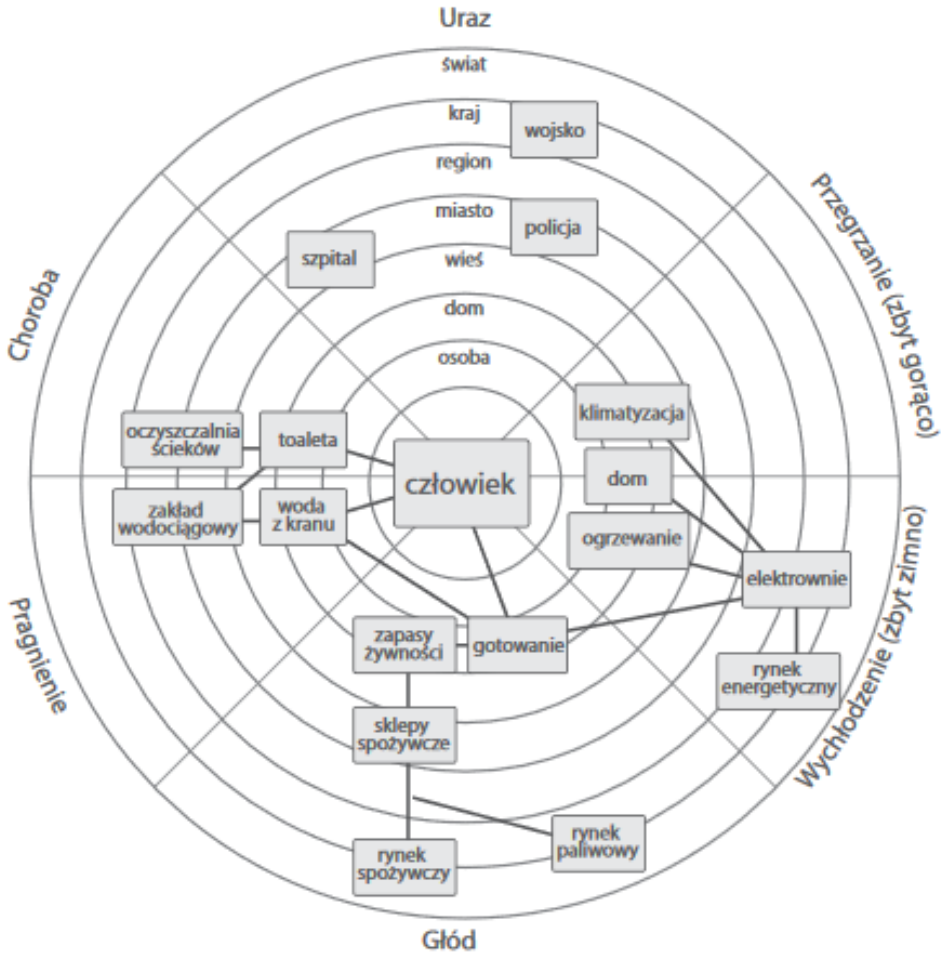
W ustawie o zarządzaniu kryzysowym (art. 3 ust. 3 ustawy) definicja OIK sformułowana została jako „[...] „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie”[439].

Jednolite i kompletne zdefiniowanie pojęcia infrastruktury krytycznej, realizowane na poziomie dokumentów strategicznych, nie jest możliwe w ujęciach teoretycznych i badawczych. W wielu definicjach akcentuje się bowiem nie tyle systemowość jej elementów, co ich znaczenie społeczne oraz psychologiczne. Nie sposób nie wspomnieć więc o pojęciu potrzeb, w perspektywie której infrastrukturę krytyczną w warunkach współczesnego państwa należy uznać za jeden z absolutnie podstawowych elementów zapewniających zaspokojenie potrzeb jego obywateli. Uznane klasyczne ujęcie Abrahama Maslowa wyszczególniające pięć grup potrzeb (fizjologiczne, bezpieczeństwa, miłości i przynależności, szacunku i uznania oraz samorealizacji),

[438] *Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz.U. 2007 nr 89 poz. 590.
[439] *Ibidem.*

uzupełnione o koncepcję Andrzeja Luszniewicza wyróżniającą siedem grup (wyżywienie, osłona (mieszkanie, odzież, obuwie), ochrona zdrowia, wykształcenie, rekreacja (czas wolny i jego wykorzystanie), zabezpieczenie społeczne i zagospodarowanie materialne), pozwala stwierdzić, iż usługi zapewniane przez niezakłócone działanie infrastruktury krytycznej zaspokajają większość z wymienionych potrzeb. Za kluczowe zadanie infrastruktury krytycznej należy uznać jednak zarówno zaspokojenie tychże, jak i ochronę przed skutkami ich niezaspokojenia – a do skutków tych należy niewątpliwie zaliczyć zagrożenie zdrowia i życia ludzkiego. Ujęcie to dobrze ilustruje mapa infrastruktury krytycznej, która odwołuje się do koncepcji 6WTD (ang. *6 ways to die*), czyli sześciu powodów, dla których życie ludzkie może zostać zagrożone. Schemat przedstawia rysunek 3.

Rysunek 3. Schemat infrastruktury krytycznej oraz tworzących ją poziomów



Źródło: M. Bennett, V. Gupta, *Dealing in Security understanding vital services and how they keep you safe.*

Warto zauważyć, że rysunku zwraca jedynie uwagę na aspekt społeczny, pomijając odniesienia do fizyczności i struktury materialnej infrastruktury krytycznej, która ma w istocie decydujące znaczenie dla realizacji podstawowych funkcji przypisywanych państwu. Przedstawiona mapa pozwala więc zauważyć, że autorzy w odmienny sposób mogą podchodzić do pojęcia infrastruktury krytycznej – w sposób częściowy bądź całościowy[440]. Obecnie coraz większa liczba teoretyków skłania się do prezentowania drugiego podejścia. Zmiana perspektywy wynika z różnych uwarunkowań, ale przede wszystkim z przekształcenia ogólnoświatowego sposobu postrzegania bezpieczeństwa państwa i jego obywateli po zamachach z września 2001 roku. Doszło wówczas do drastycznej redefinicji zagrożeń infrastruktury krytycznej oraz przeformułowania spojrzenia na możliwości jej ochrony[441] – cyberterroryzm oraz inne zagrożenia asymetryczne jedynie potęgują wrażenie wszechobecności czynników negatywnego wpływu na bezpieczeństwo.

Tylko nakreślenie wzajemnych relacji pomiędzy systemami infrastruktury krytycznej w ujęciu fizycznym, a zapewnianymi przez nie poziomami zaspokojenia potrzeb państwa i jego obywateli (oraz ochrony przed skutkami ich nie zaspokojenia) pozwala na zdefiniowanie kompletnego i pełnego pojęcia infrastruktury krytycznej.

Przytoczona powyżej definicja infrastruktury krytycznej obowiązująca w Polsce nie odbiega w znaczący sposób od ujęć definicyjnych w innych krajach EU, jak i USA. W przeważającej ich większości wskazuje się, iż zakres pojęciowy obejmuje takie systemy, obiekty czy sieci, których zniszczenie czy zakłócenie ich działania wywołałoby duże skutki dla państwa i jego obywateli. Niemniej jednak warto zwrócić uwagę na te definicje, w których ujęto społeczne aspekty pojęcia bezpieczeństwa rozumianego właśnie jako stan świadomości społecznej, a nie jedynie jako wynik procesu zapewniania niezakłóconego funkcjonowania fizycznych elementów systemów infrastruktury krytycznej. Jacek Milewski uważa na przykład, że infrastruktura krytyczna może być definiowana „jako urządzenia, instytucje usługowe, a także inne dziedziny, które mają istotny wpływ na poczucie bezpieczeństwa obywateli i sprawne funkcjonowanie gospodarki państwa”[442]. Jego ujęcie zwraca więc uwagę na rolę sprawnego funkcjonowania infrastruktury krytycznej we współczesnym państwie dla „poczucia bezpieczeństwa” – a zatem

[440] *Ibidem*, s. 17.
[441] *Ibidem*, s. 17.
[442] Milewski J., *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, „Zeszyty Naukowe Akademii Obrony Narodowej”, nr 4(105), 2016, s. 99.

stanu psychicznego niekoniecznie jednoznacznie tożsamego z bezpieczeństwem jako zasadą w ujęciu materialnym.

Na istotę społecznego ujęcia definicji infrastruktury krytycznej zwracają także uwagę Anna Dziurny, Sylwester T. Kurek oraz Zenon Stachowiak. Badacze ci zauważają, że o charakterze systemu infrastruktury krytycznej stanowi jej „służebny charakter: świadczy ona usługi produkcyjne i konsumpcyjne, nie może funkcjonować sama dla siebie, urządzania ją tworzące są niepodzielne, jej funkcjonowanie musi być kompleksowe, jej tworzenie i funkcjonowanie wymaga ponoszenia dużych nakładów, […] jest nieprzenośna i trwale związana z danym terenem, jest komplementarna, co oznacza, że jej poszczególne urządzenia się uzupełniają, a nie zastępują”[443].

Cécilia Gallais i Eric Filiol w eseju *Critical Infrastructure: Where we Stand Today*?[444] wskazują na dwa brakujące elementy w narodowych definicjach infrastruktury krytycznej: pomijanie aspektu ludzkiego oraz brak odniesienia do jej politycznego i społecznego kontekstu. Ich zdaniem – podzielanym także przez interdyscyplinarny zespół autorski Raportu Instytutu Kościuszki *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny* z 2015 roku[445], przy definiowaniu infrastruktury krytycznej, a zatem wynikowo również przy określeniu systematyki jej kwalifikacji – nie można pominąć aspektu socjologiczno-społecznego.

Zdaniem wspomnianych autorów, żadna z aktualnych definicji nie wspomina o ludziach jako bardzo istotnej części infrastruktury krytycznej, choć przecież „są oni niezbędni do funkcjonowania każdej infrastruktury bez względu czy uznaje się jej krytyczność czy też nie”. Podobnie nie uwzględniają one także otoczenia gospodarczo-technicznego systemów infrastruktury krytycznej, a są nimi z jednej strony zależność od zewnętrznych podmiotów (podwykonawców, dostawców, centrów danych itp.), z drugiej – zależność od innych systemów infrastruktury krytycznej. W efekcie „autorzy jako istotną konsekwencję tego ujęcia wskazują nazbyt wąskie postrzeganie infrastruktury krytycznej jako całkowicie wyizolowanej struktury”. Proponują zatem definicję własną oddającą szerokie ujęcie zagadnienia – zdaniem autora aktualnie najbardziej kompletną spośród znanych mu definicji infrastruktury krytycznej. W ujęciu

[443] Dziurny A., Kurek S. T., Stachowiak Z., *Infrastruktura krytyczna w modelu bezpieczeństwa publicznego*, „Polskie Stowarzyszenie Zarządzania Wiedzą. Seria: Studia i Materiały”, nr 33, 2010, s. 40-41.
[444] Gallais C., Filiol E., *Critical Infrastructure: Where we Stand Today?* http://www.tevalis.fr/images/ArticleICCWS2014.pdf, [dostęp: 25.02.2019]
[445] Pyznar M., Abgarowicz G., Wiercińska-Krużewska A, Gajek P., Świątkowska J., Dziwisz D., Ryba M., Poniewierski A, Kotłowski W i inni, *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny,* Kraków 2015, s. 17

zatem Gallais i Filiola infrastrukturą krytyczną „mogą być przedsiębiorstwa, instytucje lub organizacje z poziomu regionalnego, krajowego lub międzynarodowego, których zakłócenie działania, uszkodzenie lub zniszczenie miałoby poważny wpływ na zdrowie, bezpieczeństwo lub dobrobyt gospodarczy obywateli lub efektywne funkcjonowanie rządów i innej zależnej od niej infrastruktury. Zawiera ona w sobie ludzi, których skorumpowanie, wykluczenie lub śmierć może prowadzić do zakłócenia jej działania". Ponadto obejmuje ona:

- „instalacje (dostęp, budynki, teren itp.),
- wyposażenie (komputer, drukarka, dysk twardy itp.),
- zasoby, zarówno fizyczne jak i naturalne,
- sieci fizyczne (elektryczna, wodociągowa itp.) i wirtualne (Intranet, Internet itp.),\
- dane, zarówno fizyczne, jak i wirtualne (poufne dane, takie jak hasła lub kody dostępu, procedury, schemat organizacyjny itp.),
- obiekty sektora technologii informacyjno-komunikacyjnych,
- usługi,
- procesy,
- aktywa, w tym wizerunek,
- systemy lub ich części,
- inną infrastrukturę, z którą istnieją połączenia (np. dostawcy usług lub produktów), a których zakłócenie, uszkodzenie, kradzież lub zniszczenie miałoby poważny wpływ na zdrowie, bezpieczeństwo lub dobrostan pracowników lub skuteczne funkcjonowanie infrastruktury krytycznej. […] Elementy te można także znaleźć w otoczeniu politycznym i kulturalnym infrastruktury".

Zastosowanie tak szerokiej definicji, która z badawczego punktu widzenia wydawać się może kompletna, nie wydaje się jednak łatwe czy wręcz możliwe na poziomie praktycznym. Niemniej jednak (choć z poglądem o nieobecności wskazanych czynników ludzkiego i otoczenia społeczno-politycznego nie sposób zgodzić się w sposób bezkrytyczny – jak wskazano, część definicji infrastruktury krytycznej jednak elementy takie uwzględnia)[446], spostrzeżenia te

[446] Poza cytowanymi w pracy definicjami, na przykład w „Narodowym Programie Ochrony Infrastruktury Krytycznej" określenie otoczenia IK, w tym wynikających z niego zależności i współzależności, stanowi element oceny ryzyka, a aspekt ludzki wskazywany jest w każdym z rodzajów ochrony IK - § 4 Rozporządzenie Rady Ministrów z 30.04.2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U.10.83.54) https://www.prawo.pl/akty/dz-u-2010-83-541,17619033.html, załącznik nr 2, str. 30. [dostęp: 25.02.2019]]

pozwalają zauważyć, iż proces identyfikowania elementów infrastruktury krytycznej zawiera w sobie kilka istotnych wyzwań.

Pierwsze z nich określić można by jako problem właściwego rozróżnienie od siebie elementów infrastruktury, które z punktu widzenia państwa mają wysoki stopień krytyczności, od takiej infrastruktury, która może mieć kluczowe znaczenie na szczeblu lokalnym lub regionalnym, nie wymaga jednak centralnej interwencji w zakresie procedur jej ochrony. Kwestia problemów systematyki identyfikacji elementów infrastruktury krytycznej będzie omówiona w dalszej części rozdziału, niemniej jednak już na tym etapie nie sposób nie dostrzec zależności pomiędzy samym definiowaniem infrastruktury krytycznej, a bezpośrednio wynikającą z niego kwestią identyfikacji jej elementów. Bowiem „próba wyłonienia zasobów [infrastruktury krytycznej], bazująca jedynie na skonfrontowaniu jej z definicją, biorąc pod generalny charakter tych definicji, obarczona byłaby zbyt dużą niepewnością co do końcowego rezultatu. Dlatego najczęściej stosowane są tzw. kryteria przekrojowe, dotyczące skutków zniszczenia lub zakłócenia funkcjonowania danego obiektu, usługi czy operatora. Kryteria te z reguły korespondują z definicją infrastruktury krytycznej i wskazanymi w niej obszarami zaangażowania państwa oraz możliwościami reakcji państwa na skutki zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej”[447]. Autorzy cytowanego *Raportu*… Instytutu Kościuszki zauważają także, iż „proces definiowania dodatkowo rodzi poważne konsekwencje związane z ochroną zebranych w ten sposób informacji, które często obejmują nie tylko wykaz elementów infrastruktury krytycznej, ale również informacje dotyczące sposobów jej ochrony”[448]. Nie bez znaczenia pozostaje też fakt, iż szerokie ujęcie zakresu infrastruktury krytycznej czyni praktycznie niemożliwym nie tylko jej ochronę, ale także stawia pod znakiem zapytania realność jej prawidłowej identyfikacji w zasobach państwa. Bardzo trudne staje się bowiem opracowanie komplementarnej definicji, która może być skutecznie wykorzystana do określenia poszczególnych elementów infrastruktury. Tym samym trudności definicyjne pojęcia infrastruktury krytycznej mają, w ocenie autora, istotny wpływ na zdolność państwa do zapewnienia bezpieczeństwa systemom IK.

