KOMISJA
EUROPEJSKA

Bruksela, dnia 28.10.2019 r.
COM(2019) 546 final

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY

oceniające spójność podejść przyjętych przez państwa członkowskie w procesie identyfikacji operatorów usług kluczowych zgodnie z art. 23 ust. 1 dyrektywy (UE) 2016/1148 w sprawie bezpieczeństwa sieci i informacji

1. Wprowadzenie

Dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[1] (dyrektywa w sprawie bezpieczeństwa sieci i informacji) jest pierwszym instrumentem rynku wewnętrznego ukierunkowanym na poprawę odporności UE na zagrożenia związane z cyberbezpieczeństwem. Przyjmując art. 114 Traktatu o funkcjonowaniu Unii Europejskiej jako podstawę, dyrektywa ta ma na celu zapewnienie ciągłości świadczenia usług umożliwiających właściwe funkcjonowanie gospodarki i społeczeństwa Unii. Z myślą o tym w dyrektywie wprowadzono konkretne środki na rzecz budowania zdolności w zakresie cyberbezpieczeństwa w całej UE oraz przeciwdziałania rosnącym zagrożeniom dla sieci i systemów informatycznych wykorzystywanych do świadczenia usług kluczowych w najważniejszych sektorach.

Po wejściu w życie dyrektywy w sprawie bezpieczeństwa sieci i informacji w sierpniu 2016 r. państwa członkowskie zobowiązane były do wdrożenia krajowych środków niezbędnych do wprowadzenia przepisów tej dyrektywy do dnia 9 maja 2018 r.[2] Dyrektywa ta ma przyczynić się do stworzenia kultury zarządzania ryzykiem wśród przedsiębiorstw lub innych podmiotów świadczących usługi kluczowe, zdefiniowanych zgodnie z art. 5 jako „operatorzy usług kluczowych" (OUK). Operatorzy, którzy są objęci zakresem stosowania dyrektywy, zobowiązani są do podejmowania odpowiednich i proporcjonalnych środków technicznych i organizacyjnych w celu zarządzania ryzykami dla bezpieczeństwa ich sieci i systemów informatycznych oraz zgłaszania najpoważniejszych incydentów właściwym organom.

Współprawodawcy powierzyli wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji państwom członkowskim, które zobowiązane są do określenia usług kluczowych i identyfikacji operatorów usług kluczowych na swoich terytoriach. W art. 5 ust. 7 dyrektywy nałożono zatem na państwa członkowskie obowiązek informowania Komisji o wynikach tej identyfikacji. W celu umożliwienia koordynacji w zakresie składania sprawozdań zarówno

[1] Dz.U. L 194 z 19.7.2016, s. 1.
[2] Do września 2019 r. wszystkie 28 państw członkowskich zgłosiło, że dokonało pełnej transpozycji dyrektywy.

Komisja[3], jak i grupa współpracy ustanowiona na mocy dyrektywy[4] przekazały państwom członkowskim wskazówki dotyczące procesu identyfikacji.

Zgodnie z art. 23 ust. 1 niniejsze sprawozdanie zawiera ocenę spójności podejść przyjętych przez państwa członkowskie do identyfikacji operatorów usług kluczowych. Ze względu na to, że identyfikacja OUK oraz ryzyko fragmentacji rynku wewnętrznego w tym obszarze są ze sobą ściśle powiązane, niniejsze sprawozdanie przyczyni się również do szerszej oceny dyrektywy w sprawie bezpieczeństwa sieci i informacji, jak określono w art. 23 ust. 2, który stanowi, że Komisja dokonuje okresowego przeglądu funkcjonowania dyrektywy i ocenia wykaz sektorów i podsektorów podlegających identyfikacji OUK oraz rodzajów usług cyfrowych objętych tą dyrektywą. Pierwsze tego typu sprawozdania mają być złożone do dnia 9 maja 2021 r.

1.1 Cel sprawozdania

Operatorzy usług kluczowych muszą wykazywać szczególnie wysoki poziom odporności na cyberincydenty ze względu na ważną rolę, jaką odgrywają w całej gospodarce i całym społeczeństwie. W tym względzie spójne podejście do identyfikacji OUK przez państwa członkowskie jest ważne z kilku powodów:

1. **W celu zmniejszenia ryzyk związanych z transgranicznymi zależnościami**

   Brak spójnej identyfikacji ważnych operatorów świadczących usługi transgraniczne może skutkować nierównym poziomem odporności w dziedzinie cyberbezpieczeństwa w poszczególnych państwach członkowskich, zwiększając ryzyko, że transgraniczny incydent doprowadzi do zniszczenia infrastruktury krytycznej lub będzie skutkował utratą życia obywateli[5]. Na przykład operatorzy systemu przesyłowego z sektora energii lub rejestry domen najwyższego poziomu

[3] Komunikat Komisji do Parlamentu Europejskiego i Rady: Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, COM(2017) 476.

[4] Grupa współpracy ds. bezpieczeństwa sieci i informacji składająca się z państw członkowskich, Komisji i ENISA (Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji) utworzyła osobną grupę roboczą w celu wymiany między państwami członkowskimi informacji i najlepszych praktyk dotyczących identyfikacji OUK.

[5] Na przykład w maju 2017 r. kryptowirusowi typu ransomware WannaCry rozprzestrzenienie się na ponad 150 krajów i zawirusowanie około 200 000 komputerów zajęło zaledwie jeden dzień.

ujęci w wykazie rodzajów podmiotów w załączniku II są podmiotami, które są w największym stopniu obecne na rynku wewnętrznym, świadcząc usługi transgraniczne na rzecz konsumentów i przedsiębiorstw. Spójna identyfikacja takich dostawców w całej Unii mogłaby zatem pomóc zapobiegać rozprzestrzenianiu się zagrożeń dla cyberbezpieczeństwa na całym rynku wewnętrznym[6].

2. **W celu zapewnienia równych warunków działania operatorom na rynku wewnętrznym**

W dyrektywie w sprawie bezpieczeństwa sieci i informacji zobowiązano państwa członkowskie do ustanowienia wymogów w zakresie bezpieczeństwa oraz procedury zgłaszania incydentów, których mają przestrzegać OUK. Ze względu na to, że dyrektywa jest zgodna podejściem opartym na zasadzie minimalnej harmonizacji w odniesieniu do OUK, państwa członkowskie mają swobodę w zakresie nakładania na operatorów bardziej rygorystycznych wymogów niż te, które przewiduje dyrektywa. Chociaż takie środki wzmacniają odporność państw członkowskich, mogą jednak również przyczyniać się do powstania dodatkowych kosztów regulacyjnych dla przedmiotowych operatorów. W związku z tym ważne jest, aby operatorzy świadczący podobne usługi o podobnym znaczeniu podlegali podobnym uregulowaniom.