[447] *Ibidem*, s. 20.
[448] Pyznar M., Abgarowicz G. i inni*, op. cit.*, s. 18

7.2. Definicja infrastruktury krytycznej jako czynnik warunkujący skuteczność jej identyfikacji i ochrony

Ustawa z dnia 27 kwietnia 2007 roku o zarządzaniu kryzysowym będąca podstawą prawną ochrony infrastruktury krytycznej w Polsce określa, iż w jej skład wchodzi jedenaście systemów:

a) zaopatrzenia w energię, surowce energetyczne i paliwa,

b) łączności,

c) sieci teleinformatycznych,

d) finansowe,

e) zaopatrzenia w żywność,

f) zaopatrzenia w wodę,

g) ochrony zdrowia,

h) transportowe,

i) ratownicze,

j) zapewniające ciągłość działania administracji publicznej[449]

Tymczasem, jak zauważył już w roku 2010 Ryszard Radziszewski, analizując elementy infrastruktury krytycznej wymienione w tej ustawie – „w krajowym ustawodawstwie można znaleźć jej odpowiedniki, określone jako: „obiekty podlegające obowiązkowej ochronie" oraz „obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa"[450]. Mowa tutaj o art. 5 *Ustawy z dnia 22 sierpnia 1997 roku o ochronie osób i mienia*[451] oraz o par. 1. ust. 1 *Rozporządzenia Rady z dnia 24 czerwca 2003 roku w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony*[452]. Poddając tę kwestię analizie porównawczej, można wyróżnić następujące zapisy w wymienionych powyżej aktach prawnych:

- W *ustawie z dnia 22 sierpnia 1997 roku o ochronie osób i mienia* określono, iż „obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa podlegają obowiązkowej ochronie przez specjalistyczne uzbrojone formacje

[449] http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/U/D20070590Lj.pdf, [dostęp: 25.02.2019]
[450] Radziszewski R., *Ochrona infrastruktury krytycznej – uwarunkowania prawne,* [w:] Tyburska A. [red.], *infrastruktury krytycznej,* Szczytno 2010., s.98.
[451] http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140740, [dostęp: 25.02.2019]
[452] http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20031161090, [dostęp: 25.02.2019]

ochronne lub odpowiednie zabezpieczenie techniczne”[453], a następnie wymieniono następujące elementy infrastruktury:

1. „w zakresie obronności państwa:

– zakłady produkcji specjalnej oraz zakłady, w których prowadzone są prace naukowo-badawcze lub konstruktorskie w zakresie takiej produkcji;

– zakłady produkujące, remontujące i magazynujące uzbrojenie, urządzenia i sprzęt wojskowy;

– magazyny rezerw państwowych;

2. w zakresie ochrony interesu gospodarczego państwa:

– zakłady mające bezpośredni związek z wydobyciem surowców mineralnych o znaczeniu strategicznym;

– porty morskie i lotnicze; – banki i przedsiębiorstwa wytwarzające, przechowujące bądź transportujące wartości pieniężne w znacznych ilościach;

3. w zakresie bezpieczeństwa publicznego:

– zakłady, obiekty i urządzenia mające istotne znaczenie dla funkcjonowania aglomeracji miejskich, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi oraz środowiska, w szczególności elektrownie i ciepłownie, ujęcia wody, wodociągi i oczyszczalnie ścieków;

– zakłady stosujące, produkujące lub magazynujące w znacznych ilościach materiały jądrowe, źródła i odpady promieniotwórcze, materiały toksyczne, odurzające, wybuchowe bądź chemiczne o dużej podatności pożarowej lub wybuchowej;

– rurociągi paliwowe, linie energetyczne i telekomunikacyjne, zapory wodne i śluzy oraz inne urządzenia znajdujące się w otwartym terenie, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, środowiska albo spowodować poważne straty materialne;

4. w zakresie ochrony innych ważnych interesów państwa:

– zakłady o unikalnej produkcji gospodarczej– obiekty i urządzenia telekomunikacyjne, pocztowe oraz telewizyjne i radiowe”.

[453] http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140740, [dostęp: 25.02.2019]

W par. 5.3. określono następnie, jakie instytucje zajmują się przygotowaniem szczegółowego wykazu obszarów, obiektów, urządzenia i transportów podlegających obowiązkowej ochronie – wymieniono Prezesa Narodowego Banku Polskiego, Krajową Radę Radiofonii i Telewizji, ministrów, kierowników urzędów centralnych i wojewodów (w stosunku do podległych, podporządkowanych lub nadzorowanych jednostek organizacyjnych):

- Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 roku wprowadza pojęcie „obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa". W zapisach tego rozporządzenia są to:
- „zakłady produkujące, remontujące i magazynujące uzbrojenie i sprzęt wojskowy oraz środki bojowe, a także te, w których są prowadzone prace badawczo-rozwojowe lub konstruktorskie w zakresie produkcji na potrzeby bezpieczeństwa i obronności państwa; magazyny rezerw państwowych, w tym bazy i składy paliw płynnych, żywności, leków i artykułów sanitarnych;
- obiekty jednostek organizacyjnych podległych ministrowi obrony narodowej lub przez niego nadzorowanych;
- obiekty infrastruktury transportu samochodowego, kolejowego, lotniczego, morskiego i wodnego śródlądowego, drogownictwa, kolejnictwa i łączności oraz ośrodki dokumentacji geodezyjnej i kartograficznej;
- zapory wodne i inne urządzenia hydrotechniczne;
- obiekty jednostek organizacyjnych Agencji Wywiadu;
- obiekty: Narodowego Banku Polskiego oraz Banku Gospodarstwa Krajowego i Polskiej Wytwórni Papierów Wartościowych S.A. oraz Mennicy Państwowej S.A.;
- obiekty, w których produkuje się, stosuje lub magazynuje materiały jądrowe oraz źródła i odpady promieniotwórcze;
- obiekty telekomunikacyjne przeznaczone do nadawania programów radia publicznego i telewizji publicznej;
- obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw administracji publicznej lub przez niego nadzorowanych;
- obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw wewnętrznych lub przez niego nadzorowanych;
- muzea i inne obiekty, w których zgromadzone są dobra kultury narodowej;

- archiwa państwowe.
- obiekty jednostek organizacyjnych Agencji Bezpieczeństwa Wewnętrznego;
- obiekty Policji, Straży Granicznej i Państwowej Straży Pożarnej;
  obiekty znajdujące się we właściwości ministra sprawiedliwości, Służby Więziennej oraz jednostek organizacyjnych podległych lub nadzorowanych przez ministra sprawiedliwości;
- zakłady mające bezpośredni związek z wydobywaniem kopalin podstawowych;
  obiekty, w których produkuje się, stosuje lub magazynuje materiały stwarzające szczególne zagrożenie wybuchowe lub pożarowe;
- obiekty, w których prowadzi się działalność z wykorzystaniem toksycznych związków chemicznych i ich prekursorów, a także środków biologicznych, mikrobiologicznych, mikroorganizmów, toksyn i innych substancji wywołujących choroby u ludzi lub zwierząt;
- elektrownie i inne obiekty elektroenergetyczne;
- inne obiekty będące we właściwości organów administracji rządowej, organów jednostek samorządu terytorialnego, formacji, instytucji państwowych oraz przedsiębiorców i innych jednostek organizacyjnych, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa”[454].

Zgodnie z zapisami § 4.1 rozporządzenia, Rada Ministrów ustala wykaz obiektów uznanych za szczególnie ważne dla bezpieczeństwa i obronności państwa, a czyni to na wniosek: szefa kancelarii Prezesa Rady Ministrów, ministrów, Prezesa NBP, Prezesa BGK lub wojewodów.

Zauważyć zatem należy, że wszystkie trzy akty prawne określają obiekty, instalacje czy systemy wypełniające kryteria elementów infrastruktury krytycznej zarówno w rozumieniu Ustawy z dnia 27 kwietnia 2007 roku o zarządzaniu kryzysowym, jak i Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia[455] oraz o par. 1. ust. 1 *Rozporządzenia Rady Ministrów z dnia 24 czerwca 2003 roku*, co obrazuje tabela 13:

[454] http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20031161090, [dostęp: 25.02.2019]
[455] http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140740, [dostęp: 25.02.2019]

Tabela 13. **Zestawienie kryteriów identyfikacji elementów szczególnie istotnych**

Ustawa z dnia 22 sierpnia 1997 roku o ochronie osób i mienia	*Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 roku*	*Ustawa z dnia 27 kwietnia 2007 roku o zarządzaniu kryzysowym*
Obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa.	Obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa, ich kategorie, a także zadania w zakresie ich szczególnej ochrony oraz właściwości organów w tych sprawach.	Systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

Tabela 14, zestawiająca ze sobą elementy podlegające szczególnej ochronie, wymienione w każdym z trzech analizowanych dokumentów, wykazuje, iż każdorazowo ustawodawca ma na myśli te same obiekty, instalacje i systemy szczególnie istotne dla państwa i bezpieczeństwa publicznego.

Tabela 14. **Zestawienie katalogu elementów szczególnie istotnych w analizowanych dokumentach**

Ustawa z dnia 22 sierpnia 1997 roku o ochronie osób i mienia	*Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 roku*	*Ustawa z dnia 27 kwietnia 2007 roku o zarządzaniu kryzysowym*
- zakłady mające bezpośredni związek z wydobyciem surowców mineralnych o strategicznym znaczeniu dla państwa; - magazyny rezerw strategicznych, o których mowa w art. 15 *przechowywanie rezerw* ustawy z dnia 29 października 2010 r. o rezerwach strategicznych (Dz. U. z 2017 r. poz. 1846); - rurociągi paliwowe, linie energetyczne i telekomunikacyjne, zapory wodne i śluzy oraz inne urządzenia znajdujące się w	- magazyny rezerw państwowych, w tym bazy i składy paliw płynnych, żywności, leków i artykułów sanitarnych; - zapory wodne i inne urządzenia hydrotechniczne; - obiekty, w których produkuje się, stosuje lub magazynuje materiały jądrowe oraz źródła i odpady promieniotwórcze; - zakłady mające bezpośredni związek z wydobywaniem kopalin podstawowych; - elektrownie i inne obiekty elektroenergetyczne	zaopatrzenie w energię, surowce energetyczne i paliwa

otwartym terenie, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, środowiska albo spowodować poważne straty materialne		
- obiekty i urządzenia telekomunikacyjne, pocztowe oraz telewizyjne i radiowe	- obiekty telekomunikacyjne przeznaczone do nadawania programów radia publicznego i telewizji publicznej	łączność
- obiekty i urządzenia telekomunikacyjne, pocztowe oraz telewizyjne i radiowe	- obiekty telekomunikacyjne przeznaczone do nadawania programów radia publicznego i telewizji publicznej	sieci teleinformatyczne
- banki i przedsiębiorstwa wytwarzające, przechowujące bądź transportujące wartości pieniężne w znacznych ilościach;	- obiekty Narodowego Banku Polskiego oraz Banku Gospodarstwa Krajowego; - obiekty Polskiej Wytwórni Papierów Wartościowych S.A. oraz Mennicy Państwowej S.A.;	systemy finansowe
- obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi ujęte w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej	- magazyny rezerw państwowych, w tym bazy i składy paliw płynnych, żywności, leków i artykułów sanitarnych	zaopatrzenie w żywność
- zakłady, obiekty i urządzenia mające istotne znaczenie dla funkcjonowania aglomeracji miejskich, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi oraz środowiska, w szczególności elektrownie i ciepłownie, ujęcia wody, wodociągi i oczyszczalnie ścieków	- zapory wodne i inne urządzenia hydrotechniczne	zaopatrzenie w wodę
- zakłady, obiekty i urządzenia mające istotne znaczenie dla funkcjonowania aglomeracji miejskich, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi oraz środowiska, w szczególności elektrownie i ciepłownie,	- inne obiekty będące we właściwości organów administracji rządowej, organów jednostek samorządu terytorialnego, formacji, instytucji państwowych oraz przedsiębiorców i innych jednostek organizacyjnych, których zniszczenie lub uszkodzenie może stanowić	ochrona zdrowia

ujęcia wody, wodociągi i oczyszczalnie ścieków	zagrożenie dla życia i zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa	
- porty morskie i lotnicze; - rurociągi paliwowe, linie energetyczne i telekomunikacyjne, zapory wodne i śluzy oraz inne urządzenia znajdujące się w otwartym terenie, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, środowiska albo spowodować poważne straty materialne	- obiekty infrastruktury transportu samochodowego, kolejowego, lotniczego, morskiego i wodnego śródlądowego, drogownictwa, kolejnictwa i łączności oraz ośrodki dokumentacji geodezyjnej i kartograficznej; - zapory wodne i inne urządzenia hydrotechniczne	transport
- zakłady, obiekty i urządzenia mające istotne znaczenie dla funkcjonowania aglomeracji miejskich, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi oraz środowiska, w szczególności elektrownie i ciepłownie, ujęcia wody, wodociągi i oczyszczalnie ścieków	- magazyny rezerw państwowych, w tym bazy i składy paliw płynnych, żywności, leków i artykułów sanitarnych; - zakłady produkujące, remontujące i magazynujące uzbrojenie i sprzęt wojskowy oraz środki bojowe, a także zakłady, w których są prowadzone prace badawczo-rozwojowe lub konstruktorskie w zakresie produkcji na potrzeby bezpieczeństwa i obronności państwa; - obiekty, w których prowadzi się działalność, z wykorzystaniem toksycznych związków chemicznych i ich prekursorów, a także środków biologicznych, mikrobiologicznych, mikroorganizmów, toksyn i innych substancji wywołujących choroby u ludzi lub zwierząt	ratownictwo
- obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi ujęte w jednolitym wykazie obiektów, instalacji, urządzeń i usług	- obiekty jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych; - obiekty jednostek organizacyjnych Agencji	zapewnienie ciągłości działania administracji publicznej

wchodzących w skład infrastruktury krytycznej	Wywiadu; - obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw administracji publicznej lub przez niego nadzorowanych; - obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw wewnętrznych lub przez niego nadzorowanych; - obiekty jednostek organizacyjnych Agencji Bezpieczeństwa Wewnętrznego; - obiekty Policji, Straży Granicznej i Państwowej Straży Pożarnej; - obiekty znajdujące się we właściwości Ministra Sprawiedliwości, Służby Więziennej oraz jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Sprawiedliwości	

W tabeli 15 zamieszczono wykaz instytucji, które w myśl zapisów analizowanych dokumentów mają w swoich kompetencjach przygotowanie wykazów elementów szczególnie istotnych dla państwa i bezpieczeństwa publicznego.

Tabela 15. **Wykaz instytucji sporządzających wykazy elementów szczególnie istotnych**

Ustawa z dnia 22 sierpnia 1997 roku o ochronie osób i mienia	*Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 roku*	*Ustawa z dnia 27 kwietnia 2007 roku o zarządzaniu kryzysowym*
1. Prezes Narodowego Banku Polskiego; 2. Krajowa Rada Radiofonii i Telewizji; 3. ministrowie; 4. kierownicy urzędów centralnych; 5. wojewodowie (w stosunku do podległych, podporządkowanych lub nadzorowanych jednostek organizacyjnych. Umieszczenie w wykazie	1. Szef Kancelarii Prezesa Rady Ministrów; 2. ministrowie i przewodniczący komitetów wchodzących w skład Rady Ministrów; 3. Prezes Narodowego Banku Polskiego; 4. Prezes Zarządu Banku Gospodarstwa Krajowego; 5. wojewodowie	Dyrektor Rządowego Centrum Bezpieczeństwa sporządza na podstawie szczegółowych kryteriów, o których mowa w ust. 2 pkt 3, we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy, jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy. W wykazie wyróżnia się także

określonego obszaru, obiektu lub urządzenia następuje w drodze decyzji administracyjnej)		europejską infrastrukturę krytyczną zlokalizowaną na terytorium Rzeczypospolitej Polskiej oraz europejską infrastrukturę krytyczną zlokalizowaną na terytorium innych państw członkowskich Unii Europejskiej, mogącą mieć istotny wpływ na Rzeczpospolitą Polską

Identyfikacja tych samych zasobów na podstawie trzech różnych aktów prawnych (z których żaden nie znosi poprzedniego ani nie jest też jego nowelizacją), przy odwołaniu się każdorazowo do innych organów jako odpowiedzialnych za proces sporządzenia wykazu elementów szczególnie istotnych, przyczynia się do braku właściwej klasyfikacji systemów infrastruktury krytycznej. Multiplikacja zapisów dotyczących identyfikacji zasobów IK nie zwiększa w żaden sposób zdolności administracji centralnej do zapewnienia skutecznej ochrony prawnej elementów ocenianych jako szczególnie istotne dla państwa – przeciwnie, sytuację tę należy ocenić jako wadę procesu legislacyjnego mogącą wywołać negatywne skutki dla bezpieczeństwa systemów infrastruktury krytycznej.

7.3. Metodologia rozwiązań regulacyjnych a zapewnienie cyberbezpieczeństwa systemów infrastruktury krytycznej w Polsce

Jako kolejne z wyzwań w procesie ochrony infrastruktury krytycznej można wskazać kwestię wyboru metodologii podejścia do identyfikacji jej zasobów, a wskutek tego zapewnienia bezpieczeństwa systemom określonym w procesie selekcji (zgodnie z zapisami *Ustawy z dnia 27 kwietnia 2007 roku o zarządzaniu kryzysowym)* jako elementy infrastruktury krytycznej.

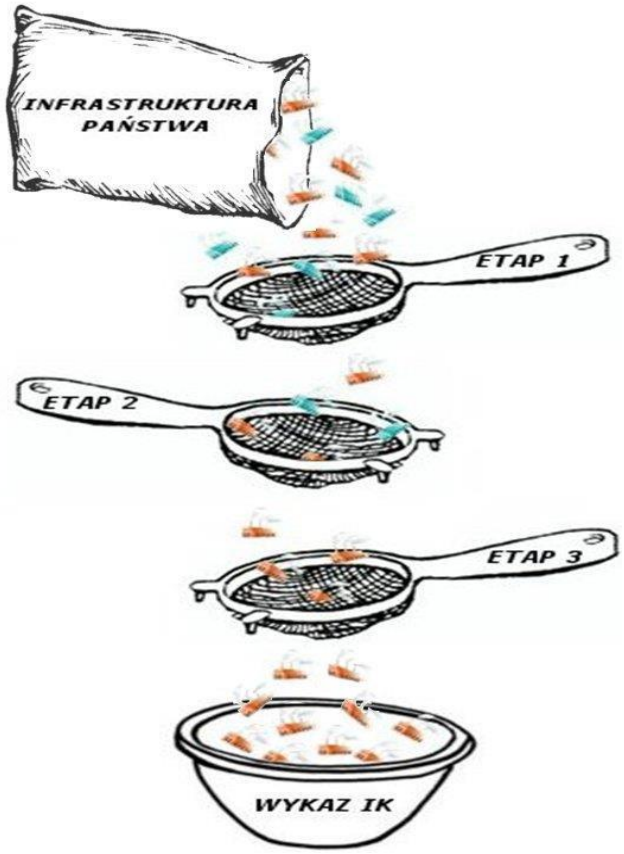
Odnosząc się do wzorów krajów europejskich, można wyróżnić przynajmniej dwie metody wyłaniania zasobów infrastruktury krytycznej – proceduralną oraz strukturalną. Metoda proceduralna to wyłanianie obiektów należących do IK na poziomie centralnym, natomiast podejście strukturalne zakłada zupełnie inną drogę – stałe dążenie do zmniejszania krytyczności infrastruktury. „Efekt ten można osiągnąć poprzez dalszą rozbudowę infrastruktury, tak by w konsekwencji doprowadzić do sytuacji celowej nadmiarowości (redundancji) lub poprzez przybliżanie, w sensie geograficznym, wybranej infrastruktury do obywatela. Koncepcja przybliżania zakłada wyposażanie jednostkowego obywatela lub mniejszych ich grup w

infrastrukturę pozwalającą na niezależność od usług dostarczanych przez bardziej oddaloną infrastrukturę. Tym samym, niektóre usługi stałyby się mniej krytyczne z punktu widzenia państwa, gdyż zwiększyłaby się odporność i niezależność tej grupy obywateli od IK. [Przykładami takiej „rozproszonej" infrastruktury są przed wszystkim indywidualne źródła energii, najczęściej odnawialne - elektrownie PV, turbiny wiatrowe itp.] Ten model zwiększa możliwości potencjalnej odpowiedzi służb państwowych na zakłócenie przybliżonej infrastruktury i kreuje stan, w którym liczba dotkniętych jednorazowo obywateli jest radykalnie mniejsza"[456]. „Postulowane (i stosowane) przez niektóre kraje (np. Francję) jako IK całych systemów (np. systemu elektroenergetycznego) lub nawet procesów wydaje się, na chwilę obecną, w polskich warunkach zbyt wyrafinowane. System (proces) rozumiany jako np. łańcuch zaopatrzenia może być realizowany w wielu lokalizacjach i mieć wielu właścicieli. Zrodziłoby to określone problemy, w tym także prawne. Podobnie wygląda kwestia zależności i współzależności. Obecnie łatwiej jest je wskazać dla konkretnego obiektu niż dla systemu czy procesu. Prawdopodobne jest jednak, że wraz z rozwojem systemu ochrony IK i dojrzałością jego uczestników będzie zachodzić zmiana w tym obszarze"[457].

W procesie identyfikacji krajowych zasobów infrastruktury krytycznej zastosowano podejście, które można by roboczo określić jako kierunkowe „z góry do dołu", choć autor jako bardziej odpowiedni uznaje raczej termin „scentralizowane". Polega ono bowiem na zastosowaniu jednolitych kryteriów do całej krajowej infrastruktury w celu oceny jej krytyczności. Systematykę klasyfikacji jej zasobów zawiera Narodowy Program Ochrony Infrastruktury Krytycznej[458], jeżeli chodzi natomiast o dobór kryteriów, zastosowane zostały zarówno kryteria sektorowe, jak i przekrojowe. W NPOIK do zobrazowania tego procesu wykorzystano następujący schemat – w ocenie autora dalece niewystarczający do przedstawienia zasad identyfikacji IK.

[456] *Ibidem*, s. 24.
[457] Pyznar M., Abgarowicz G. i inni*, op. cit.*, s. 22.
[458] *http://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf., s. 4,* dostęp: [25.02.2019]

Rysunek 4. **Schemat wyłaniania zasobów infrastruktury krytycznej**



Źródło: Narodowy Program Ochrony Infrastruktury Krytycznej

Zgodnie z zapisami Narodowego Programu Ochrony Infrastruktury Krytycznej procedura identyfikacji obejmuje:

- *Etap pierwszy* – w celu dokonania pierwszej selekcji obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za elementy infrastruktury krytycznej w danym systemie, do infrastruktury systemu należy zastosować kryteria systemowe, właściwe dla danego systemu infrastruktury krytycznej;
- *Etap drugi* – w celu sprawdzenia czy obiekt, urządzenie, instalacja lub usługa pełni kluczową rolę dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, do infrastruktury wyłonionej w etapie pierwszym należy zastosować definicję zawartą w art. 3 pkt 2 ustawy o zarządzaniu kryzysowym;

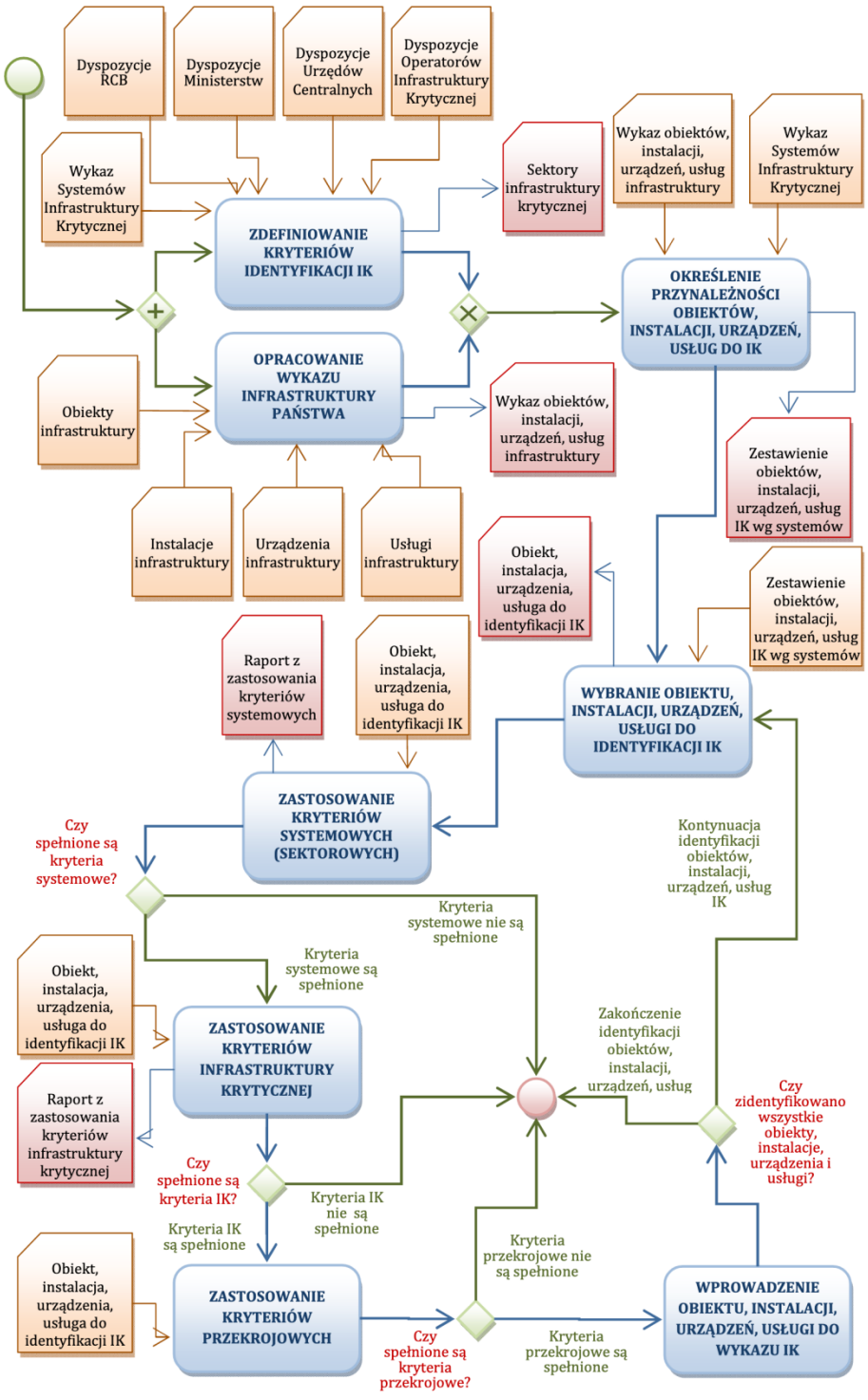
- *Etap trzeci* – w celu oceny potencjalnych skutków zniszczenia lub zaprzestania funkcjonowania potencjalnej infrastruktury krytycznej, do infrastruktury wyłonionej w etapie pierwszym i drugim należy zastosować kryteria przekrojowe, przy czym potencjalna infrastruktura krytyczna musi spełnić przynajmniej dwa kryteria przekrojowe[459].

Proces identyfikacji elementów infrastruktury krytycznej RP zatem możliwy jest dopiero po realizacji dwóch niezależnych od siebie czynności: zdefiniowania kryteriów identyfikacji infrastruktury krytycznej i opracowania wykazu infrastruktury krytycznej. Zdefiniowanie kryteriów identyfikacji zgodnie z zapisami *Ustawy z dnia 27 kwietnia 2007 roku o zarządzaniu kryzysowym* przyporządkowano dyrektorowi Rządowego Centrum Bezpieczeństwa – ustalane są one we współpracy z ministerstwami, urzędami centralnymi oraz operatorami infrastruktury krytycznej. Realizacja zadania stworzenia wykazu elementów infrastruktury krytycznej państwa ma pozwalać na zidentyfikowanie wszystkich obiektów, instalacji, urządzeń oraz usług mających kluczowe znaczenie dla niezakłóconego funkcjonowania państwa i społeczeństwa. Następnie – dopiero po stworzeniu katalogu zidentyfikowanych elementów infrastruktury krytycznej – możliwe jest określenie przynależności poszczególnych obiektów, instalacji, urządzeń oraz usług do systemów IK definiowanych przez ustawę o zarządzaniu kryzysowym.

Opracowanie kompletnego wykazu obiektów, instalacji, urządzeń oraz usług według przynależności do poszczególnych systemów stanowi podstawę do zastosowania kryteriów systemowych (sektorowych) w odniesieniu do każdego elementu z osobna. Na podstawie tego kryterium następuje przyporządkowanie obiektu, instalacji, urządzeń oraz usługi do konkretnego systemu infrastruktury krytycznej. Dopiero następnym zadaniem w procesie identyfikacji infrastruktury krytycznej jest zastosowanie kryteriów infrastruktury krytycznej, które mają wykazać, czy wskazane obiekty, instalacje czy systemy są kluczowe dla bezpieczeństwa państwa i jego obywateli. Ostatnim etapem identyfikacji elementów infrastruktury krytycznej jest prognozowanie skutków ich ewentualnego zniszczenia lub przerwy w funkcjonowaniu. Proces identyfikacji elementów infrastruktury krytycznej przedstawia rysunek 5:

[459] *Ibidem, s 4*. dostęp: [25.02.2019]

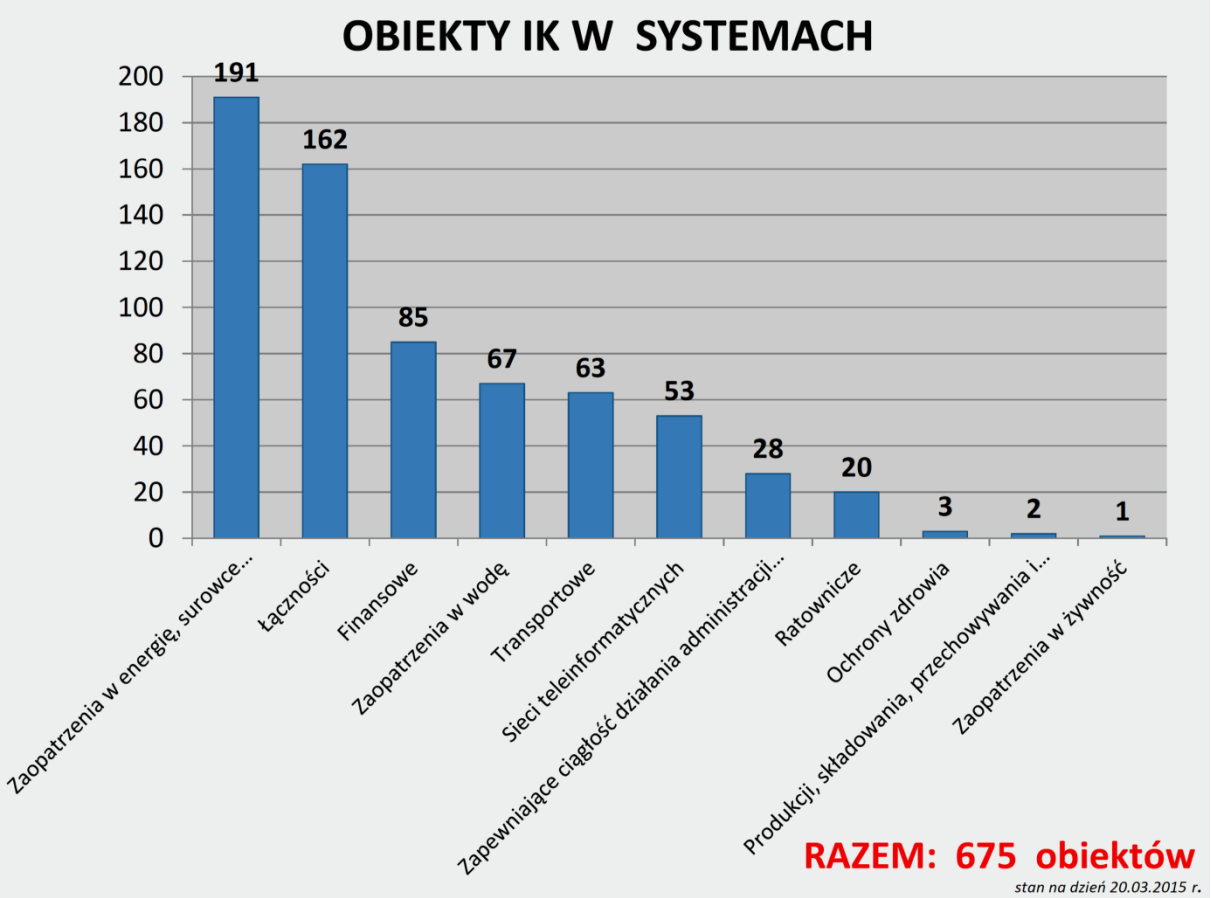
Rysunek 5. Proces identyfikacji elementów infrastruktury krytycznej



Jednakże, pomimo systemu identyfikacji opartego głównie na zakresie usług dostarczanych przez infrastrukturę (w istocie ocenie krytyczności podlegają właśnie te usługi), w

sporządzonym jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej znajdują się jednak przede wszystkim określone, fizyczne obiekty zarządzane przez konkretnych operatorów i posiadające konkretną lokalizację. Wykaz ten został opracowany w formie załącznika 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej[460]. Dane zbiorcze z 2015 roku przedstawia poniższy wykres:

Wykres 1. **Obiekty należące do infrastruktury krytyczne RP według kryteriów sektorowych**



Źródło: Narodowy Program Ochrony Infrastruktury Krytycznej

W ocenie autora przyjęty system identyfikacji elementów infrastruktury krytycznej może wywołać niekorzystne skutki dla bezpieczeństwa IK, z uwagi na zastosowane podejście „od góry do dołu", w którym przyporządkowanie fizycznego obiektu do zasobów infrastruktury krytycznej następuje w wyniku klasyfikacji usług. Skorelowane jest ono z przyjętym w ustawie o zarządzaniu kryzysowym oraz NPOIK rozumieniem infrastruktury krytycznej jako systemów, obiektów,

[460] https://rcb.gov.pl/wp-content/uploads/NPOIK-za%C5%82%C4%85cznik-1.pdf. [dostęp: 27.02.2019]

instalacji i usług, których zniszczenie lub zakłócenie funkcjonowania spowodowałoby poważne skutki dla bezpieczeństwa państwa i jego obywateli oraz sprawnego działania organów administracji publicznej, instytucji przedsiębiorców. W efekcie w wykazie elementów IK znajdują się tylko i wyłącznie obiekty spełniające kryteria (niejawne), opracowane przez dyrektora Rządowego Centrum Bezpieczeństwa, które ściśle wiążą pojęcie infrastruktury krytycznej z sytuacją kryzysową. Tym samym katalog obiektów należących do infrastruktury krytycznej – a więc podlegających szczególnej ochronie – jest bardzo nieliczny i zdecydowanie nie obejmuje wszystkich elementów infrastruktury narażonych na zniszczenie lub uszkodzenie w efekcie ataku z cyberprzestrzeni. Przyjęta kwalifikacja zasobów należących do infrastruktury krytycznej powoduje więc wykluczenie z ochrony wielu obiektów o wysokim stopniu krytyczności dostarczanych usług, a z uwagi na zastosowane technologie mogących stać się potencjalnym celem ataku o kaskadowych skutkach.