3. **W celu zmniejszenia ryzyka rozbieżności w interpretacji dyrektywy**

Dyrektywę opracowano w taki sposób, aby zapewnić państwom członkowskim pole manewru w wyborze odpowiednich podmiotów z uwzględnieniem specyfiki krajowej. Podejście to zwiększa jednocześnie ryzyko rozbieżności we wdrażaniu przepisów dyrektywy i może potencjalnie prowadzić do niespójności w zakresie środków wprowadzanych przez państwa członkowskie. Ma to szczególne znaczenie dla przedsiębiorstw, które prowadzą działalność w kilku państwach i w związku z tym są zobowiązane do spełnienia wymogów regulacyjnych więcej niż jednego państwa członkowskiego.

[6] Zdaniem grupy współpracy ds. bezpieczeństwa sieci i informacji otwartość rynku wewnętrznego dla usług może prowadzić do „transgranicznych ryzyk i zależności mających zasadniczy wpływ na dostępność, integralność oraz poufność takich usług”.

4. **W celu opracowania kompleksowego przeglądu poziomu odporności w dziedzinie cyberbezpieczeństwa w całej UE**

   OUK podlegają działaniom nadzorczym, które mają na celu weryfikację skutecznego wdrażania polityk w zakresie bezpieczeństwa oraz powiadamiania o istotnych incydentach. Nadzór sprzyja nawiązaniu ściślejszej współpracy między sektorem publicznym i prywatnym, prowadząc do rozwoju wspólnej wiedzy na temat gotowości w dziedzinie cyberbezpieczeństwa w danym państwie członkowskim. Grupa współpracy umożliwia wspólne dzielenie się doświadczeniami krajowymi na poziomie UE, w tym informacjami dotyczącymi zgłoszonych incydentów[7], oraz wykorzystywanie ich do dokładniejszej oceny najpoważniejszych zagrożeń i najistotniejszych potrzeb. Aby jednak działanie to było skuteczne, wymiana takich informacji powinna opierać się na wspólnym zrozumieniu kwestii tego, które podmioty należy identyfikować jako OUK.

1.2 Procedura identyfikacji określona w dyrektywie w sprawie bezpieczeństwa sieci i informacji

W załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji znajduje się wykaz siedmiu sektorów oraz odpowiadających im podsektorów i rodzajów podmiotów istotnych z punktu widzenia procesu identyfikacji (tabela 1). W art. 5 ust. 3 zobowiązano państwa członkowskie do ustanowienia wykazu usług kluczowych w oparciu o te sektory, podsektory oraz rodzaje podmiotów. Dzięki przyjętemu w dyrektywie podejściu opartemu na zasadzie minimalnej harmonizacji państwa członkowskie mogą wykroczyć poza zakres stosowania załącznika II i przeprowadzić identyfikację w dodatkowych sektorach i podsektorach.

[7] Zgodnie z art. 10 ust. 3 dyrektywy w sprawie bezpieczeństwa sieci i informacji państwa członkowskie co roku przekazują grupie sprawozdanie podsumowujące na temat otrzymanych zgłoszeń dotyczących incydentów.

Sektor	Podsektor
1. Energetyka	a) Energia elektryczna
	b) Ropa naftowa
	c) Gaz
2. Transport	a) Transport lotniczy
	b) Transport kolejowy
	c) Transport wodny
	d) Transport drogowy
3. Bankowość	
4. Infrastruktura rynków finansowych	
5. Służba zdrowia	
6. Zaopatrzenie w wodę pitną i jej dystrybucja	
7. Infrastruktura cyfrowa	

Tabela 1: Sektory i podsektory wymienione w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji

W art. 5 ust. 2 określono trzy **kryteria**, które państwa członkowskie mają stosować do identyfikacji operatorów usług kluczowych:

1. podmiot, którego dotyczy procedura identyfikowania, musi świadczyć **usługę, która ma kluczowe znaczenie** dla utrzymania krytycznej działalności społecznej lub gospodarczej. W tym celu właściwe organy krajowe muszą korzystać z ustanowionych wcześniej wykazów usług kluczowych;
2. świadczone usługi muszą **zależeć od sieci i systemów informatycznych**;
3. incydent musiałby mieć istotne **skutki zakłócające** dla świadczenia danej usługi. W art. 6 stwierdzono, że istotność incydentu należy ocenić, korzystając z **czynników międzysektorowych** oraz, w stosownych przypadkach, **czynników sektorowych**[8].

Ponadto zgodnie z art. 5 ust. 4 dyrektywy państwa członkowskie zobowiązane są do konsultowania się ze sobą, jeżeli stwierdzą, że potencjalny OUK świadczy usługi w więcej niż jednym państwie członkowskim. Ta obowiązkowa procedura ma pomóc państwom

[8] Jako przykłady czynników międzysektorowych można wskazać liczbę użytkowników korzystających z usługi lub udział danego podmiotu w rynku. Przykładowe czynniki sektorowe obejmują liczbę systemów autonomicznych podłączonych do punktu wymiany ruchu internetowego (IXP) lub roczną liczbę transakcji przeprowadzonych przez instytucję finansową.

członkowskim w ocenie ewentualnego wpływu cyberincydentu na podmioty prowadzące działalność transgraniczną oraz służyć jako ochrona dla przedsiębiorstw objętych tą procedurą w innych państwach członkowskich.

1.3 Metodyka sprawozdania

Podstawę wyników przedstawionych w niniejszym sprawozdaniu stanowi ocena przeprowadzona w okresie od listopada 2018 r. do września 2019 r. Wiele państw członkowskich nie udostępniło Komisji na czas informacji wymaganych do sporządzenia niniejszego sprawozdania. Przyjęcie sprawozdania należało zatem przełożyć na termin późniejszy niż dzień 9 maja 2019 r. przewidziany w art. 23 ust. 1 dyrektywy w sprawie bezpieczeństwa sieci i informacji. Dane zgromadzono za pośrednictwem wielu kanałów: informacji przekazywanych przez państwa członkowskie w oparciu o standardowy wzór opracowany przez ENISA, standaryzowanych rozmów z wybranymi organami krajowymi, spotkań grupy współpracy, w tym warsztatów poświęconych temu zagadnieniu, które odbyły się dnia 19 marca 2019 r.

W oparciu o zgromadzone informacje w sprawozdaniu przeprowadzono ocenę stopnia spójności podejść do identyfikacji przyjętych przez poszczególne państwa członkowskie poprzez:

1. porównywanie poszczególnych metod identyfikacji wybranych przez organy krajowe;
2. analizę wykazów usług kluczowych oraz progów wybranych przez państwa członkowskie;
3. analizę liczby OUK w poszczególnych państwach członkowskich.

W sprawozdaniu dokonano również oceny wdrożenia przepisów dyrektywy dotyczących transgranicznej procedury konsultacji (art. 5 ust. 4) oraz zasady *lex specialis* (art. 1 ust. 7). Przedstawiono w nim analizę faktyczną procesu identyfikacji prowadzonego przez państwa członkowskie oraz wstępne wnioski i pytania otwarte do dalszej refleksji.

1.4 Dostępność danych

Przepisy dyrektywy w sprawie bezpieczeństwa sieci i informacji nakładają na państwa członkowskie obowiązek przekazywania Komisji jedynie ograniczonego zbioru danych.

Organy krajowe nie mają na przykład obowiązku przekazywania nazw zidentyfikowanych podmiotów, co utrudnia służbom Komisji porównywanie wyników procesu identyfikacji pod kątem kompletności wykazu oraz wpływu na przedsiębiorstwa tej samej wielkości i należących do tego samego sektora.

Zgodnie z art. 5 ust. 7 wszystkie państwa członkowskie powinny przekazać informacje niezbędne do celów niniejszego sprawozdania nie później niż dnia 9 listopada 2018 r. Do tego dnia istotne dane przekazało jednak tylko 15 państw (zob. załączona tabela w sekcji 4.1). Pomimo wielokrotnych upomnień ze strony Komisji pozostały istotne luki w danych. W związku z tym dnia 26 lipca 2019 r. Komisja skierowała do sześciu państw członkowskich[9] wezwanie do usunięcia uchybienia, wzywając je do przekazania brakujących danych w terminie dwóch miesięcy.

Na dzień publikacji niniejszego sprawozdania wszystkie dane wymagane na podstawie art. 5 ust. 7 przekazały 23 państwa członkowskie: Bułgaria, Chorwacja, Cypr, Dania, Estonia, Finlandia, Francja, Grecja, Hiszpania, Irlandia, Litwa, Luksemburg, Łotwa, Malta, Niderlandy, Niemcy, Polska, Portugalia, Republika Czeska, Szwecja, Słowacja, Włochy i Zjednoczone Królestwo. Pozostałe pięć państw członkowskich (Austria, Belgia, Słowenia, Rumunia i Węgry) przekazało tylko częściowe dane na temat zidentyfikowanych krajowych OUK, gdyż państwa te nie zdołały ukończyć procesu identyfikacji przed publikacją niniejszego sprawozdania.

[9] Austrii, Belgii, Grecji, Rumunii, Słowenii i Węgier.

2. Identyfikacja OUK w państwach członkowskich

W dyrektywie w sprawie bezpieczeństwa sieci i informacji ustanowiono ramy identyfikacji operatorów usług kluczowych, które zapewniają państwom członkowskim swobodę w zakresie uwzględniania specyfiki krajowej. W związku z tym państwa członkowskie opracowały szeroką gamę praktyk identyfikacyjnych.

2.1 Metody stosowane przez państwa członkowskie

Państwa członkowskie opracowały różne metody identyfikacji operatorów, w pełni korzystając z elastyczności, jaką zapewnia im dyrektywa w sprawie bezpieczeństwa sieci i informacji. Jednym z elementów mających wpływ na metody krajowe było wcześniejsze istnienie ram, takich jak Dyrektywa Rady 2008/114/WE w sprawie infrastruktury krytycznej[10] czy inne przepisy krajowe dotyczące „ważnych podmiotów". W takich przypadkach państwa członkowskie korzystały ze swojego wcześniejszego doświadczenia jako punktu odniesienia oraz uwzględniały specyfikę dyrektywy w sprawie bezpieczeństwa sieci i informacji w istniejących metodach.

Różnice w zakresie metod krajowych można przyporządkować do następujących głównych kategorii: usługi kluczowe, wykorzystanie progów, stopień centralizacji, organy odpowiedzialne za identyfikację oraz ocena zależności od sieci i systemów informatycznych. Ze względu na duże znaczenie usług kluczowych i progów dla oceny spójności w zakresie identyfikacji OUK analizie tych kwestii poświęcono oddzielne sekcje. Pozostałe kryteria omówiono w niniejszej sekcji.

Stopień centralizacji

Większość państw członkowskich zdecydowało się powierzyć część procesów decyzyjnych dotyczących różnych elementów procesu identyfikacji organom sektorowym (ministerstwom, agencjom itp.). Stopień decentralizacji różni się w poszczególnych przypadkach, przy czym większość państw członkowskich jako jednostkę odpowiedzialną za przekazywanie wskazówek organom sektorowym oraz konsolidowanie informacji wyznaczyło jeden organ.

[10] 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. Dyrektywa ta ma na celu wzmocnienie ochrony infrastruktury krytycznej w sektorach energetyki i transportu.

Niektóre państwa zdecydowały się jednak na powierzenie procesu identyfikacji jednemu organowi. Istnieją również przypadki wyjątkowo wysokiego stopnia decentralizacji, gdy organy sektorowe odpowiedzialne są za tworzenie własnych metod.

Wiele państw członkowskich dokładnie rozważyło poszczególne aspekty struktury instytucjonalnej identyfikacji OUK. Organy wskazują, że jedną z zalet scentralizowanej identyfikacji jest unikanie konfliktu interesów: operatorzy najwyraźniej niechętnie ujawniają istotne informacje sektorowym organom regulacyjnym, ponieważ boją się, że informacje te mogłyby również posłużyć do innych celów regulacyjnych.

Z drugiej strony podejścia zdecentralizowane wydają się wspierać dialog wśród właściwych organów zajmujących się bezpieczeństwem sieci i informacji (zarówno zajmujących się cyberbezpieczeństwem, jak i sektorowych), pomagając im w lepszej identyfikacji konsekwencji występowania zależności międzysektorowych. Ponadto organy sektorowe zwykle rozumieją sektory lepiej niż organy wiodące.

Procedura identyfikacji (odgórna i oddolna)

Kolejną ważną różnicę można zauważyć między państwami członkowskimi, w których proces identyfikacji przeprowadzają organy publiczne (identyfikacja odgórna), a państwami członkowskimi, w których operatorów rynkowych wzywa się do samodzielnego sprawdzenia, czy spełniają wymogi operatorów usług kluczowych (tzw. identyfikacja oddolna lub samoidentyfikacja). Aby to ostatnie podejście było skuteczne, państwa członkowskie powinny ustanowić kary, które będą wystarczająco wysokie, aby zniechęcić operatorów do nieujawniania się, jak określono w art. 21 dyrektywy w sprawie bezpieczeństwa sieci i informacji. W większości przypadków proces identyfikacji jest odgórny. W praktyce organy często polegają jednak częściowo na pewnych elementach samooceny, takich jak kwestionariusze, które mają być wypełniane przez potencjalnych OUK.

Jeżeli zasady i progi regulujące identyfikację OUK są wyraźne i przejrzyste, zarówno identyfikacja odgórna, jak i identyfikacja oddolna powinny przynieść podobne efekty. Wybór jednego podejścia względem drugiego nie powinien mieć zatem co do zasady żadnego wpływu na spójność.