7.4. Niejasności dotyczące odpowiedzialności prawnej za bezpieczeństwo infrastruktury krytycznej

W Polsce wybrano rozwiązanie regulacyjne, które można określić jako metodę proceduralną (systemową), zakładające mianowicie obowiązkowy udział podmiotów w systemie ochrony infrastruktury krytycznej. W omawianych w poprzednim rozdziale zapisach ustawy o zarządzaniu kryzysowym[461] ustawodawcy zawarli obowiązki: „ochrony infrastruktury krytycznej przez jej właścicieli oraz posiadaczy samoistnych i zależnych, sporządzenia planu ochrony oraz wyznaczenia osoby do kontaktów z administracją”[462]. Ich zakres precyzuje *Rozporządzenie z dnia 30 kwietnia 2010 roku w sprawie planów ochrony infrastruktury krytycznej*[463]. „Rozporządzenie określa sposób tworzenia, aktualizacji oraz strukturę planów ochrony infrastruktury krytycznej przez właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej”[464], szczegółowo została też wskazana zawartość planów oraz tryb i terminy ich uzgadniania oraz zatwierdzenia.

Rozwiązanie systemowe (proceduralne), którego egzemplifikacją jest omawiane rozporządzenie, implikuje konkretne skutki dla skuteczności ochrony infrastruktury krytycznej

[461] § 13 *Rozporządzenie Rady Ministrów z 30.04.2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej* (Dz.U.10.83.54) https://www.prawo.pl/akty/dz-u-2010-83-541,17619033.html [dostęp: 28.02.2019]
[462] *Ibidem*.
[463] *Rozporządzenie Rady Ministrów z dn. 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej* (Dz. U. nr 83, poz. 542, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20100830542 [dostęp: 28.02.2019]
[464] *Ibidem*.

przed zagrożeniami. Co prawda, są one nieuniknioną konsekwencją przyjętego podejścia, zatem założyć należy, że ustawodawca był świadomy nieuchronności ich wystąpienia – niemniej jednak mają one determinujący wpływ na oczekiwaną skuteczność legislacji. Przyjęte rozwiązanie jest bowiem nakazowe wymuszające na stronę administracji centralnej powołanie i utrzymanie struktur, których zadaniem jest prowadzenie działalności kontrolnej oraz postępowań w przypadkach zaniedbania obowiązków stosowania procedur ochrony bezpieczeństwa infrastruktury krytycznej, zaś po stronie wykonawców (operatorów IK) niechęć do realizacji tychże. Można przyjąć, iż niechęć owa związana jest przede wszystkim ze znacznymi obciążeniami finansowymi dla operatorów.

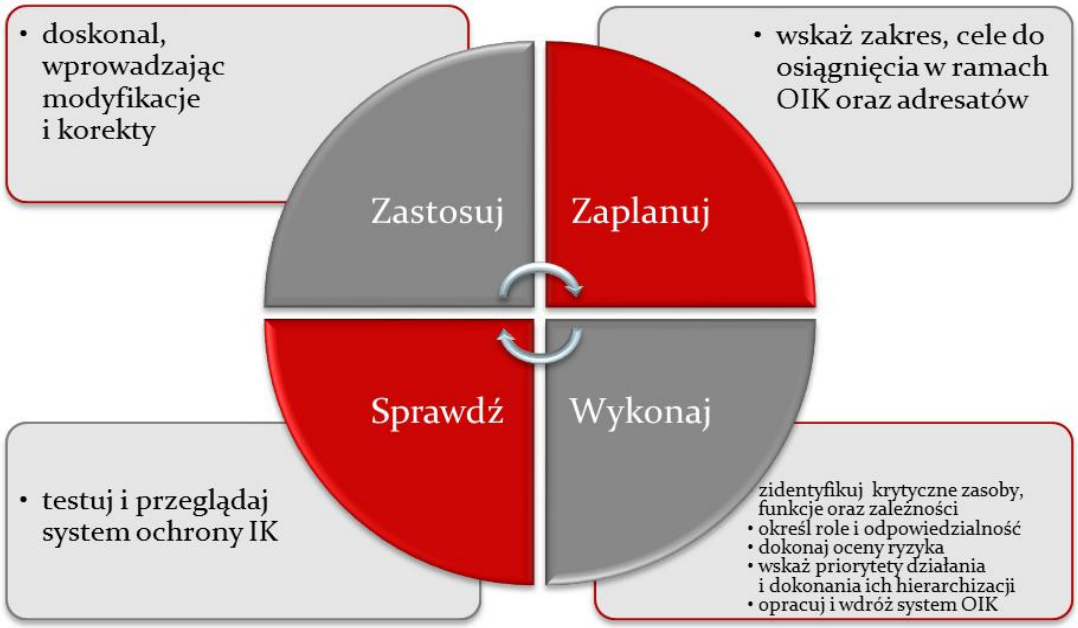
Warto zwrócić uwagę na fakt, iż w uchwale Rady Ministrów z dnia 9 kwietnia 2013 roku o przyjęciu *Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*[465] jej autorzy zauważają, iż „bezpieczeństwo infrastruktury krytycznej zaczyna mieć wymiar bezpieczeństwa narodowego, a dostęp do kluczowych usług pozostaje wymiernym aspektem bezpieczeństwa narodowego i obowiązkiem państwa w stosunku do obywatela […]”[466]. Ustawodawca dostrzega także fakt, że „aby ochrona infrastruktury krytycznej mogła być skuteczna, powinna stanowić wspólny wysiłek zarówno administracji rządowej, samorządowej, jak i operatorów oraz właścicieli. Ochrona infrastruktury krytycznej musi być zatem zadaniem jej właściciela lub operatora, natomiast rola państwa ogranicza się do funkcji koordynująco-nadzorującej. Interwencję dopuszcza się w przypadku, gdy dany element infrastruktury krytycznej nie jest dostatecznie chroniony lub gdy likwidacja skutków zaistniałej sytuacji kryzysowej przekracza możliwości danego właściciela lub operatora”[467]. Biorąc pod uwagę przyjęte w Polsce podejście do identyfikacji i ochrony systemów infrastruktury krytycznej, trudno uznać wyrażony w *Strategii* pogląd za możliwy do realizacji w praktyce.

W myśl zapisów cytowanej strategii „Narodowy Program Ochrony Infrastruktury Krytycznej” jest podstawowym dokumentem strategicznym dla stworzenia skutecznego systemu ochrony infrastruktury krytycznej. W intencji ustawodawcy NPOIK w kompleksowy sposób definiuje między innymi wizję i cele ochrony infrastruktury krytycznej, w tym kwestię odpowiedzialności za jej bezpieczeństwo. Założono, iż zapewnienie akceptowalnego poziomu

[465] Uchwała nr 67 Rady Ministrów z 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022ttp://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20130000377 [dostęp: 25.02.2019]
[466] *Ibidem,* s. 25.
[467] Ibidem.

bezpieczeństwa infrastruktury krytycznej jest procesem dynamicznym, długotrwałym, zakładającym stałe doskonalenie się jego uczestników. Proces ten przedstawiono za pomocą następującego schematu:

Rysunek 6. Proces realizacji programu ochrony infrastruktury krytycznej



Źródło: Narodowy Program Ochrony Infrastruktury Krytycznej

Przyjęcie takiego rozwiązania oparto na modelu systemu identyfikacji i ochrony infrastruktury krytycznej, obowiązującym w Republice Francuskiej[468], na który składają się następujące elementy:

- wyznaczenie na operatora IK i obowiązek jej ochrony,
- obowiązek sporządzenia Planu Bezpieczeństwa Operatora,
- sankcje dla operatorów IK nierealizujących narzuconych obowiązków,
- obowiązek sporządzenia przez administrację publiczną Zewnętrznego planu bezpieczeństwa.

[468] http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_stock_taking.pdf [dostęp: 28.02.2019]

Niemniej jednak bardzo poważną różnicą, mającą kluczowe znaczenie dla skuteczności ochrony infrastruktury krytycznej, jest określenie w systemie francuskim z jednej strony katalogu sankcji nakładanych na operatorów IK, z drugiej – znaczące wsparcie finansowe i organizacyjne państwa dla posiadaczy samoistnych i zależnych systemów infrastruktury krytycznej. W Polsce natomiast przekazując operatorom odpowiedzialność za bezpieczeństwo systemów, przyjęto podejście bezsankcyjne, ale nie zaoferowano im praktycznie żadnego wsparcia. Można domniemywać, że u podłoża tego podejścia znajdowało się założenie, że zwiększenie skuteczności ochrony może nastąpić jedynie poprzez działania operatorów wspieranych przez możliwości i potencjał administracji centralnej, niemniej jednak realizację tego poglądu oparto na systemie nakazowym, a nie motywacyjnym i premiującym. Z jednej strony słusznie uznano, że to właśnie operatorzy infrastruktury krytycznej mają największą wiedzę oraz kompetencje niezbędne do zwiększania poziomu bezpieczeństwa swoich systemów, ale z drugiej strony z tego właśnie powodu (jak można by uznać) nie są w żaden sposób wspierani ze środków budżetowych. To właśnie na operatorów IK spada obowiązek ponoszenia wszystkich kosztów związanych z obroną instalacji, na przykład przed atakiem cyberterrorystycznym.

Należy jednak zauważyć, że choć system ten został określony jako „bezsankcyjny", w istocie w owe sankcje wyposażony, o czym świadczy ten oto zapis: „właściciele oraz posiadacze samoistni i zależni, którzy świadomie niedopełniają obowiązku ochrony IK narażają pracowników i innych ludzi na bezpośrednie niebezpieczeństwo utraty życia albo ciężkiego uszczerbku na zdrowiu, mogące być skutkiem zakłócenia funkcjonowania IK, co jest zagrożone karą pozbawienia wolności do lat 3 (art. 160 § 1 Kodeksu karnego)"[469].

Szerokie możliwości interpretacyjne zapisu „świadome niedopełnienie obowiązku ochrony", jak i niesprecyzowanie, na czym właściwie polega ów „obowiązek ochrony" i dlaczego przy zasadzie dobrowolności obowiązek ten w ogóle istnieje, stawiają pod znakiem zapytania ową „bezsankcyjność" obowiązku ochrony infrastruktury krytycznej RP. Wprowadzone w NPOIK podejście do ochrony infrastruktury krytycznej polega w intencji autorów *Programu* na rozbudowanej współpracy, wzajemnym zaufaniu i współodpowiedzialności zainteresowanych stron, a także na stałym doskonaleniu się jego uczestników, jak i założeniu, iż dobrowolne

[469] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. 1997 Nr 88 poz. 553), http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU19970880553/U/D19970553Lj.pdf [dostęp: 25.02.2019]

działania operatorów IK zostaną aktywnie wsparte przez administrację centralną. Niemniej jednak po stronie administracji centralnej leży jedynie zaplanowanie zadań związanych z ochroną infrastruktury krytycznej w planach zarządzania kryzysowego na każdym poziomie administracji (w przypadku poziomów niższych niż krajowym warunkiem umieszczenia tych zadań jest występowanie IK na obszarze objętym planem[470]). Trudno uznać to za „aktywne wsparcie", wręcz można by zastanowić się, czy jest to jakiekolwiek wsparcie? Od operatorów obiektów infrastruktury krytycznej (w większości będących własnością sektora prywatnego) oczekuje się przecież dobrowolnego poniesienia dodatkowych kosztów niezbędnych dla zapewnienia bezpieczeństwa obiektów, a tym samym uznania nadrzędności interesów państwa nad rachunkiem zysków inwestora. Ochrona infrastruktury krytycznej, z punktu widzenia operatora będącego właścicielem i inwestorem konkretnego obiektu czy instalacji, postrzegana jest więc jako dodatkowy koszt bilansowy, zatem z jego punktu widzenia optymalizacja wydatków na bezpieczeństwo i ochronę jest zasadna z uwagi na zwiększenie zysku z inwestycji.

W ocenie autora konieczne więc staje się zwrócenie uwagi na następujące kwestie:

a) które z funkcjonujących zapisów za obowiązujące dla siebie powinni uznawać operatorzy IK: deklarowane „bezsankcyjne" podejście z NPOIK czy może jednak postanowienia ustawy o zarządzaniu kryzysowym oraz *Ustawy z dnia 22 sierpnia 1997 roku o ochronie osób i mienia*, które to dokumenty sankcję przewidują?

   Zdaniem autora odpowiedź na to pytanie winna być poprzedzona analizą zgodności Narodowego Programu Ochrony Infrastruktury Krytycznej z obowiązującym w Polsce prawem. Choć pkt 1.6 Narodowego Programu Ochrony Infrastruktury Krytycznej[12] określa, iż jest on zgodny z obowiązującymi aktami prawnymi i nie narusza postanowień żadnego z nich, to jednak, w ocenie autora tego opracowania, NPOIK w zakresie zapisu o „bezsankcyjności" narusza zarówno przepisy U*stawy z dnia 26.04.2007 roku o zarządzaniu kryzysowym,* jak i *Ustawy z dnia 22 sierpnia 1997 roku o ochronie osób i mienia*. Pomimo tego, iż załącznik do NPOIK zawierający katalog fizycznych obiektów wchodzących w skład infrastruktury krytycznej RP jest niejawny, należy założyć, iż znacząca większość obiektów należących do IK na mocy zapisów ustawy o zarządzaniu kryzysowym, to jednocześnie obiekty podlegające obowiązkowej ochronie w myśl

[470] *Art. 5 ust. 2 pkt 3 Ustawy z 26.04.2007 r. o zarządzaniu kryzysowym (Dz.U.07.89.590 z późn. zm.), http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id = WDU20070890590* – [dostęp: 25.02.2019]

zapisów ustawy o ochronie osób i mienia. Ustawa ta zaś określa, iż „niezapewnienie im należytej ochrony jest zagrożone sankcją z art. 48 – i podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2”[471]; natomiast w art. 6 ustawy o zarządzaniu kryzysowym zawarto zapis, iż „właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony”[472].W ocenie autora obecność w aktach prawnych wyższego rzędu cytowanych zapisów pozwala uznać je za jedynie właściwe do stosowania. Pomimo sprzeczności z „bezsankcyjnością” zawartą w postulatach NPOIK należy dostrzec, iż Narodowy Program Ochrony Infrastruktury Krytycznej nie jest aktem prawnym i pozostaje jedynie dokumentem o charakterze strategicznym, a jego zapisy nie mają mocy ustawy.

b) Autorzy *Narodowego Programu Ochrony Infrastruktury Krytycznej* dokonali (umiarkowanie samokrytycznej) identyfikacji słabości procedury nakładania na operatorów infrastruktury krytycznej obowiązków w drodze nakazowej, przy jednocześnie postulowanej „bezsankcyjności”. Uznano jednak to podejście za nietrafne jedynie „ze względu na realny brak możliwości prowadzenia audytu i kontroli ich realizacji. Mając to na uwadze, w działania z zakresu ochrony IK w większym stopniu należy zaangażować podmioty, które nią zarządzają – jednak nie jedynie w drodze nakazów, ale świadomego udziału w przedsięwzięciach mających na celu poprawę bezpieczeństwa systemów istotnych dla funkcjonowania społeczeństwa, poprzez intensyfikację współpracy sektora prywatnego i publicznego w tym zakresie”[473]. Czy jednak istotnie „brak możliwości przeprowadzenia audytu” jawi się jako największa słabość przyjętego podejścia do odpowiedzialności za ochronę systemów IK? Zdaniem autora piszącego te słowa, jest nią raczej rażąca systemowa niezgodność postulowanych rozwiązań nie tylko z obowiązującym prawem, ale zauważalna także niejako „wewnętrznie”, czyli na poziomie samych dokumentów strategicznych. Z jednej strony uznaje się bowiem ochronę IK za zadanie wspólne dla operatorów i administracji centralnej, z drugiej natomiast całość obowiązków spada na operatora IK, zaś funkcję

[471] http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140740, [dostęp: 25.02.2019]
36 *Art. 5 ust. 5 pkt 1 Ustawy z 26.04.2007 r. o zarządzaniu kryzysowym (Dz.U.07.89.590 z późn. zm.), http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id = WDU20070890590* – [dostęp: 25.02.2019]
[473] Uchwała nr 67 Rady Ministrów z 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022”, *op. cit*., s. 73

państwa ograniczono w istocie do nadzoru, nadzór ów oceniając jednocześnie jako trudny w realizacji z uwagi na „brak możliwości prowadzenia audytu i kontroli ich realizacji".

c) Autorzy *Narodowego Programu Ochrony Infrastruktury Krytycznej* zaznaczając, iż interwencja państwa jest dopuszczalna w sytuacji, gdy brak jest dostatecznej ochrony elementu infrastruktury krytycznej lub gdy usunięcie skutków zdarzenia niepożądanego przekroczy możliwości operatora, nie precyzują w żaden sposób kryteriów ani metody oceny czy sytuacja taka istotnie ma miejsce. Jeżeli procedurę przeprowadzenia audytu uznano za niemożliwą („realny brak możliwości"), nasuwa się pytanie, w jaki właściwie sposób administracja centralna dokona weryfikacji ochrony konkretnego elementu infrastruktury krytycznej? A także, jaki właściwie poziom ochrony uznawany jest za wystarczający i jakie są kryteria oceny tego poziomu? Próba odpowiedzi na to zagadnienie nasuwa jednak kolejne pytanie, czy „wystarczający poziom ochrony" jest tym samym w ocenie operatora IK oraz administracji państwowej?

d) Autorzy *Narodowego Programu Ochrony Infrastruktury Krytycznej* zapowiadając interwencję państwa w przypadku braku dostatecznej ochrony elementu infrastruktury krytycznej lub kiedy usunięcie skutków przekroczy możliwości operatora, w żaden sposób nie określają, jakie procedury zostaną wówczas wdrożone i jakimi środkami będą przeprowadzone? Czy będę one zmierzać jedynie do ukarania operatora, czy mają mieć charakter pomocowy? Jeśli tak, jaka będzie to pomoc i kto konkretnie będzie ją świadczył? Dodajmy, że odpowiedzi na te pytania operator powinien poznać znacznie wcześniej, niż dopiero w sytuacji realnego zagrożenia bezpieczeństwa zarządzanego przez siebie obiektu, bowiem, zgodnie z zapisami NPOIK[474], jego zadaniem jest przedstawienie w planie ochrony nie tylko „zasobów własnych", które będą „możliwe do wykorzystania w ochronie infrastruktury krytycznej", ale także „zasobów właściwych terytorialnie organów";

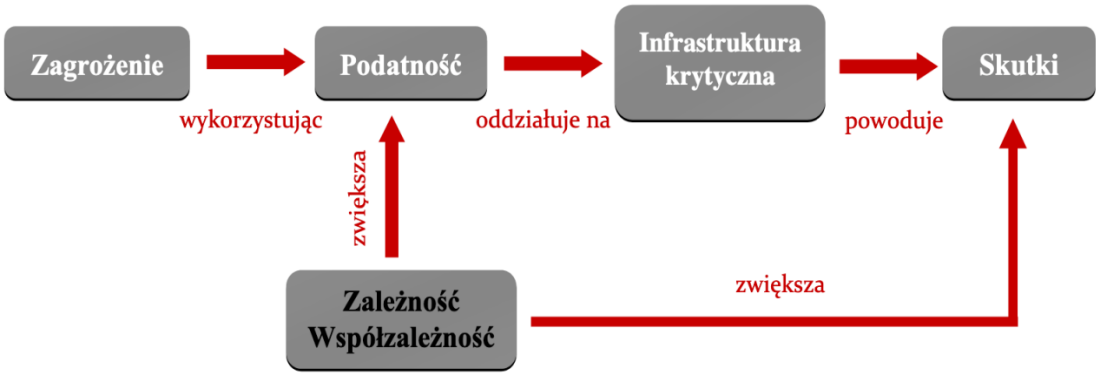
e) *Narodowy Program Ochrony Infrastruktury Krytycznej* określa także, iż wybór metod i rodzajów ochrony powinien być uzależniony „od oceny ryzyka zakłócenia funkcjonowania danej infrastruktury"[475]. W myśl zapisów NPOIK „ocena ryzyka powinna

[474] Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, D.U. nr 83, poz. 542, § 2 pkt c i d

[475] *Ibidem*, pkt. 4.2 s. 32

być podstawą określenia standardów ochrony IK i ustalenia priorytetów działań", co ilustrować ma poniższy schemat:

Rysunek 7. Proces oceny ryzyka zagrożenia obiektu infrastruktury krytycznej



Źródło: Narodowy Program Ochrony Infrastruktury Krytycznej

Ani powyższy schemat, ani też żaden z zapisów NPOIK, nie wyjaśniają jednakże, kto i w jaki sposób ma owo ryzyko oszacować. Można wnioskować, iż jest to zadanie operatora, jednakże ten nie ma dostępu do analiz wywiadowczych czy innych dokumentów rządowych, które określałby poziom zagrożenia konkretnego obiektu, na przykład atakiem cyberterrorystycznym. W celu określenia poziomu ryzyka niezbędna jest także znajomość powiązań, jakie występują pomiędzy konkretnymi elementami infrastruktury krytycznej, rozwiązaniami z zakresu technologii informacyjnych, z których korzystają, potencjalnymi zagrożeniami terrorystycznymi i innymi, o których wiedzę posiada administracja centralna oraz ich ewentualnymi skutkami[476];

f) warto w tym miejscu również postawić pytanie, dlaczego operatorzy IK nie mają praktycznie żadnego udziału w planowaniu procedur i doborze metod ochrony systemów, którymi zarządzają, i za które odpowiadają? I choć Trybunał Konstytucyjny potwierdził, „że w ustawie o zarządzaniu kryzysowym nie wprowadzono przepisów, które zawierałyby jakiekolwiek sankcje wobec tych zarządców infrastruktury krytycznej, którzy nie zastosują się do dyspozycji zawartych w przepisach ustawy i odmówią współpracy z

[476] Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki informacyjne", nr 1-2, 2014, s. 28.

administracją publiczną”[477], niemniej jednak sytuację taką (czyli odmowę współpracy) trudno uznać za prawdopodobną. Trudno także dostrzec w tym podejściu deklarowane w NPOIK, strategiach bezpieczeństwa RP i wielu innych dokumentach (omówionych szczegółowo w poprzednich rozdziałach) dążenie do większego udziału sektora społecznego i gospodarczego w procesie zapewnienia bezpieczeństwa infrastrukturze krytycznej. Partnerstwo publiczno-prywatne, będące postulowaną i wdrażaną podstawą ochrony infrastruktury krytycznej w Stanach Zjednoczonych, w Polsce rozumiane jest jedynie jako „rodzaj współpracy między jednostkami administracji publicznej a podmiotami prywatnymi, poprzez na przykład wymianę wszelkich informacji mogących mieć wpływ na osiągnięcie celów NPOIK. Takie partnerstwo nie przewiduje natomiast zawarcia jakiejkolwiek umowy, na podstawie której następowałaby realizacja za wynagrodzeniem przez partnera prywatnego przedsięwzięcia na rzecz podmiotu publicznego”[478].

Reasumując, przyjęte podejście do identyfikacji zasobów infrastruktury krytycznej oraz nakazowy i jedynie teoretycznie „bezsankcyjny” obowiązek uczestnictwa w systemie ochrony dla jej operatorów, bez zapewnienia im wsparcia finansowego ze strony państwa, można ocenić jako jeden z kluczowych problemów dla skuteczności zapewnienia bezpieczeństwa systemom IK. W ocenie autora do pogłębienia niejasności dotyczących obowiązku ochrony i odpowiedzialności za bezpieczeństwo systemów infrastruktury krytycznej w znaczniej mierze przyczyniają się niezgodne z obowiązującymi aktami prawnymi zapisy Narodowego Programu Ochrony Infrastruktury Krytycznej.

7. 5. Sektor elektroenergetyczny infrastruktury krytycznej jako szczególnie narażony na atak cyberterrorystyczny

W analizowanych dokumentach strategicznych i prawnych, związanych z ochroną infrastruktury krytycznej, wymienia się szereg systemów wchodzących w jej skład. Tymczasem poziom krytyczności poszczególnych systemów pozostaje różny. Wyrażane w dokumentach zalecenia i wskazania konieczności ochrony IK nie określają, które z tych systemów są nadrzędne

[477] *Wyrok Trybunału Konstytucyjnego z 21.04. 2009 r.,* sygn. akt K 50/07, http://prawo.sejm.gov.pl/isap.nsf/ DocDetails.xsp?id= WDU 20090650553 – [dostęp: 25.02.2019]

[478] Wiercińska-Krużewska A., Gajek P., *Prawne uwarunkowania ochrony infrastruktury krytycznej* [w:] *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny, Kraków 2015, s*. 32.

względem pozostałych jako najważniejsze dla funkcjonowania RP. W celu zrozumienia tej zależności istotne jest przedstawienie powiązań, jakie występują pomiędzy elementami infrastruktury krytycznej, rozwiązaniami z zakresu technologii informacyjnych, z których korzystają, potencjalnymi zagrożeniami terrorystycznymi oraz ich ewentualnymi skutkami[479].

W ocenie autora niniejszej pracy, popartej analizą dotychczas występujących zagrożeń cyberterrorystycznych, systemem najbardziej narażonym na ten rodzaj zagrożeń, a z drugiej strony takim, którego zaatakowanie będzie wyjątkowo szkodliwe dla państwa, jest sektor elektroenergetyczny.

Współczesny system elektroenergetyczny (SEE) funkcjonujący na terenie Rzeczpospolitej Polskiej jest zbiorem powiązanych ze sobą elementów służących do wytwarzania, przetwarzania, przesyłu i rozdziału energii elektrycznej oraz ośrodków dyspozytorskich sterujących pracą systemu. Zgodnie z *Rozporządzeniem Ministra Gospodarki z dnia 4 maja 2007 roku w sprawie szczegółowych warunków funkcjonowania systemu elektroenergetycznego* [Dz.U. 2007 Nr 93 poz.623], głównym celem systemu elektroenergetycznego jest niezawodne dostarczanie wytworzonej energii elektrycznej do odbiorców przy zachowaniu określonych wymagań i norm jakościowych.

Wytwórczy system energetyczny składa się z następujących elementów:

- elektrowni cieplnych kondensacyjnych, współpracujących synchronicznie z systemem elektroenergetycznym, wytwarzających tylko energię elektryczną pracujących na węglu kamiennym lub brunatnym. W elektrowniach z turbinami gazowymi czynnikiem roboczym są gazy, najczęściej spalinowe, wytwarzane w komorach spalania;
- elektrowni wodnych przepływowych i szczytowo-pompowych;
- elektrowni wykorzystujących energie odnawialne: wiatru i słońca;
- elektrociepłowni miejskich i przemysłowych wytwarzających energię elektryczną w skojarzeniu z wytwarzaniem energii cieplnej.

W skład systemu wytwórczego energii elektrycznej wchodzą:

a) elektrownie systemowe (zawodowe) – w Polsce funkcjonuje obecnie dziewiętnaście elektrowni tego typu, w których energia elektryczna wytwarzana jest ze spalania węgla

[479] Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki informacyjne", nr 1-2, 2014, s. 28.

brunatnego i węgla kamiennego. W elektrowniach tych produkowane jest 75% całości energii zużywanej w kraju. Do największych z tych elektrowni należą: Bełchatów, Opole i Turów oraz Połaniec, Kozienice, Rybnik i Dolna Odra.

b) Elektrociepłownie (EC), w których jednocześnie wytwarzana jest energia elektryczna i ciepło. W Polsce pracuje obecnie ponad pięćdziesiąt elektrociepłowni zlokalizowanych przy większych aglomeracjach miejskich, na przykład zlokalizowana w Warszawie i należąca do PGNiG Termika – Elektrociepłownia Żerań czy znajdująca się we Wrocławiu Kogeneracja.
c) Elektrociepłownie (tzw. przemysłowe) lokalizowane są również w obrębie większych zakładów przemysłowych. Obecnie funkcjonuje około 170 takich obiektów.

Z uwagi na to, iż system elektroenergetyczny to system rozległy terytorialnie obejmujący cały teren kraju oraz – co najistotniejsze – jest powiązany z systemami elektroenergetycznymi innych krajów odpowiednimi połączeniami transgranicznymi, jest on szczególnie narażony na atak cyberterrorystyczny. Wytwarzanie i przesyłanie energii elektrycznej odbywa się praktycznie jednocześnie, a z uwagi na bardzo wysokie koszty, praktycznie nie występuje możliwość magazynowania energii elektrycznej. Stąd każdy skuteczny atak na system elektroenergetyczny ma efekt kaskadowy. Co prawda, system elektroenergetyczny RP teoretycznie zapewnia dostawę energii elektrycznej do odbiorców również w czasie wyłączenia z ruchu określonej liczby uszkodzonych lub wymagających naprawy czy konserwacji elementów systemu, to jednak zabezpieczenie (rezerwa mocy) może okazać się niewystarczające w przypadku skutecznego ataku na dużą elektrownię zawodową czy jedną z głównych linii dystrybucyjnych najwyższych napięć. Również atak wymierzony w jeden z ważniejszych Głównych Punktów Zasilania (GPZ) może spowodować brak dostaw prądu na bardzo dużym obszarze. Z uwagi na brak możliwości magazynowania energii elektrycznej (w każdym razie na skalę strategiczną), konieczne dla sprawnego funkcjonowania państwa jest ciągłe i niezakłócone utrzymywanie w systemie odpowiednich stanów, konfiguracji i mocy źródeł, w celu zapewnienia bieżącego pokrywania obciążeń.

Ataki cyberterrorystyczne wymierzone w sektor energetyczny przeprowadzane są coraz częściej i przy użyciu coraz bardziej zaawansowanych metod. Doświadczenia USA sprzyjają poglądowi, że ataki na ten sektor dokonywane przez grupy aktywistów politycznych, na przykład ekologów czy radykalnych kontestatorów politycznych, są stosunkowo niegroźne – z reguły nie mają charakteru cyberterrorystycznego. Prawdziwe zagrożenie tkwi bowiem w działaniach

cyberterrorystycznych prowadzonych przez rządy innych państw. Cyberatak na system energetyczny może być przeprowadzony jako część składowa (najczęściej początkowa, o charakterze inicjatywnym) większej, militarnej akcji lub też mieć postać samodzielnego ataku. Ataki cyberterrorystyczne wykonywane na zlecenie rządów są doskonale przygotowane, wykonywane przez wyspecjalizowanych hakerów i mają najczęściej charakter sabotażowy. Brak dostaw energii elektrycznej może dotknąć duże obszary i wiele milionów ludzi jednocześnie, czego efektem są nie tylko duże straty czy zniszczenie, ale też ofiary śmiertelne.

Systemy przedsiębiorstw energetycznych pełnią kluczową rolę nie tylko z punktu widzenia działalności koncernów, ale i całego systemu gospodarczego państwa. To samo tyczy się także energetycznych sieci dystrybucyjnych. Szczególna podatność na ataki cyberterrorystyczne staje się coraz większym zagrożeniem dla fizycznego, jak i ekonomicznego bezpieczeństwa energetycznego państwa.

Nie sposób nie odnieść się do tego ostatniego terminu, zwłaszcza dla zrozumienia całości zagadnień związanych z zagrożeniem cyberterroryzmem sektora energetycznego. Bezpieczeństwo energetyczne jest pojęciem zbyt często rozumianym nazbyt wąsko – jako stan, „w którym gospodarka danego państwa ma zapewniona niezbędną dla jej funkcjonowania i rozwoju podaż czynników produkcji, w tym wystarczalność energetyczną”[480]. To definiowanie czysto gospodarcze, w którym najistotniejsze jest bezpieczeństwo surowcowe, a także finansowe. Ujęcie to dotyczy głównie zatem kosztów uzyskania energii oraz zapewnienia ciągłości dostaw[481]. Energia jest bardzo specyficznym produktem, ponieważ musi być dostępna w sposób ciągły, bez wyjątku, także w sytuacji kryzysów politycznych, ekonomicznych czy nawet militarnych. Brak płynności w dostawach energii wiąże się z zagrożeniami dla całej gospodarki państwa, czy wręcz grup państw, i to nie tylko w zakresie ich stabilności gospodarczej, ale przede wszystkim zdrowia i życia obywateli. Sektor energetyczny odgrywa wiec zasadniczą role nie tylko w kształtowaniu efektywności i konkurencyjności gospodarki, ale wpływa też (bezpośrednio i pośrednio) na kompleksowe funkcjonowanie społeczeństwa oraz systemu państwowego. Stąd też każdy atak cyberterrorystyczny, wymierzony w energetyczną infrastrukturę krytyczną, prowadzi nie tylko do

[43] Haliżak E., *Ekonomiczny wymiar bezpieczeństwa narodowego i międzynarodowego*, [w:] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, Warszawa 1997, s. 78 – 82.
[44] Gradziuk A., Lach W., Poseł – Częścik E., Sochacka K., *Co to jest bezpieczeństwo energetyczne państwa?*, [w:] Dębski S., Górka –Winter B., [red.], *Kryteria bezpieczeństwa międzynarodowego państwa*, Warszawa 2003, s. 76.

zaburzenia bezpieczeństwa energetycznego w klasycznym, ekonomicznym rozumieniu tego terminu, ale pociąga za sobą realne i bezpośrednie zagrożenie dla państwa i jego obywateli.

Liczba ataków o charakterze cyberterrorystycznym wymierzonych w bezpieczeństwo i stabilność sektora energetycznego gwałtownie rośnie. Można by z odnieść się w tym momencie do prostej korelacji, że ponieważ rośnie w ogóle liczba wszystkich cyberataków kwalifikowanych jako terrorystyczne, tendencja ta tyczy się również sektora energetycznego. Ataki na systemy i przedsiębiorstwa energetyczne, z uwagi na skalę i charakter potencjalnych szkód, które mogą wyrządzić, mają jednakże znaczenie szczególne i tak właśnie powinny być traktowane przez rządy, organizacje międzynarodowe i grupy państw. Według zespołu ICS-CERT *(Industrial Control System-Cyber Emergency Response Team*) Departamentu Bezpieczeństwa Wewnętrznego USA odpowiedzialnego za reagowanie na incydenty komputerowe przeciwko energetycznej infrastrukturze krytycznej, w 2011 roku zanotowano 198 cyberataków. Tymczasem w roku poprzedzającym było ich zaledwie 49. Z kolei w pierwszej połowie 2013 roku było ich już 203. Co prawda, w raporcie za rok 2014 odnotowano 245 ataków skierowanych na urządzenia klasy ICS w sektorze energetyki i kluczowej produkcji (*Critical Manufacturing*), więc wzrost nie jest więc już tak dynamiczny, jednakże nadal wyraźny. Warto też zwrócić uwagę na badania ICS – CERT przeprowadzone w roku 2013 wśród 150 przedsiębiorstw sektora energetycznego USA – aż 9% z nich poinformowało, że do prób atakowania ich systemów dochodzi niemal codziennie. W roku 2014 liczba ta wzrosła do 12%[482].