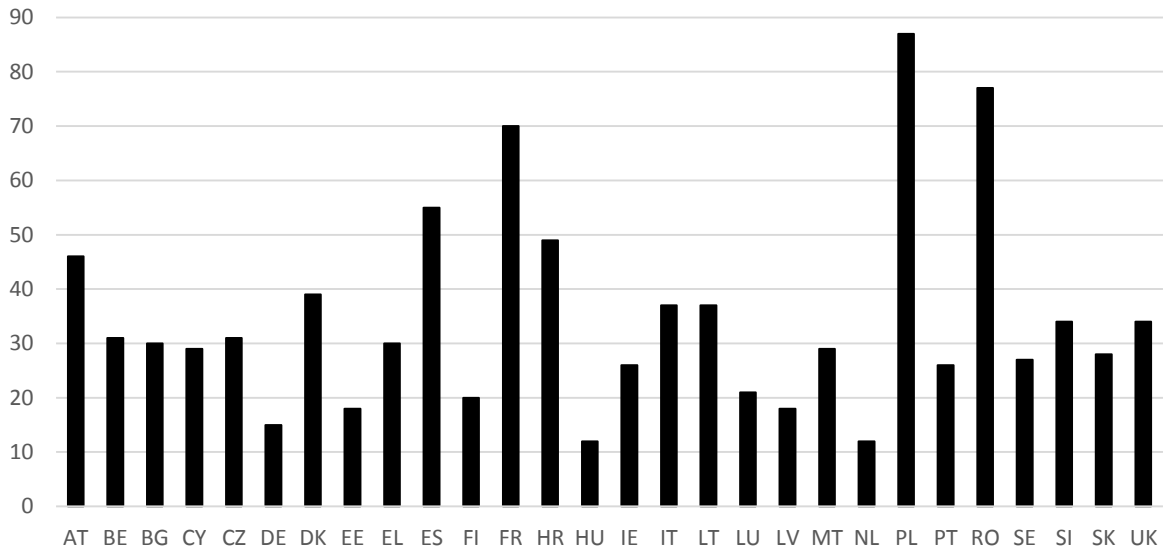
Ocena zależności od sieci

Jak wyjaśniono w sekcji 1.2, w art. 5 ust. 2 lit. b) zobowiązano państwa członkowskie do oceny zależności operatora od sieci i systemów informatycznych w ramach procedury identyfikacji OUK. Podczas stosowania tych kryteriów szereg państw członkowskich uznaje zależność od sieci i systemów informatycznych za rzecz oczywistą w obecnej gospodarce cyfrowej. Niektóre organy dokonują jednak wyboru bardziej wyszukanych praktyk, przeprowadzając na przykład szczegółowe oceny lub prosząc operatorów o samoocenę stopnia ich zależności.

2.2 Identyfikacja usług

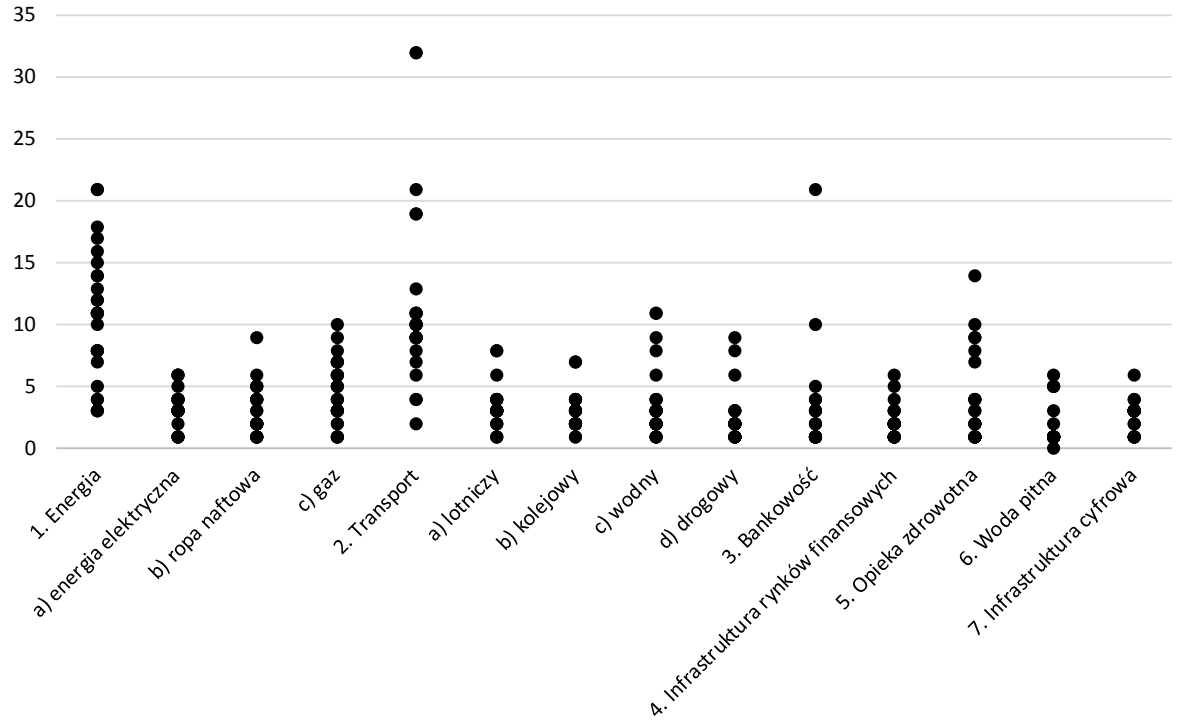
W motywie 23 dyrektywy w sprawie bezpieczeństwa sieci i informacji wyraźnie wymieniono wykazy usług kluczowych jako wkład, który należy wykorzystywać do „oceny praktyk regulacyjnych poszczególnych państw członkowskich z myślą o zapewnieniu ogólnego poziomu spójności". Ze względu na to, że wykazy usług kluczowych ustanawiane przez państwa członkowskie służą jako podstawa identyfikacji operatorów, różnice w zidentyfikowanych usługach mogłyby prowadzić do niespójnej identyfikacji operatorów w poszczególnych państwach członkowskich, w szczególności jeśli określone usługi świadczone we wszystkich państwach są identyfikowane tylko przez niektóre państwa członkowskie.

Liczba zidentyfikowanych przez państwa członkowskie usług uwzględnionych w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji, które zgłoszono Komisji, znacząco różni się w poszczególnych państwach członkowskich (dane liczbowe wszystkich państw członkowskich znajdują się w załączniku do sekcji 4.2). Na państwo członkowskie przypada średnio 35 usług, a liczba zidentyfikowanych usług waha się od 12 do 87, jak przedstawiono na rys. 1. Mimo że większe państwa członkowskie identyfikują zwykle nieco więcej usług niż mniejsze państwa członkowskie, wydaje się, że nie ma silnej korelacji między wielkością państwa członkowskiego a liczbą zidentyfikowanych usług. Właśnie tego należy oczekiwać, ponieważ w praktyce konsumenci i przedsiębiorstwa mają zwykle dostęp do takich samych rodzajów usług we wszystkich państwach członkowskich, niezależnie od ich wielkości.



Wykres 1: Ogólna liczba usług kluczowych zidentyfikowanych przez państwa członkowskie

Liczba zidentyfikowanych usług nie tylko różni się w przypadku państw członkowskich jako całości, lecz również w przypadku dokładniejszej analizy sektorów i podsektorów. Na przykład w sektorze bankowym liczba zidentyfikowanych usług waha się od 1 do 21. Jak przedstawiono na rys. 2, zakres zidentyfikowanych usług znacznie różni się w poszczególnych państwach w przypadku większości sektorów i podsektorów.