Najważniejszymi, ujawnionymi jak dotąd, przykładami ataków cyberterrorystycznych na systemy elektroenergetyczne były:

1992 - uszkodzenie i wyłączenie systemu monitorowania bezpieczeństwa w elektrowni jądrowej Davis-Besse (USA) – robak Slammer;

2010 - sabotaż irańskiego programu nuklearnego przez USA i Izrael – wirus Stuxnet;

2012 - cyberatak ze strony USA na sześć irańskich terminali naftowych;

2014 - instalacja złośliwego oprogramowania (chińskie robaki Dragonfly, BlackEnergy, Sandworm) w systemach informatycznych firm energetycznych w USA i Europie.

W sektorze elektroenergetycznym stopień wykorzystania systemów OT (*Operational Technology*), czyli cyfrowych systemów sterowania procesem produkcyjnym, jest wyjątkowo wysoki, ze stałą tendencją wzrostową. Wytwarzanie, przesył i dystrybucja energii elektrycznej są

[482] http://geopolityka.org/analizy/andrzej-kozlowski-cyberbezpieczenstwo-infrastruktury-energetycznej [dostęp: 03.06.2018]

procesami całkowicie uzależnionymi od kompleksowych systemów monitorujących i sterujących, a coraz większą rolę odgrywają też systemy sterujące ograniczaniem czasów niedostępności energii, optymalizacją procesu utrzymania instalacji oraz lepszym dostosowaniem produkcji do chwilowych potrzeb makroekonomicznych. Tak duże nasycenie technologiami teleinformatycznymi sprawia, iż sektor elektroenergetyczny infrastruktury krytycznej jest wyjątkowo podatny na zagrożenia cyberterrorystyczne. Specyfika systemów OT sprawia też, że włamania do nich są stosunkowo łatwiejsze. W odróżnieniu od systemów IT, często aktualizowanych i na bieżąco modyfikowanych dla lepszego zabezpieczenia przez zagrożeniami teleinformatycznymi, oprogramowanie OT projektowane jest na dłuższy okres niezmiennej eksploatacji. Średni czas użytkowania systemu OT przekracza dekadę (w warunkach polskich często więcej), z reguły nie jest on też uaktualniany pod względem bezpieczeństwa o nowe definicje zagrożeń.

W zakresie zastosowań można wymienić kilka czynników zwiększających ryzyko:

- SCADA (Supervisory Control And Data Acquisition)[483], czyli wykorzystywanie systemów informatycznych OT, nadzorujących i kontrolujących przebieg procesu technologicznego oraz produkcyjnego. Choć systemy SCADA są bardzo podatne na ataki zewnętrzne, to pozostają głównym narzędziem zarządzania i kontroli sieci przesyłowych, rurociągów gazowych i naftowych, głównie z uwagi na automatyzację produkcji prowadzącą do jej stabilności i zmniejszenia kosztów wytworzenia produktu.
- Inteligentne systemy elektroenergetyczne (Smart Grid), czyli dostarczanie odbiorcom energii elektrycznej lub szerzej – usług energetycznych – z wykorzystaniem środków IT, zapewniające obniżenie kosztów i zwiększenie efektywności oraz zintegrowanie rozproszonych źródeł energii, także odnawialnej. Coraz powszechniejsze wykorzystanie tych systemów również stwarza zagrożenie dla cyberbezpieczeństwa sektora energetycznego – atak na system dystrybucyjny może nastąpić nawet z poziomu inteligentnego urządzenia pomiarowego.
- Nowe technologie informatyczne, jak na przykład powszechne wykorzystanie serwerów wirtualnych nie tylko do archiwizacji danych, ale również do bieżącej pracy obliczeniowej. „Chmura" to narzędzie wygodne, szybkie i tańsze niż klasyczna

[484] *https://inductiveautomation.com/what-is-scada*

architektura oparta na serwerach stacjonarnych, niemniej jednak bardziej narażone na niebezpieczeństwo cyberataku.

- Brak wystarczającego zabezpieczenia sieci z uwagi na wysoki koszt – budżety wielu koncernów przygotowane są raczej na usuwanie skutków ataków niż do ponoszenia bardzo wysokich, stałych kosztów zapobiegania im. W sytuacji, w której celem cyberataku jest pozyskiwanie informacji, zwłaszcza regularne, nie zaś zniszczenie infrastruktury, zagrożenie bezpieczeństwa może przez długi czas pozostawać niewykryte.
- Powszechne dążenie do ograniczenia kosztów – co w sposób oczywisty wpływa na skuteczność ochrony przed cyberatakami. Aspekt ten tyczy się zarówno dużych koncernów energetycznych, jak i ich podwykonawców. Kryterium stopnia zabezpieczenia przed możliwością cyberataku kategorycznie winno być brane pod uwagę przy wyborze firmy do współpracy. Korzystanie z usług podwykonawców wytwarza konieczność połączenia (choćby czasowego) systemów komputerowych koncernów z systemami małych firm outsourcingowych. Cześć z nich nie zabezpiecza w sposób wystarczający swojej sieci, otwierając w ten sposób możliwość ataku pośredniego na serwery usługodawcy.
- Czynnik ludzki, który nie jest związany oczywiście tylko i wyłącznie z sektorem energetycznym, jednakże lojalność, wiedza i doświadczenie pracowników w tej dziedzinie gospodarki pozostają kluczowymi, choć często niedocenianymi elementami istotnymi dla jej cyberbezpieczeństwa. Używanie przez pracowników przenośnych urządzeń typu dysk czy pendrive, niska skuteczność haseł, korzystanie z portali społecznościowych czy prywatnej poczty e-mail w miejscu pracy stwarza duże ryzyko dla bezpieczeństwa sieci firmy. Nie sposób pominąć działania zamierzonego, intencjonalnego, obliczonego na kradzież danych czy wyrządzenie szkód. Atak cyberterrorystyczny, prowadzony przy wsparciu z wewnątrz atakowanej organizacji, może być jednym z największych zagrożeń dla infrastruktury krytycznej.

Zniszczenie, poważne uszkodzenia i będąca wynikiem tego utrata ciągłości pracy Krajowego Systemu Elektroenergetycznego, stanowi – zdaniem autora – potencjalnie najpoważniejsze zagrożenie dla funkcjonowania państwa. System elektroenergetyczny jest bowiem w praktyce nadrzędny dla innych systemów wchodzących w skład infrastruktury krytycznej, a zakłócenie jego działania przez atak cyberterrorystyczny wywołałoby trudne do

prognozowania skutki społeczne, gospodarcze, a także militarne. Z uwagi na fakt, iż położenie geograficzne Polski należy uznać za korzystne z punktu widzenia możliwości wystąpienia poważnych zagrożeń pochodzenia naturalnego (powodzie, huragany, bardzo niskie temperatury), to właśnie atak cyberterrorystyczny staje się najbardziej prawdopodobną przyczyną *blackout*u. Dodatkowym czynnikiem mającym niekorzystny wpływ na bezpieczeństwo krajowego sektora energetycznego jest wiek oraz stan eksploatacyjny bardzo wielu jednostek wytwórczych – w ciągu najbliższej dekady blisko 25% aktualnie wykorzystywanych mocy, pochodzących z elektrowni konwencjonalnych, będzie wymagać całkowitej wymiany. Również współczynnik koncentracji mocy stanowi zagrożenie dla bezpieczeństwa krajowego systemu elektroenergetycznego – przykładowo atak cyberterrorystyczny na elektrownię Bełchatów, który doprowadziłby do jej wyłączenia, miałby poważne skutki dla około 20% krajowych odbiorców energii elektrycznej. Podobne konsekwencje wywołałby skuteczny atak na stację najwyższych napięć Rogowiec będącą kluczowym elementem systemu zapewniającego dystrybucję około 15% całkowitego wolumenu mocy osiąganego przez krajowe elektrownie.

Z uwagi na powyższe uwarunkowania dla zapewnienia odpowiedniego poziomu bezpieczeństwa sektorowi elektroenergetycznemu infrastruktury krytycznej niezbędnym krokiem wydaje się wyodrębnienie tego systemu IK w ramach legislacji jako najistotniejszego jej elementu i nadanie jego ochronie najwyższego priorytetu. Aktualne regulacje prawne w żaden sposób nie określają nadrzędnego charakteru tego sektora zarówno w zakresie zapewniania krytycznych dla społeczeństwa usług, jak i nie uwzględniają zależności pozostałych elementów infrastruktury krytycznej państwa od niezakłóconego funkcjonowania systemu elektroenergetycznego.

Zakończenie

Niezakłócone działanie infrastruktury krytycznej ma ogromne znaczenie nie tylko dla systemu gospodarczego państwa, jest także niezbędna dla efektywnego i sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. Zatem zapewnienie jej skutecznej ochrony stało się w przeciągu ostatnich lat jedną z kluczowych kwestii bezpieczeństwa narodowego współczesnych państw.

W polskim prawodawstwie pojęcie infrastruktury krytycznej nie było obecne aż do 2007 roku – przyjęta wówczas *Ustawa o zarządzaniu kryzysowym* precyzowała, iż jako IK należy „rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców”[484]. W skład infrastruktury krytycznej wchodzi 11 systemów, które mają kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli, dlatego też wszystkie działania skierowane przeciwko niej są uznawane za przestępstwa. *Ustawa o zarządzaniu kryzysowym* w art. 3 ust. 3 zawiera także definicje ochrony infrastruktury krytyczne, przez którą należy rozumieć „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie”.[485] Za podstawowy dokument strategiczny dla ochrony przyjmuje się *Narodowy Program Ochrony Infrastruktury Krytycznej* (NPOIK) przygotowany przez Rządowe Centrum Bezpieczeństwa (RCB)[486], przyjęty uchwałą Rady Ministrów 26 marca 2013 r. Jego zapisy wynikają bezpośrednio z zapisów *Ustawy o zarządzaniu kryzysowym* i zawartej w niej definicji infrastruktury krytycznej. To właśnie ta definicja stała się podstawą dla oceny, które obiekty, urządzenia, instalacje i usługi są kluczowe dla bezpieczeństwa państwa i jego obywateli, a także służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. *NPOIK* określa natomiast – w założeniu

[484] Art. 3, ust. 2, Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 nr 89 poz. 590.
[485] *Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz.U. 2007 nr 89 poz. 590, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id= WDU20070890590 – [dostęp: 25.02.1019]
[485] *Ibidem.*
[486] Zakres kompetencyjny oraz rolę RCB w procesie identyfikacji i ochrony infrastruktury krytycznej opisano szerzej w pkt. 4.2.4 niniejszej pracy

autorów – narodowe priorytety oraz standardy w zakresie ochrony tychże, w zakresie odpowiedzialności administracji rządowej, samorządowej oraz służb powołanych do zapewnienia bezpieczeństwa narodowego. W załączniku nr 3 do *NPOIK* określono także kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej[487]. Wraz z jednolitym wykazem infrastruktury krytycznej kryteria te zostały opracowane i zaktualizowane przez Rządowe Centrum Bezpieczeństwa we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnych za poszczególne systemy.

W niniejszej pracy, starając się odpowiedzieć na pytanie, jaki wpływ ma zjawisko cyberterroryzmu oraz inne zagrożenia asymetryczne na rozwój regulacji prawnych, chroniących bezpieczeństwo infrastruktury krytycznej w Polsce, w istocie podjęto polemikę z autorami *Narodowego Programu Ochrony Infrastruktury Krytycznej*. W toku analizy instytucjonalno-prawnej dostrzeżono bowiem, iż próba wyodrębnienia najbardziej istotnych problemów ochrony prawnej infrastruktury krytycznej przed zagrożeniami o charakterze cyberterrorystycznym, wiąże się z koniecznością identyfikacji usterek i niejasności, zawartych w obowiązujących regulacjach i strategiach. Jedynie ten kierunek uprawniać może do podjęcia próby prognozy kierunków ewolucji polityk i strategii ochrony infrastruktury krytycznej RP. Dlatego też - w ocenie autora - dla prawidłowego zdefiniowania najważniejszych problemów ochrony prawnej infrastruktury krytycznej w Polsce determinujące staje się odwołanie do dwóch podstawowych dla tego zagadnienia kwestii. Pierwsza z nich to problemy definicyjne terminu „infrastruktura krytyczna", druga natomiast – przyjęte podejście do identyfikacja elementów IK w zasobach państwa.

Poddając analizie pogląd (trwale obecny w literaturze przedmiotu), iż precyzyjne zdefiniowanie pojęcia infrastruktury krytycznej, choć jest możliwe na poziomie dokumentów strategicznych powstałych w wyniku procedur legislacyjnych, nie jest osiągalne w ujęciu teoretycznym i badawczym, autor doszedł do wniosku, iż jedynie uwzględnienie szerokiego kontekstu politycznego, społecznego i gospodarczego otoczenia infrastruktury krytycznej pozwoli na jej prawidłowe definiowanie - będące wszak podstawą dla identyfikacji elementów IK w zasobach państwa. Nie tylko bowiem sama systemowość infrastruktury krytycznej – czyli wynikowo rozumienie jej jako zbioru fizycznych obiektów, ale także wpływ jej otoczenia społecznego i gospodarczego, warunkują w efekcie poprawną identyfikację jej elementów.

[487] Jest to dokument zawierający informacje niejawne, zgodnie z przepisami ustawy z 5.8.2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 poz. 1167

Niemożność ujęcia całego zakresu procesu tworzenia definicji w ramy podejścia o charakterze systemowo-technicznym, w istocie stawia pod znakiem zapytania możliwość poprawnego zidentyfikowania jej w zasobach współczesnego państwa.

W ocenie autora istotne byłoby zatem wypracowanie takiej definicji infrastruktury krytycznej, która, uwzględniając kryterium systemowości (rozumianej jako klasyfikacja dostarczanych usług), zawierałaby także elementy postrzegania IK jako wieloaspektowego procesu. Obecnie przyjęta definicja określa bowiem identyfikację elementów infrastruktury krytycznej jedynie jako „systemów, obiektów, instalacji i usług, których zniszczenie lub zakłócenie funkcjonowania spowodowałoby poważne skutki dla bezpieczeństwa państwa i jego obywateli oraz sprawnego działania organów administracji publicznej, instytucji przedsiębiorców". W efekcie w wykazie elementów IK znajdują się tylko i wyłącznie obiekty spełniające kryteria ściśle wiążące pojęcie infrastruktury krytycznej z zaistnieniem sytuacji kryzysowej. Przyjęta definicja – a co za tym idzie – wyłanianie systemów należących do infrastruktury krytycznej, powoduje wykluczenie z ochrony wielu obiektów o wysokim stopniu krytyczności dostarczanych usług. Katalog fizycznych obiektów zakwalifikowanych do infrastruktury krytycznej (i dzięki temu podlegającym szczególnej ochronie prawnej) zdecydowanie nie obejmuje wszystkich elementów infrastruktury państwa, narażonych na zniszczenie lub uszkodzenie w efekcie ataku cyberterrorystycznego z cyberprzestrzeni.

W wyniku dalszej analizy rozwiązań legislacyjnych dotyczących ochrony prawnej systemów IK, autor skłania się poglądu, iż przyjęte w Polsce podejście do odpowiedzialności za bezpieczeństwo obiektów infrastruktury krytyczne również określić można jako niewłaściwe. Założenia *Narodowego Programu Ochrony Infrastruktury Krytycznej* oceniać należy istotnie jako innowacyjne i prekursorskie. Jednocześnie poważne wątpliwości budzić może nie tylko prognoza ich potencjalnej skuteczności, ale przede wszystkim – w ocenie autora - brak zgodności z obowiązującym prawem. *Narodowy Program Ochrony Infrastruktury Krytycznej* w teorii zwalnia operatorów IK z obowiązku ochrony infrastruktury krytycznej, ale fakt owego „zwolnienia" w istocie nie może być zrealizowany, stoi bowiem w sprzeczności z zapisami aktów normatywnych wyższego rzędu. Przekazując operatorom odpowiedzialność za bezpieczeństwo systemów przyjęto założenie, że zwiększenie skuteczności ochrony może nastąpić jedynie poprzez działania operatorów wspieranych przez możliwości i potencjał administracji centralnej – i z rozumowaniem tym trudno nie zgodzić. Bowiem to operatorzy infrastruktury krytycznej mają

największą wiedzę oraz kompetencje niezbędne do zwiększania poziomu bezpieczeństwa systemów pozostających pod ich zarządem - jednakże ich działania w tym kierunku nie są w żaden sposób wspierane ze środków budżetowych.

W ocenie autora „bezsankcyjność", w intencji ustawodawcy rozumiana jest jako rodzaj rekompensaty dla operatorów IK za obowiązek ponoszenia wszystkich kosztów związanych z ochroną systemów – i jest to rekompensata jedynie pozorna. Albowiem w istocie sankcje za niedopełnienie obowiązku ochrony IK znajdują się w zapisach *Ustawy o zarządzaniu kryzysowym oraz* Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia oraz w *art. 160 § 1 Kodeksu karnego.* Znacząca większość obiektów należących do IK w zakresie definiowanym zapisami *Ustawy o zarządzaniu kryzysowym,* to jednocześnie obiekty podlegające obowiązkowej ochronie w myśl przepisów *Ustawy o ochronie osób i mienia.* Szerokie możliwości interpretacyjne zapisu „świadome niedopełnienie obowiązku ochrony", niesprecyzowanie, na czym właściwie polega „obowiązek ochrony" i dlaczego przy deklarowanej dobrowolności, obowiązek ten w ogóle istnieje – niejasności te pozwalają wątpić, czy przepisy dotyczące bezpieczeństwa IK mogą być oceniane jako racjonalne i skuteczne.

Biorąc pod uwagę fakt, iż Narodowy Program Ochrony Infrastruktury Krytycznej jest jedynie dokumentem o charakterze strategicznym, nietrudno uznać, że operatorzy IK podlegają pod sankcje ustawowe niezależnie od wizji dobrowolności ochrony i i braku odpowiedzialności za jej brak zawartej w NPOIK. Rozumowanie przeciwne świadczyłoby, zdaniem autora, o świadomym uznaniu państwa za niezdolne do egzekwowania stanowionego przez siebie prawa.

„Bezsankcyjne" podejście do ochrony infrastruktury krytycznej, oparte na wizji rozbudowanej współpracy, wzajemnym zaufaniu i współodpowiedzialności zainteresowanych stron, a także na stałym doskonaleniu się jego uczestników, można ocenić pozytywnie jedynie w ujęciu etycznym. W rzeczywistości ochrona infrastruktury krytycznej postrzegana jest z punktu widzenia operatora będącego właścicielem i inwestorem konkretnego obiektu czy instalacji jako koszt – i obietnica braku sankcji może sprawić jedynie, iż koszt ten będzie coraz bardziej zmniejszany, a zatem i ochrona będzie coraz mniej skuteczna.

Autor jest zdania, iż dalsze prace legislacyjne nad programami ochrony IK powinny uwzględniać i rozwijać podejście budowane na modelu francuskim. Dystynktywną jego cechą jest określenie z jednej strony katalogu sankcji, nakładanych na operatorów IK, z drugiej – znaczące wsparcie finansowe i organizacyjne państwa dla posiadaczy samoistnych i zależnych

systemów infrastruktury krytycznej. Kierunek ten wydaje się właściwy nie tylko z uwagi na fakt, iż system motywacji finansowej jako istotny determinant dla utrzymania wysokiego standardu ochrony potwierdzony będzie katalogiem sankcji za niedopełnienie obowiązków. Podejście takie będzie także egzemplifikacją założenia, iż rolą administracji publicznej w procesie ochrony IK jest tworzenie mechanizmów prawnych ochrony infrastruktury krytycznej, zapewnienie pomocy dla ich wprowadzania i egzekwowaniu ich stosowania, zaś rolą operatów jest wypełnianie obowiązku ochrony bez ryzyka zmniejszenia przychodu. Prezentowany w NPOIK sposób rozumienia odpowiedzialności za ochronę IK może prowadzić do konstatacji, iż aktualnie premiowane jest raczej ograniczanie ochrony – bowiem zwiększa ono przychody operatora, przy jednoczesnym (choć pozornym) braku zagrożenia sankcjami. Poprawa standardów zapewnianego bezpieczeństwa może być oczekiwana jedynie w sytuacji, w której operatorzy IK będą objęci przepisami jasno i jednoznacznie określającymi zarówno ich zadania i obowiązki, jak i zakres realnej pomocy państwa przy ich wypełnianiu. Państwo powinno zaś nie tylko kontrolować operatorów (czego obecnie w praktyce i tak nie jest zdolne przeprowadzić), nie tylko wyznaczać ramowe założenia ochrony, ale przede wszystkim – aktywnie, racjonalnie i w formie uwzględniającej istnienie mechanizmów rynkowych wspomagać ich w wykonywaniu obowiązków.

Bibliografia

Publikacje książkowe i artykuły

Adamski A., *Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady*, Warszawa 2005.

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Aleksandrowicz T., *Strategia Bezpieczeństwa Narodowego RP*, Warszawa 2014.

Aleksandrowicz T., *Strategie bezpieczeństwa w cyberprzestrzeni. Cyberwojny*, Warszawa 2014.

Aleksandrowicz T., *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014.

Alexander Y., Hoenig M., *Superterroryzm biologiczny, chemiczny i nuklearny*, Warszawa 2001.

Anszczak M., *Zabić tysiące, przestraszyć miliony*, Warszawa 2009.

Arquilla, J., Ronfeldt D., *Networks and Netwars. The Future of Terror, Crime and Militancy*, Santa Monica 2001.

Babak A., Staniforth A., Bosco F., *Cyber Crime and Cyber Terrorism. Investigator's Handbook*, Waltham 2015.

Babak A., *Combating Cybercrime and Cyberrterrorism*, Sheffield 2016.

Balcerowicz B., *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010.

Banasiak M., Parafianowicz R., *Teoria i praktyka działań hybrydowych*, Warszawa 2015.

Banasiak M., *How to understand the hybrid war*, Warszawa 2015.

Białek T., *Terroryzm - manipulacja strachem*, Warszawa 2005.

Bolechów B., *Terroryzm w świecie podwubiegunowym*, Toruń 2002.

Bógdoł-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

Brickey, J., Defining Cyberterrorism: *Capturing a Broad Range of Activities in Cyberspace, Combating Terrorism*, West Point 2012.

Chen T.M., Jarvis L., *Cyberterrorism. Understanding, Assessment, and Response*, Londyn 2014.

Chmielowski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w EU i państwa członkowskich*, Warszawa 2016.

Ciekanowski Z., Rejman K., Wyrębek M., *Cyberterroryzm jako współczesna broń masowego rażenia*, Biała Podlaska 2018.
Clarke R.A., Knake R.A., *Cyber War. The Next Threat to National Security and What to Do About It*, Nowy Jork 2011.
Colarik A.M., *Cyber Terrorism: Political and Economic Implications*, Londyn 2006.
Cragin R. K., *The Early History of al-Qa`ida*, Cambridge 2008.
Denning D., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.
Deshpande V., *Hybrid Warfare: The changing character of conflict*, Waszyngton 2018.
Dni, które wstrząsnęły Estonią: bezradni wobec e-terroru, tł. P. Bukalska, „Tygodnik Powszechny", Warszawa 2009, nr 20, s. 7.
Dziurny A., Kurek S.T., Stachowiak Z., *Infrastruktura krytyczna w modelu bezpieczeństwa publicznego*, Warszawa 2010.
Dziwisz D., *Stany Zjednoczone a międzynarodowe bezpieczeństwo cybernetyczne*, Kraków 2015.
El Ghamari M., *Ochrona cyberprzestrzeni – wyzwanie naszych czasów?*, „Bezpieczeństwo i Technika Pożarnicza" 2018, nr 1, s. 24..
Erickson J., *Hacking sztuka penetracji*, Gliwice 2004.
Filar M., *Terroryzm – problemy definicyjne oraz regulacje prawne w polskim prawie karnym w świetle prawa międzynarodowego i porównawczego*, Toruń 2002.
Florianczyk-Kardaś M., *Kilka uwag o ochronie infrastruktury krytycznej w świetle przepisów ustawy o zarządzaniu kryzysowym i ustawy o „złotej akcji" Skarbu Państwa*, Warszawa 2015.
Gancarz G., *Podstawy współpracy z zakresie zwalczania terroryzmu w prawie Unii Europejskiej*, Warszawa 2008.
Ganor B., *Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter*, Routledge 2002.
Gelberg L., *Prawo międzynarodowe i historia dyplomacji*, Warszawa 1960.
Goldsmith J., Wu T., *Who Controls the Internet? Illusions of a Borderless World*, Oxford 2008.
Gorzkowicz A., *Wojna hybrydowa na Ukrainie jako przykład współczesnych konfliktów zbrojnych*, Warszawa 2017.
Grabowska K., *Próba wyjaśnienia pojęcia i istoty wojen hybrydowych*, Warszawa 2016.

Gradziuk A., Lach W., Poseł-Częścik E., Sochacka K., *Co to jest bezpieczeństwo energetyczne państwa?*, Warszawa 2003.
Gruszczak A., *Prewencja i antycypacja zagrożeń terrorystycznych w polityce bezpieczeństwa Unii Europejskiej*, [w:] Współczesne oblicze terroryzmu, Kraków 2016.
Gruszczak A., *Unia Europejska wobec terroryzmu po 11 września 2001 roku*, Kraków 2002.
Gryz J., *Terroryzm międzynarodowy jako zjawisko społeczne w początkach XXI wieku*, „Zeszyty Naukowe AON" 2016, nr 1, s. 5.
Grzelak M, *Międzynarodowa strategia USA dla cyberprzestrzeni*, Warszawa 2010.
Haliżak E., *Ekonomiczny wymiar bezpieczeństwa narodowego i międzynarodowego*, Warszawa 1997.
Haliżak E., *Terroryzm w świecie współczesnym*, Warszawa, 2004.
Hanusek T., *W sprawie pojęcia współczesnego terroryzmu*, Warszawa 1980.
Healey J., *America's New Cyberspace Strategy*, Waszyngton 2011.
Healey J., *Preparing for Cyber 9/12*, Waszyngton 2012.
Healey J., *The US Cyber Policy Reboot*, Waszyngton 2012.
Hoffman B., *Oblicza terroryzmu*, Warszawa 2001.
Hoffman B., *Recent Trends and Future Prospects of Iranian Sponsored International Terrorism*, Santa Monica 2008.
Jagusiak B., *Teoretyczne i metodologiczne problemy badań nad bezpieczeństwem*, Poznań 2014.
Janczewski L.J., Coralik A.M., *Cyber Warfare and Cyber Terrorism*, Londyn 2008.
Janik W., *Logistyka współczesnego terroryzmu*, Elbląg 2016.
Jaroszyński K., *Koncepcja współczesnych działań antyterrorystycznych*, Warszawa 2003.
Jasiński F., Narojek M., Rakowski P., *Wewnętrzne i zewnętrzne aspekty współpracy antyterrorystycznej w Unii Europejskiej w kontekście Polski, jako państwa członko*wskiego, Warszawa 2006.
Jaskiernia A., *Uwarunkowania skuteczności zwalczania terroryzmu w świetle prac Rady Europy*, Warszawa 2002.
Kańciak A., *Problematyka cyberprzestępczości w Unii Europejskiej*, Warszawa 2013.
Konieczny J., *Bezpieczeństwo w zrównoważonym rozwoju. Projekt badań zintegrowanych*, Poznań 2014.
Kośla R., *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski*, Warszawa 2002.

Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, Warszawa 2014.
Koziej S, *Strategie Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2003 i 2007 roku*, Warszawa 2015.
Koziej S., Brzozowski A., *25 lat polskiej strategii bezpieczeństwa*, Warszawa 2014.
Krajski S., *Traktat z Maastricht. Wstęp i komentarz*. Warszawa 1998.
Kuehl D.T., *From Cyberspace to Cyberpower: Defining the Problem*, Waszyngton 2009.
Kwiatkiewicz P., *Bezpieczeństwo energetyczne. Rynki surowców i energii. Energetyka w czasach politycznej niestabilności*, Poznań 2015.
Lakomy M., *Cyberwojna jako rzeczywistość XXI wieku*, Warszawa 2011.
Lenaerts K., Van Nuffel P., *Podstawy prawa europejskiego*, Warszawa 1998.
Lewis, J. A., *Assessing the risk of cyber terrorism, cyber war and other cyber threats*, 2002.
Libicki M.C., *Cyberspace Is Not a Warfighting Domain*, Columbus 2012.
Lichocki E, *Cyberterroryzm państwowy i niepaństwowy, początki, formy, skutki*, Gdynia 2011.
Lichocki E., *Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych RP*, Warszawa 2009.
Lidwa W., Krzeszowski W., Więcek W., Kamiński P., *Ochrona infrastruktury krytycznej*, Warszawa 2012.
Liedel K., *Bezpieczeństwo informacyjne państwa*, Warszawa 2011.
Liedel K., Piasecka P., *Ochrona obywateli i instytucji publicznych przed atakami terroryzmu i przemocy*, Warszawa 2004.
Lin H., *Cyber Conflict and National Security*, Boston 2013.
Lynn W.J. III, *Defending a New Domain*, Waszyngton 2010.
Schachtman N., *Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack*, Waszyngton 2010.
Madej M., *Międzynarodowy terroryzm polityczny*, Warszawa 2001.
Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, Warszawa 2009.
Madej M., *O koncepcji i praktyce harmonizacji prawa w krajach EWG*, Warszawa 1972.

Mierzejewski D.J., *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych*, Toruń 2011.
Mickiewicz P., *System bezpieczeństwa narodowego*, Wrocław 2012.
Mildner D., *Analiza pojęcia cyberterroryzmu*. *Próba uporządkowania chaosu*, Warszawa 2013,
Milewski J., *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, Warszawa 2016.
Mitnick K., *Sztuka podstępu*, Warszawa 2003.
Mogadeshi R., *Critical infrastructure. Protection and uncertainty analysis*, Londyn 2017.
Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.
Pacek B., Hoffman R., *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013.
Panasiuk A., Sierański S., *Bezpieczeństwo państwa i obywateli. Ochrona obiektów infrastruktury krytycznej*, Warszawa 2017.
Pawłowski A., *Terroryzm polityczny w Europie w XIX i XX wieku*, Zielona Góra 1980.
Pyznar M., Abgarowicz G., Wiercińska-Krużewska A, Gajek P., Świątkowska J., Dziwisz D., Ryba M., Poniewierski A., Kotłowski W. i inni, *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, Kraków 2015.
Radziejewski R., *O infrastrukturze krytycznej krytycznie*, Warszawa 2013.
Rypulak-Mirowska K., *Zwalczanie terroryzmu – Wybrane zagadnienia polityki bezpieczeństwa wewnętrznego Unii Europejskiej – szanse i zagrożenia dla Polski*, Warszawa 2008.
Sawicki M., *Cyberprzestępczość,* Warszawa 2013.
Siadkowski A., *Bezpieczeństwo i ochrona w cywilnej komunikacji lotniczej na przykładzie Polski, Stanów Zjednoczonych i Izraela*, Szczytno 2013.
Sienkiewicz P., Świeboda H., *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, Warszawa 2009.
Sienkiewicz P.: *Terroryzm w cybernetycznej przestrzeni*, Warszawa, 2010.
Siwicki M., *Podział i definicja cyberprzestępstw*, Warszawa 2012.
Skoneczny Ł, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, Warszawa 2011.
Skrzypczak J., *Bezpieczeństwo teleinformatyczne w świetle Europejskiej Konwencji o Cyberprzestępczości*, Poznań 2011.
Słownik języka polskiego, Warszawa 2002.

Smolski W., *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, Wrocław 2015.
Soloch P., *NATO a ochrona infrastruktury krytycznej*, Warszawa 2007.
Starr L.K., *Cyberpower and National Security*, Waszyngton 2009.
Stępień M., *Ochrona cyberprzestrzeni Rzeczypospolitej Polskiej a współpraca państw członkowskich Unii Europejskiej*, Siedlce 2017.
Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem,* Warszawa 2010.
Szewczyk T., *Europejski program ochrony infrastruktury krytycznej*, Warszawa 2012.
Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Warszawa 2005.
Świątkowska J., *Bezpieczeństwo infrastruktury krytycznej – wymiar technologiczny*, Kraków 2014.
Tekielska P., Czekaj Ł., *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, Warszawa 2014.
Tomasiewicz J., *Terroryzm na tle przemocy politycznej*, Katowice 2000.
Trejnis Z, Trejnis P.Z., *Polityka ochrony cyberprzestrzeni w państwie współczesnym*, Warszawa 2017.
Trubalska J., *System antyterrorystyczny w Polsce – wybrane zagadnienia*, Warszawa 2016.
Vatis M. A., *The Council of Europe Convention on Cybercrime*, Waszyngton 2010.
Verton D., *Black ice: niewidzialna groźba cyberterroryzmu*, Gliwice 2004.
Wawrzyk P., *Polityka Unii Europejskiej w obszarze spraw wewnętrznych i wymiaru sprawiedliwości*, Warszawa 2007.
Wejkszner A., *Terroryzm sponsorowany przez państwa. Casus bliskowschodnich państw-sponsorów*, Warszawa, 2010.
White K. C., *Cyber-Terrorism: Modem Mayhem*, Carlisle 1998.
Wiercińska-Krużewska A., Gajek P., *Prawne uwarunkowania ochrony infrastruktury krytycznej*, Kraków 2015.
Włodarski A., Bralewski A., *Istota i cel ochrony infrastruktury krytycznej*, „Zeszyty Naukowe SGSP" 2015, nr 2, s. 43.
Wojciechowski S., *Hybrydowy model globalnego terroryzmu,* „Przegląd Strategiczny" 2011, nr 2.

Wojciechowski S., *Terroryzm na początku XXI wieku. Pojęcie. Przejawy. Przyczyny*, Poznań 2013.
Wojnicz L., *Nieformalne struktury państw Unii Europejskiej w walce z międzynarodowym terroryzmem. Bilans współpracy i wyzwania*, Szczecin 2007.
Zenderowski R., *Stosunki międzynarodowe Vademecum*, Wrocław 2006.
Zięba R., *Bezpieczeństwo międzynarodowe w pierwszej dekadzie XXI wieku w kontekście nowych wyzwań i zagrożeń*, „Krakowskie Studia Międzynarodowe" 2007, nr 4.
Zięba R., *Bezpieczeństwo międzynarodowe w XXI wieku*, Warszawa 2018.
Żuber M., *Infrastruktura krytyczna państwa jako obszaru potencjalnego oddziaływania terrorystycznego*, Warszawa 2014.