Wykres 2: Liczba usług zidentyfikowanych przez państwa członkowskie w każdym sektorze i podsektorze. Każdy punkt danych odzwierciedla liczbę usług zidentyfikowanych przez państwo członkowskie w odpowiednim (pod)sektorze[11].

W pewnym stopniu liczby przedstawione na rys. 2 odzwierciedlają różne podejścia metodologiczne poszczególnych państw. Na przykład w ramach identyfikacji usług niektóre państwa członkowskie podjęły decyzję o stosowaniu podejścia bardziej szczegółowego niż inne państwa członkowskie, w związku z czym liczby w takich państwach członkowskich są wyższe. Z danych, które Komisja otrzymała od państw członkowskich, wynika jednak wyraźnie, że różnice w liczbach są również spowodowane niespójnościami w podejściach wybranych przez państwa członkowskie, o czym świadczą przykłady podsektorów energii elektrycznej i transportu kolejowego:

[11] Identyczne punkty danych pokrywają się. W związku z tym na wykresie nie widać wszystkich 28 punktów danych. Na przykład 17 państw członkowskich zidentyfikowało dokładnie trzy usługi kluczowe w ramach infrastruktur cyfrowych.

Estonia (najmniej szczegółowe podejście)	Portugalia	Dania	Bułgaria (najbardziej szczegółowe podejście)
Dostawy energii elektrycznej	Operatorzy systemu dystrybucyjnego	Dystrybucja energii elektrycznej	Dystrybucja energii elektrycznej
			Zapewnienie funkcjonowania i utrzymania systemu dystrybucji energii elektrycznej
	Operator systemu przesyłowego	Przesył energii elektrycznej	Przesył energii elektrycznej
			Eksploatacja, utrzymywanie oraz rozbudowa sieci przesyłowej energii elektrycznej
	(luki w zakresie spójności)	Produkcja energii elektrycznej	Produkcja energii elektrycznej
	(luki w zakresie spójności)	*(luki w zakresie spójności)*	Rynek energii elektrycznej

Tabela 2: Poglądowe przykłady podejść wybranych przez państwa członkowskie w ramach identyfikacji usług kluczowych w podsektorze energii elektrycznej

W tabeli 2 porównano niektóre ze sposobów identyfikacji przez państwa członkowskie usług kluczowych w podsektorze energii elektrycznej. Niektóre państwa (m.in. Estonia) wybrały podejście bardzo ogólne umożliwiające identyfikację praktycznie każdego operatora w podsektorze energii elektrycznej, którego uznają za kluczowy. Inne państwa (m.in. Portugalia, Dania i Bułgaria) zdecydowały się na znacznie bardziej szczegółowe podejście. Na przykład Bułgaria sporządziła niezwykle szczegółowy wykaz usług, który zawiera nawet usługę nieuwzględnioną w załączniku II (rynki energii elektrycznej). Portugalia i Dania zastosowały jednak podejście szczegółowe, nie decydując się na uwzględnienie pewnych usług, które zostały ujęte przez inne państwa. Może to doprowadzić do nierównych warunków działania w gronie OUK na rynku wewnętrznym.

Luki w zakresie spójności, takie jak luki zidentyfikowane w tabeli 2, wynikają z różnych sposobów wdrażania przez poszczególne państwa dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz w przypadku sektorów niewchodzących w zakres załącznika II (takich jak rynki energii elektrycznej) są konsekwencją stosowania podejścia opartego na zasadzie

minimalnej harmonizacji. Luki w zakresie spójności nie oznaczają zatem koniecznie, że państwa członkowskie, które nie zidentyfikowały pewnej usługi, niepoprawnie zastosowały przepisy dyrektywy.

W tabeli 3 przedstawiono podejścia wybrane przez cztery państwa w odniesieniu do podsektora transportu kolejowego. Francja sporządziła bardzo szczegółowy i kompleksowy wykaz usług kluczowych dla funkcjonowania transportu kolejowego, natomiast pozostałe trzy państwa wybrały jedynie niewielki podzestaw tych usług. W przypadku Polski nie jest do końca jasne, które usługi należą do kategorii „transportu kolejowego towarów" i „transportu kolejowego pasażerów". Ich nazwy są na tyle ogólne, że mogłyby równie dobrze obejmować niektóre z usług zidentyfikowanych przez Francję, takich jak „kontrola ruchu kolejowego i zarządzanie ruchem kolejowym". Warto zauważyć, że Komisja nie dysponuje środkami, aby zbadać bardziej szczegółowo takie przypadki: w dyrektywie w sprawie bezpieczeństwa sieci i informacji nie zobowiązano organów krajowych do ujawnienia bardziej szczegółowych informacji.

Finlandia	Francja	Irlandia	Polska
Zarządzanie infrastrukturą państwową	Utrzymanie infrastruktury	Zarządcy infrastruktury	*(luki w zakresie spójności)*
(luki w zakresie spójności)	Utrzymanie taboru kolejowego	*(luki w zakresie spójności)*	*(luki w zakresie spójności)*
Usługi zarządzania ruchem	Kontrola ruchu kolejowego i zarządzanie ruchem kolejowym	*(luki w zakresie spójności)*	Przygotowywanie rozkładów jazdy pociągów
(luki w zakresie spójności)	Przewóz towarów i materiałów niebezpiecznych	Przedsiębiorstwa kolejowe	Transport kolejowy towarów
(luki w zakresie spójności)	Przewóz pasażerów		Transport kolejowy pasażerów
(luki w zakresie spójności)	Metro, tramwaje i inne przewozy lekkimi pojazdami szynowymi (w tym koleje podziemne)		*(luki w zakresie spójności)*
(luki w zakresie spójności)	Przewozy kolejowe	*(luki w zakresie spójności)*	*(luki w zakresie spójności)*

Tabela 3: Poglądowe przykłady podejść wybranych przez państwa członkowskie w ramach identyfikacji usług kluczowych w podsektorze transportu kolejowego

Państwa członkowskie przedstawione w tabeli 2 i tabeli 3 zostały wybrane jedynie w celach poglądowych oraz dlatego, że ich podejścia metodyczne umożliwiają łatwe porównanie. Większość innych państw członkowskich wybrała podobne usługi i w związku z tym wykazują podobne „luki w zakresie spójności". „Luki w zakresie spójności" takie jak luki dotyczące podsektorów energii elektrycznej i transportu kolejowego istnieją bowiem we wszystkich państwach członkowskich i sektorach uwzględnionych w załączniku II do dyrektywy. Większość przypadków niespójności jest spowodowana zidentyfikowaniem usług jedynie w niektórych, a nie we wszystkich państwach członkowskich. Pełne wykazy usług w podsektorach energii elektrycznej i transportu kolejowego obejmujące wszystkie państwa członkowskie można znaleźć w załączniku do niniejszego sprawozdania.

2.3 Progi

Chociaż większość państw członkowskich stosuje progi w celu identyfikacji OUK, rola, jaką odgrywają te progi, jest różna w poszczególnych państwach. W zakresie progów międzysektorowych można zdefiniować progi opierające się na:

- pojedynczym czynniku ilościowym (np. liczba użytkowników zależnych od danej usługi) w celu określenia, czy podmiot należy uznać za OUK w kontekście określonej usługi;
- większym zestawie czynników ilościowych (np. liczba użytkowników zależnych od danej usługi i udział w rynku);
- połączeniu czynników ilościowych i jakościowych.

Ponadto zgodnie z dyrektywą oprócz progów międzysektorowych państwa członkowskie mogą stosować również progi sektorowe. Dzięki temu organy krajowe mają większą swobodę podczas procesu identyfikacji, co pozwala im uwzględnić specyfikę danego państwa i sektora. Jednocześnie prowadzi to do powstania bardzo skomplikowanego zestawu progów, co może mieć negatywny wpływ na ogólną spójność identyfikacji OUK.

Przykład takiej różnorodności podejść przedstawiono w tabeli 4. Przykład ten ilustruje, że progi wybrane przez państwa członkowskie w odniesieniu do sektora infrastruktury cyfrowej różnią się nie tylko pod względem ilościowym (na przykład w Niemczech dostawcy usług DNS są identyfikowani jako OUK, jeżeli zarządzają co najmniej 250 000 domen, natomiast Polska ustaliła ten próg na poziomie 100 000 domen), ale również pod względem jakościowym (na przykład „liczba podłączonych systemów autonomicznych" w stosunku do „udziału w rynku").

Same spójnie wybrane progi ilościowe nie zapewniają pełnej spójności między podejściami krajowymi. Biorąc pod uwagę, że w niektórych państwach członkowskich progi stanowią jedynie jedno z kryteriów identyfikacji OUK, wyniki procesu identyfikacji mogą wciąż być bardzo różne, nawet w przypadku stosowania podobnych progów. Na przykład niektóre państwa członkowskie stosują złożone systemy punktacji obejmujące kilka czynników będących częścią jednego wzoru[12]. Czynniki te mogą na przykład obejmować zależność podmiotu od sieci i systemów informatycznych lub niektóre z czynników, o których mowa

[12] Na przykład jedno państwo członkowskie opracowało siedem czynników (cztery tak zwane „czynniki zależne od operatora" i trzy „czynniki zależne od wpływu"), które były częścią jednego wzoru. Jeżeli ostateczny wynik obliczenia przekracza pewien próg, dany operator uznawany jest za OUK.

w art. 6 ust. 1 dyrektywy w sprawie bezpieczeństwa sieci i informacji. Ponadto niektóre państwa członkowskie nie stosują progów w ogóle lub stosują progi wyłącznie we wstępnej fazie oceny. Rozważania te są ważne nie tylko w odniesieniu do sektora infrastruktury cyfrowej, ale również w odniesieniu do wszystkich sektorów uwzględnionych w załączniku II.

Ustalenie odpowiedniego progu może stanowić wyzwanie, zwłaszcza w przypadku sektorów, które charakteryzują się obecnością wielu małych operatorów. Przykładem takiej różnorodności jest wiele małych zakładów opieki zdrowotnej (np. kliniki lub służby ratownictwa medycznego), które świadczą usługi kluczowe na rzecz stosunkowo niewielkiej liczby użytkowników, ale których niedostępność, wynikająca z cyberincydentu, mogłaby doprowadzić do śmierci pacjentów. Inny problem pojawia się, gdy funkcjonowanie łańcuchów dostaw jest uzależnione od usług świadczonych przez operatorów, którzy stanowią małe, ale jednak kluczowe ogniwa łańcucha (na przykład w sektorach takich jak logistyka[13]). Jedno państwo członkowskie rozważa zastosowanie kryteriów związanych ze znaczeniem lub kluczowym charakterem świadczonej usługi jako potencjalne rozwiązanie tego problemu.

[13] Sektor logistyki nie został uwzględniony w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji.

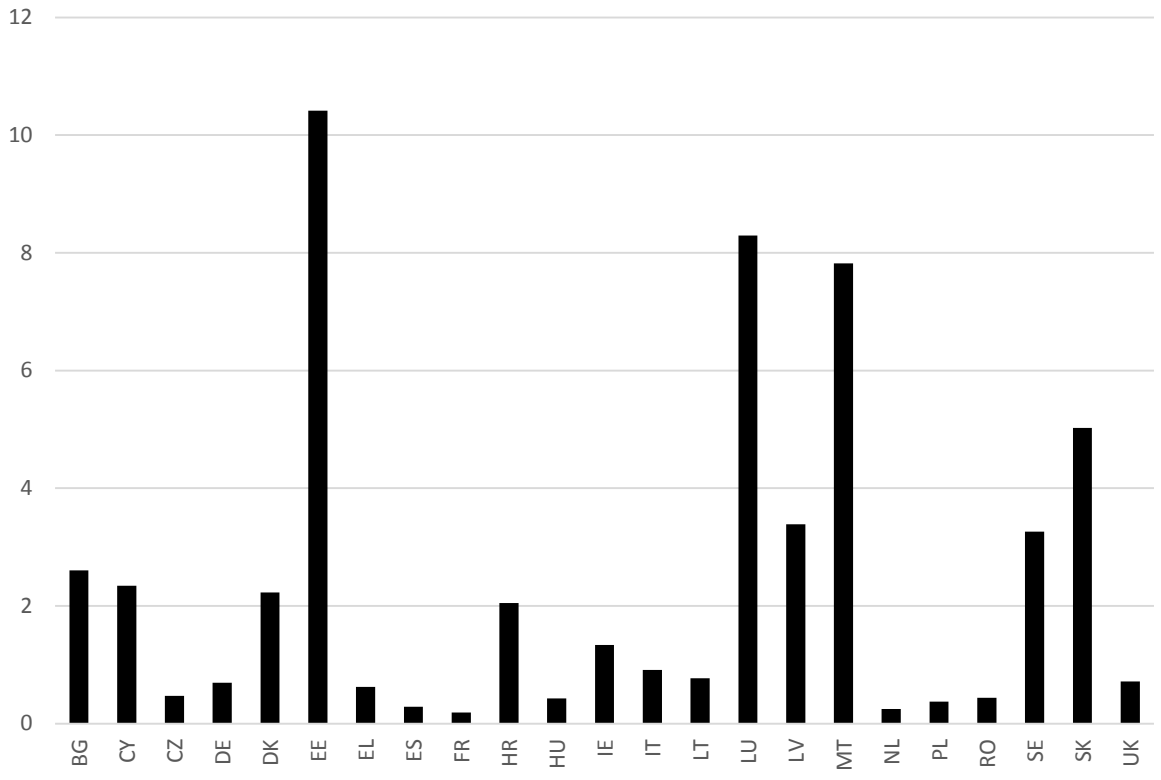
Państwo	Punkty wymiany ruchu internetowego (IXP)	Dostawcy usług DNS	Rejestry nazw domen najwyższego poziomu
Stosowanie głównie progów sektorowych			
AT	podłączone systemy autonomiczne >100	Funkcje rozpoznawania nazw z systemu nazw domen: 88 000 użytkowników; serwery zwierzchnie DNS: 50 000 domen	50 000 domen
DE	podłączone systemy autonomiczne >300	Funkcje rozpoznawania nazw z systemu nazw domen: 100 000 użytkowników; serwery zwierzchnie DNS: 250 000 domen	*(usługa niezidentyfikowana)*
DK	średnia dzienna ilość danych >200 Gb/s	Funkcje rozpoznawania nazw z systemu nazw domen: 100 000 użytkowników; serwery zwierzchnie DNS: 100 000 domen	500 000 domen
EE	*(usługa niezidentyfikowana)*	*(usługa niezidentyfikowana)*	Rejestr domen najwyższego poziomu państwa
FI	*(usługa niezidentyfikowana)*	*(usługa niezidentyfikowana)*	Rejestry domen najwyższego poziomu państwa i regionu
FR	*(brak oficjalnego progu)*	*(brak oficjalnego progu)*	*(brak oficjalnego progu)*
HR	podłączeni członkowie >15	Usługi DNS dla domen najwyższego poziomu państwa	Rejestr domen najwyższego poziomu państwa
IE	*(próg nieznany)*	Funkcje rozpoznawania nazw z systemu nazw domen: 100 mln zapytań na dobę; serwery zwierzchnie DNS: 50 000 domen	Rejestr domen najwyższego poziomu państwa
MT	25 % udziału w rynku	Funkcje rozpoznawania nazw z systemu nazw domen: 78 000 wniosków dziennie; serwery zwierzchnie DNS: 7 800 domen	750 000 zapytań dziennie
PL	podłączone systemy autonomiczne ≥100	Serwery zwierzchnie DNS: 100 000 domen	Rejestry domen najwyższego poziomu dla co najmniej 100 000 abonentów
SE	*(usługa niezidentyfikowana)*	Funkcje rozpoznawania nazw z systemu nazw domen: 100 000 użytkowników; serwery zwierzchnie DNS: 25 000 domen	250 000 domen
SK	*System autonomiczny łączący co najmniej dwa inne systemy autonomiczne przy 2 Gb/s*	Funkcje rozpoznawania nazw z systemu nazw domen: 3 mln zapytań na dobę; serwery zwierzchnie DNS: >1 000 domen	Rejestr domen najwyższego poziomu