Źródła internetowe

http://lexblog.pl/definicja-cyberprzestepstwa/Lexblog.pl.
http://www.europapraw.org/files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf.
https://www.state.gov/j/ct/list/c14151.htm.
https://www.state.gov/j/ct/rls/crt/index.htm.
https://www.state.gov/documents/organization/286410.pdf.
http://www.nopc.gov./publication/highlight/2001/highlight-01-06.htm.
http://www.cs.georgetown.edu/~denning/infosec/pollitt.html].
http://eng.cnews.ru/news/top/indexEn.shtml?2008/03/27/293913.
europa.eu/rapid/press-release_IP-17-3193_pl.pdf.
europa.eu/rapid/press-release_IP-18-6759_pl.pdf.
http://register.consilium.europa.eu/pdf/pl/05/st14/st14469-re04.pl05.pdf.
http://europa.eu/rapid/press-release_IP-15-4865_pl.htm.
http://www.schneier.com/blog/archives/2010/12/book_review_ cyb.html.
http://www.wired.com/threatlevel/2010/03/ schmidt-cyberwar.
bbn.gov.pl/portal/pl/2/915/O_przyszlosci_NATO.html?search=474159029.
http://www.acus.org/new_atlanticist/americas-new_cyberspace-strategy.
http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.
http://www.fas.org/sgp/ library/pccip.pdf.

https://cyberpolicy.nask.pl/cp/dobre-praktyki/isac/69,ISAC-Information-Sharing-and-Analysis-Center-Centra-Wymiany-i-Analizy-Informacji.html,
http://www.fas.org/sgp/ library/pccip.pdf.
https://www.nrc.gov/reading-rm/doc-collections/commission/secys/2000/secy2000-0088/2000-0088scy.pdf.
https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf.
http://www.whitehouse.gov/cybersecurity/ comprehensive-national-cybersecurity-initiative.
http://www.whitehouse.gov/blog/2010/03/02/transparent-cybersecurity.
http://www.state.gov/s/cyberissues/.
http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP19900090066.
https://www.academia.edu/19961908/Strategia_Obronna_RP_z_2000_r.
https://www.msz.gov.pl/resource/93e1e4c7-e129-41c7-8365-39dbad8b1c54:JCR.
https://www.msz.gov.pl/resource/93e1e4c7-e129-41c7-8365-39dbad8b1c54:JCRm.
https://docplayer.pl/2820895-Polityka-ochrony-cyberprzestrzeni-rp.html.
https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109.
http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersjapl.pdf.
https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=BG.
https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022.
https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/#_edn8.
https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/pobierz,kpb~p_14_043_20140617104838140300211 8~01,typ,kk.pdf.
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148.
http://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf.
https://rcb.gov.pl/narodowy-program-ochrony-infrastruktury-krytycznej-przyjety-przez-rade-ministrow-2.
https://www.abw.gov.pl/pl/prawo/273,Prawo.html.

https://bip.abw.gov.pl/bip/struktura/47,Struktura-organizacyjna.html.
http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101821228.
https://aw.gov.pl/prawo/.
http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WMP20180000660/O/M20180660.pdf.
http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040709.
https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/organy-pomocnicze/organy-pomocnicze-rady/128,Miedzyresortowy-Zespol-do-Spraw-Zagrozen-Terrorystycznych.html.
http://www.pse-operator.pl/index.php?dzid=80&did=23.
http://www.pse-operator.pl/index.php?dzid=79&did=22.
http://www.cire.pl/rynekenergii/import.php?smid=205.
http://bip.ure.gov.pl/portal/bip/75/787/Operatorzy_systemow_elektroenergetycznych__dane_adresowe_i_obszary_dzialania.html.
http://www.gkpge.pl/relacje-inwestorskie/grupa/kim-jestesmy.
http://www.energa.pl/dla-domu/grupa-energa/grupaenerga.
http://www.tauron-pe.pl/tauron/grupa-tauron/Strony/o-grupie-tauron.aspx.
http://www.tauronpe.pl/tauron/o-tauronie/Documents/raport-roczny-tauron-2016.pdf.
http://www.firma.enea.pl/47/grupa-enea/wszystko-o-enea/przedmiot-dzialalnosci-162.html.
http://bip.ure.gov.pl/portal/bip/76/786/Operatorzy_systemow_gazowych_dane_adresowy_i_obszary_dzialania.html.
http://www.pern.com.pl/?q=node/45.
http://www.pern.com.pl/?q=node/59.
http://www.olpp.pl/uslugi.
http://www.stat.gov.pl/cps/rde/xbcr/gus.
http://www.krrit.gov.pl/Data/Files/_public/Portals/0/kontrola/program/radio/kwartalne/rynek_3_kw12.pdf.
http://www.krrit.gov.pl/Data/Files/_public/Portals/0/publikacje/analizy/rynek-tv-iii-kw2012.pdf.
http://www.uke.gov.pl/_gAllery/56/31/56314/Raport_o_stanie_rynku_telekomunikacyjnego_za_2011_zm02.pdf.
http://www.stat.gov.pl/cps/rde/xbcr/gus/tl_lacznosc_wyniki_dzialalnosci_2011.pdf.
http://www.stat.gov.pl/cps/rde/xbcr/gus/zo_zdrowie_i_ochrona_zdrowia_w_2016.pdf.
www.abw.gov.pl/download/1/1886/Szewczyk.pdf.

http://geopolityka.org/analizy/andrzej-kozlowski-cyberbezpieczenstwo-infrastruktury-energetycznej.
http://www.tevalis.fr/images/ArticleICCWS2014.pdf.
http://www.egov.pl/index2.php?op-tion=content&task=view&id=11&pop=1&page=0.
http://iks_pn.sggw.pl/z38/art7.pdf.
https://www.google.com/search?client=safari&rls=en&q=Szewczyk+T.,+Pyznar+M.,+Ochrona+infrastruktury+krytycznej+a+zagro%C5%BCenia+asymetryczne&ie=UTF-8&oe=UTF-8.

Akty prawne i inne dokumenty

Bezpieczna Europa w Lepszym Świecie – Europejska Strategia Bezpieczeństwa z dnia 12 grudnia 2003 r.
Decyzja Ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne.
Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej.
Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym.
Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218 z 14 VIII 2013 r. poz. 8).
Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE L 218 z 14.08.2013).
Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.
Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE L 345 z 23.12.2008).

Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony.
Internet Governance – Council of Europe Strategy 2012–2015, Rada Europy.
Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, European Commission, Brussels, 7.2.2013.
Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, W kierunku ogólnej strategii zwalczania cyberprzestępczości, KOM (2007).
Komunikat Komisji Wspólnot Europejskich do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, Bruksela, 1 VI 2005 COM(2005) 229 końcowy.
Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.
Konwencja o ochronie praw człowieka i podstawowych wolności, Rzym, 4 listopada 1950 r. (Dz. U. 1993, Nr 61, poz. 264, z późn. zm.).
Konwencja Rady Europy o Cyberprzestępczości z 23 listopada 2001 r.
Międzynarodowy Pakt Praw Obywatelskich i Politycznych, Nowy Jork ,19 grudnia 1966 r. (Dz. U. 1977, Nr 38, poz. 167).
Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej z 25 czerwca 2013 r.
Presidential Decision Directive 63, 22.05.1998.
Proposal for a Directive of the European Parliament and of the Council, concerning measures to ensure a high common level of network and information security across the Union, Brussels, 7.2.2013.
Raport o Stanie Gospodarki, Warszawa, 2016.
Rezolucja Rady Bezpieczeństwa nr 1701.
Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.Urz. nr 83 z 17 maja 2010 r., poz. 541).
Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.Urz. nr 83 z 17 maja 2010 r., poz. 542).

Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz.Urz. nr 83 z 17 maja 2010 r., poz. 540).
Rozporządzenie Rady Ministrów z 30.04.2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.Urz.10.83.54).
Sprawozdanie z działalności Prezesa Urzędu Regulacji Energetyki w 2016 r.
Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, przyjęta przez Radę Ministrów w dniu 9 kwietnia 2007 r., a zatwierdzona przez Prezydenta RP w dniu 13 listopada 2007 r.
The Report of the President's Commission on Critical Infrastructure Protection, October 1997.
The Report of the President's Commission on Critical Infrastructure Protection, October 1997.
U.S. Department of Homeland Security. (2013a). *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience,* Washington DC, 2009.
Uchwała Komitetu Obrony Kraju z dnia 21 lutego 1990 r. w sprawie doktryny obronnej Rzeczypospolitej Polskiej.
Uchwała nr r 67 Rady Ministrów z 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022" (M. P. z 16 maja 2013 r., poz. 377).
Ustawa z 10.04.1997 r. Prawo energetyczne (Dz. U. z 2003 r. Nr 153, poz. 1504, z późn. zm.).
Ustawa z 18.03.2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz.U.10.65.404).
Ustawa z 21.11.1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2004 r. Nr 241, poz. 2416, z późn. zm.).
Ustawa z 24.08.1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2002 r. Nr 147, poz. 1230, z późn. zm.).
Ustawa z 4.02.1994 r. Prawo geologiczne i górnicze (Dz. U. z 2005 r. Nr 228, poz. 1947, z późn. zm.).
Ustawa z 5.06.1998 r. o administracji rządowej w województwie (Dz. U. z 2001 r. Nr 80, poz. 872, z późn. zm.).

Ustawa z 5.06.1998 r. o samorządzie powiatowym (Dz. U. z 2001 r. Nr 142, poz. 1592, z późn. zm.).
Ustawa z 5.06.1998 r. o samorządzie województwa (Dz. U. z 2001 r. Nr 142, poz. 159 0, z późn. zm.).
Ustawa z 6.04.1990 r. o Policji (Dz. U. z 2002 r. Nr 7, poz. 58, z późn. zm.).
Ustawa z 7.07.1994 r. Prawo budowlane (Dz. U. z 2003 r. Nr 207, poz. 2016, z późn. zm.).
Ustawa z 30.05.1996 r. o rezerwach państwowych oraz zapasach obowiązkowych paliw (Dz. U. z 2003 r. Nr 24, poz. 197, z późn. zm.).
Ustawa z 8.03.1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591), z późn. zm.).
Ustawa z 9.11.2000 r. o bezpieczeństwie morskim (Dz. U. Nr 109, poz. 1156, z późn. zm.).
Ustawa z 29.11.2000 r. Prawo atomowe (Dz. U. z 2004 r. Nr 161, poz. 1689, z późn. zm.).
Ustawa z 21.12.2000 r. o żegludze śródlądowej (Dz. U. z 2001 r. Nr 5, poz. 43, z późn. zm.).
Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. (Dz.U. poz. 1514).
Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. Nr 31, poz. 206, z późn. zm.).
Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 nr 89 poz. 590).
Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (tekst jednolity: Dz.U. z 2014 poz. 1815, ze zm.).
Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jednolity: Dz.U. z 2016 r. poz. 1137).
Ustawa z 12.10.1990 r. o ochronie granicy państwowej (Dz. U. z 2005 r. Nr 226, poz. 1944).
Ustawa z 24.08.1991 r. o ochronie przeciwpożarowej (Dz. U. z 2002 r. Nr 147, poz. 1229, z późn. zm.).
Ustawa z dnia 5.08.2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., Nr 182, poz. 1228 z późn. zm.).
Wyrok Trybunału Konstytucyjnego z 21.04. 2009 r., sygn. akt K 50/07.
Zielona księga w sprawie europejskiego programu ochrony infrastruktury krytycznej. Komisja Wspólnot Europejskich, Bruksela, dnia 17.11.2005 r., KOM (2005) 576 wersja ostateczna.

Spis tabel

Spis map

Spis rysunków

Spis wykresów

Cyberterroryzm w polityce bezpieczeństwa państwa. Problemy ochrony infrastruktury krytycznej.

Streszczenie

Zasadniczym problem badawczym pracy jest próba odpowiedzi na pytanie, jaki wpływ ma zjawisko cyberterroryzmu oraz inne zagrożenia asymetryczne na rozwój regulacji prawnych, chroniących bezpieczeństwo infrastruktury krytycznej w Polsce. W zakresie objętym badaniem mieści się również próba wyodrębnienia najbardziej istotnych problemów ochrony infrastruktury krytycznej przed zagrożeniami o charakterze cyberterrorystycznym.

Do osiągnięcia wytyczonego celu badawczego wykorzystano przede wszystkim teoretyczne metody badawcze, w szczególności analizę instytucjonalno-prawną. Dokonano przeglądu dotychczasowego stanu legislacji związanej z ochroną bezpieczeństwa cyberprzestrzeni w dokumentach strategicznych Unii Europejskiej (rozdział II), Stanów Zjednoczonych Ameryki Północnej (rozdział III) oraz Rzeczpospolitej Polskiej (rozdział IV), zwracając uwagę nie tylko na zależności ściśle chronologiczne w ramach procesu prawotwórczego, lecz także na funkcje wzajemnego wpływu. Znaczący nacisk położono więc szczególnie na analizę problematyki niejednolitości identyfikacyjnej zarówno zjawiska cyberterroryzmu, jak i pojęcia infrastruktury krytycznej.

W rozdziale V poddano analizie fakt, iż precyzyjne zdefiniowanie infrastruktury krytycznej, choć możliwe na poziomie dokumentów strategicznych powstałych w wyniku procedur legislacyjnych, nie zawsze jest osiągalne i możliwe w ujęciach teoretycznym i badawczym. Jedynie uwzględnienie szerokiego kontekstu politycznego, społecznego i gospodarczego otoczenia infrastruktury krytycznej pozwala na prawidłowe definiowanie infrastruktury krytycznej.

W rozdziale VI, z kolei, będącym próbą analizy strategicznych założeń ochrony infrastruktury krytycznej RP, przedstawiono najważniejsze akty prawne regulujące procedury identyfikacji i ochrony infrastruktury krytycznej w Polsce. Z uwagi na bardzo obszerny materiał badawczy dokonano zawężenia analizowanego zakresu do legislacji krajowej w odróżnieniu od przyjętego uprzednio w rozdziałach dotyczących bezpieczeństwa cyberprzestrzeni szerokiego ujęcia uwzględniającego także USA i Unię Europejską. Przyjęcie tej perspektywy pozwoliło ocenić, w jakim stopniu wytworzenie procedur prawnych ochrony infrastruktury krytycznej przed

zagrożeniami z cyberprzestrzeni stało się jednym z priorytetów stojących przed państwem, a także zdefiniować trudności, jakie stwarza konieczność realizacji tego priorytetu na poziomie legislacyjnym. Decyzja o poddaniu analizie najważniejszych aktów prawnych regulujących procedury identyfikacji i ochrony infrastruktury krytycznej w Polsce zaowocowała także zamieszczeniem w pracy (w rozdziale VII) szczegółowego opisu systemów infrastruktury krytycznej RP.

Do najistotniejszych problemów ochrony prawnej infrastruktury krytycznej w Polsce zaliczono: trudności definicyjne pojęcia IK, wady przyjętego podejścia do identyfikacji zasobów infrastruktury krytycznej oraz niejasności w zakresie oceny krytyczności poszczególnych elementów systemu. Jako problemy ochrony zdiagnozowano także: niezgodność zapisów *Narodowego Programu Ochrony Infrastruktury Krytycznej* z obowiązującymi przepisami wyższego rzędu, przyjęte podejście do odpowiedzialności za ochronę systemów IK, wskazano także potrzebę wzmocnienia ochrony prawnej systemu elektroenergetycznego, uznanego za najważniejszy z katalogu zasobów infrastruktury krytycznej.

Słowa kluczowe: cyberterroryzm, cyberprzestępczość, infrastruktura krytyczna, terroryzm, polityka bezpieczeństwa państwa

Cyber terrorism in the state security policy. Problems of critical infrastructure protection.

Summary

The fundamental problem of the research work is the attempt to answer the question what is the effect of cyber-terrorism and other asymmetrical threats to the development of legal regulations that protect the security of critical infrastructure in Poland. The scope of the study also includes an attempt to identify the most important problems of critical infrastructure protection against cyber threats.

The theoretical research methods, in particular the institutional and legal analysis, were used to achieve the set research goal. The previous state of legislation related to the protection of cyberspace security in strategic documents of the European Union (chapter II) has been reviewed, United States of America (Chapter III) and the Republic of Poland (Chapter IV), paying attention not only to strictly chronological relationships as part of the law-making process, but also to the functions of mutual influence. Significant emphasis was therefore placed especially on the analysis of the non-unification problem of both the phenomenon of cyberterrorism and the concept of critical infrastructure.

Chapter V analyzes the fact that the precise definition of critical infrastructure, although possible at the level of strategic documents created as a result of legislative procedures, is not always achievable and possible in theoretical and research approaches. Only taking into account the broad political context, social and economic environment of critical infrastructure allows for proper defining of critical infrastructure.

Chapter VI, which is an attempt to analyze the strategic assumptions of the protection of the critical infrastructure of the Republic of Poland, presents the most important legal acts regulating the procedures for the identification and protection of critical infrastructure in Poland. Due to the very extensive research material, the analyzed scope was narrowed down to national legislation as opposed to the broad approach previously adopted in the cyberspace security chapters, which also includes the US and the European Union. The adoption of this perspective made it possible to assess to what extent the creation of legal procedures for the protection of critical infrastructure against cyber threats has become one of the state's priorities, as well as to define the difficulties created by the necessity to implement this priority at the legislative level. The decision to subject the analysis of the most important legal acts regulating the procedures for

the identification and protection of critical infrastructure in Poland also resulted in the inclusion in the paper (in Chapter VII) of a detailed description of the critical infrastructure systems of the Republic of Poland.

The most important problems of legal protection of critical infrastructure in Poland include: the definition difficulties of the CI concept, the disadvantages of the adopted approach to the identification of critical infrastructure resources and ambiguities in the assessment of the criticality of individual system components. Security problems were also diagnosed as: incompatible provisions of the National Critical Infrastructure Protection Program with the applicable higher-level regulations, accepted approach to responsibility for the protection of CI systems, and the need to strengthen the legal protection of the power system, recognized as the most important of the critical infrastructure resources catalog.

Key words: cyber terrorism, cybercrime, critical infrastructure, terrorism, state security policy