UK	udziału w rynku >50 % lub wzajemne połączenie z globalnymi szlakami internetowymi ≥50 %	Funkcje rozpoznawania nazw z systemu nazw domen: 2 000 000 klientów dziennie; serwery zwierzchnie DNS: 250 000 domen	Rejestry domen najwyższego poziomu ≥2 mld zapytań dziennie
Stosowanie progów międzysektorowych			
CY	50 000 użytkowników lub 5 % abonentów rynku	50 000 użytkowników lub 5 % abonentów rynku	50 000 użytkowników lub 5 % abonentów rynku
LT	liczba mieszkańców >145 000	liczba mieszkańców >145 000	liczba mieszkańców >145 000
LU	100 % udziału w rynku	13 500 umów	100 % udziału w rynku

Tabela 4: Progi wybrane przez 16 państw członkowskich w odniesieniu do sektora infrastruktury cyfrowej

2.4 Liczba zidentyfikowanych operatorów

Wykaz usług kluczowych i progi są najważniejszymi wyznacznikami spójnej identyfikacji OUK. Z poprzednich sekcji wynika, że w obu przypadkach państwa członkowskie zastosowały przepisy dyrektywy w sprawie bezpieczeństwa sieci i informacji na różne sposoby, co wskazuje, że może to doprowadzić do problemu ze spójnością w przypadku późniejszej identyfikacji OUK. W niniejszej sekcji porównane zostaną liczby zidentyfikowanych w państwach członkowskich operatorów z sektorów i podsektorów uwzględnionych w załączniku II.

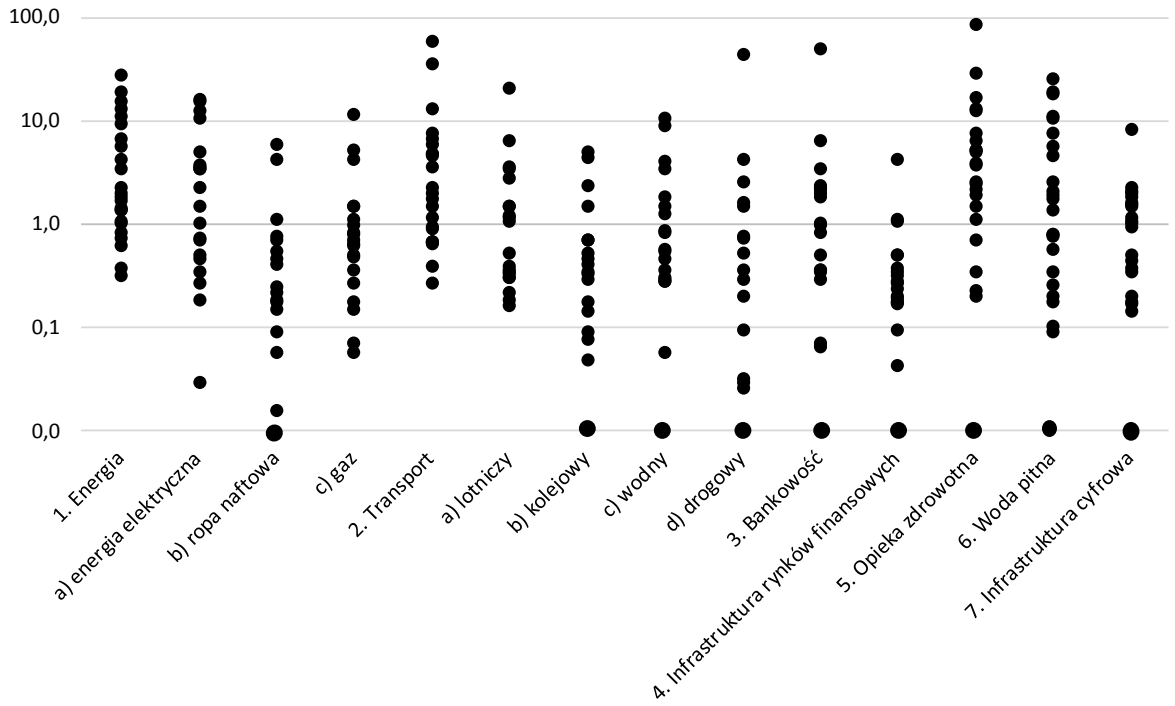


Wykres 3: OUK zidentyfikowani przez państwa członkowskie ze wszystkich sektorów uwzględnionych w załączniku II (na 100 000 mieszkańców, wartości oddalone i brakujące dane pominięto w celu zapewnienia czytelności)

Łączna liczba OUK zgłoszonych Komisji przez państwa członkowskie waha się od 20 do 10 897, wynosząc średnio 633 OUK na państwo członkowskie (dane liczbowe dotyczące wszystkich państw członkowskich można znaleźć w sekcji 4.2 załącznika do niniejszego sprawozdania). Ogólnie rzecz biorąc, istnieje wyraźny, pozytywny związek między wielkością państwa a liczbą zidentyfikowanych operatorów. Nie stanowi to jednak wystarczającego wyjaśnienia znacznych różnic w liczbach zgłoszonych przez państwa członkowskie. W celu uwzględnienia związku między wielkością i populacją na rys. 3 porównano liczby zgłoszonych OUK we wszystkich państwach członkowskich w przeliczeniu na 100 000 mieszkańców. Wynika z niego, że podejścia przyjęte przez państwa członkowskie w celu identyfikacji operatorów przyniosły bardzo zróżnicowane wyniki.

Bardziej dogłębne badanie sektorów i podsektorów wskazuje, że liczby zidentyfikowanych operatorów z wszystkich sektorów uwzględnionych w załączniku II różnią się znacznie w poszczególnych państwach członkowskich (rys. 4). Na przykład w sektorze energetycznym liczba ta waha się od 0,3 operatora do 29 operatorów na 1 000 000 mieszkańców. Dane

liczbowe dotyczące sektora bankowego wahają się od 0,07 operatora do 51 operatorów na 1 000 000 mieszkańców (bez uwzględnienia państw członkowskich, które nie zidentyfikowały w tym sektorze żadnego OUK).



Wykres 4: Liczba OUK zidentyfikowanych przez 25 państw członkowskich w każdym sektorze i podsektorze (na 1 000 000 mieszkańców, na skali logarytmicznej, wartości oddalone pominięto w celu zachowania czytelności). Każdy punkt danych odzwierciedla liczbę OUK zidentyfikowanych przez państwo członkowskie w odpowiednim (pod)sektorze[14].

2.5 Stosowanie dyrektywy do sektorów innych niż uwzględnione w załączniku II

Z badania przedłożonych danych wynika, że 11 spośród 28 państw członkowskich zidentyfikowało usługi kluczowe w sektorach nieobjętych zakresem stosowania załącznika II do dyrektywy. Z tych 11 państw członkowskich 7 zidentyfikowało łącznie 157 OUK świadczących usługi nieuwzględnione w wykazie rodzajów podmiotów w załączniku II.

[14] Identyczne punkty danych pokrywają się. W związku z tym na wykresie nie widać wszystkich 25 punktów danych. Na przykład zarówno Dania, jak i Niderlandy zidentyfikowały 0,35 OUK na 1 000 000 mieszkańców w podsektorze transportu lotniczego.

Dodatkowy sektor	Przykładowe podmioty	Liczba państw członkowskich
Infrastruktura informacyjna	Ośrodki przetwarzania danych, klastry serwerów	5
Usługi finansowe (podmioty niewymienione w załączniku II)	Zakłady ubezpieczeń i reasekuracji	4
Usługi publiczne	Usługi elektroniczne dla obywateli	4
Ciepło	Producenci i dostawcy ciepła	3
Ścieki	Zakłady odprowadzania i oczyszczania ścieków	3
Logistyka	Usługi pocztowe	2
Żywność	Producenci, systemy obrotu	2
Środowisko	Usuwanie odpadów niebezpiecznych	2
Krajowe służby bezpieczeństwa/ratunkowe	112, zarządzanie kryzysowe	2
Przemysł chemiczny	Dostawcy i producenci substancji	2
Usługi społeczne	Podmioty odpowiedzialne za świadczenia społeczne	1
Kształcenie	Organy odpowiedzialne za egzaminy państwowe	1
Żywienie zbiorowe	Zarządzanie dystrybucją	1
Woda	Obiekty hydrauliczne	1

Tabela 5: Sektory wybrane przez państwa członkowskie poza sektorami wymienionymi w załączniku II

Do najpopularniejszej kategorii należą infrastruktura informacyjna (zidentyfikowana przez pięć państw członkowskich), usługi finansowe świadczone przez podmioty niewymienione w załączniku II (zidentyfikowane przez cztery państwa członkowskie) i usługi publiczne (zidentyfikowane przez cztery państwa członkowskie) (tabela 5).

Z uwagi na kluczowy charakter cyberodporności dla funkcjonowania gospodarki i społeczeństwa jako całości szereg państw członkowskich podjęło decyzję o skorzystaniu z okazji, aby uwzględnić sektory inne niż tylko wymienione w załączniku II. Fakt, że kilka państw członkowskich podjęło decyzję o zastosowaniu dyrektywy w sprawie bezpieczeństwa sieci i informacji do dodatkowych sektorów, nasuwa pytanie, czy obecny zakres załącznika II

jest właściwy, aby spełnić cel polegający na ochronie wszystkich operatorów w Unii, których działalność jest kluczowa dla społeczeństwa i gospodarki.

2.6 Procedura konsultacji transgranicznych

W art. 5 ust. 4 dyrektywy w sprawie bezpieczeństwa sieci i informacji nałożono na państwa członkowskie obowiązek wzajemnej konsultacji przed podjęciem ostatecznej decyzji dotyczącej identyfikacji operatorów świadczących usługi w więcej niż jednym państwie członkowskim. Grupa współpracy opublikowała w lipcu 2018 r. dokument referencyjny, aby ułatwić państwom członkowskim przeprowadzanie prawidłowych konsultacji transgranicznych[15].

Na podstawie otrzymanych informacji jedynie kilka organów krajowych podjęło decyzję o nawiązaniu kontaktu ze swoimi odpowiednikami w innych państwach członkowskich i tylko dwa państwa członkowskie nawiązały wszechstronny kontakt z innymi państwami członkowskimi. Ponadto tylko kilka państw członkowskich stwierdziło, że zwróciły się do innych organów w mniej usystematyzowany sposób. Pomimo istotnego znaczenia usług transgranicznych na rynku wewnętrznym większość państw członkowskich nawiązała kontakt z innymi państwami członkowskimi jedynie w odniesieniu do bardzo ograniczonej liczby operatorów. Mimo że państwa członkowskie stosują tę procedurę w ograniczonym stopniu, wiele organów krajowych wyraziło zainteresowanie procesem konsultacji transgranicznych i uznaje go za ważny element ram identyfikacji bezpieczeństwa sieci i informacji. Kilka państw członkowskich wyraziło nawet obawę, że bez skutecznych konsultacji transgranicznych operatorzy mogą być zmuszeni spełnić wiele różnych wymogów regulacyjnych lub znajdą się w niekorzystnej sytuacji w porównaniu z innymi, nie tak ściśle uregulowanymi OUK działającymi na rynku.

Wraz z organami krajowymi Komisja wskazała kilka powodów, dla których procedura konsultacji nie jest jak dotąd stosowana zgodnie z założeniami:

---

[15] *Identification of Operators of Essential Services – Reference document on modalities of the consultation process in cases with cross-border impact* [Identyfikacja operatorów usług kluczowych – dokument referencyjny dotyczący warunków procesu konsultacji w przypadku wpływu transgranicznego], publikacja grupy współpracy z lipca 2018 r.

- wielu państwom członkowskim zidentyfikowanie OUK zajęło więcej czasu, niż zakładano. W związku z tym państwa, które wcześnie zidentyfikowały OUK, ich zdaniem nie były w stanie prowadzić konsultacji z tymi państwami;
- brak bezpiecznych kanałów przekazywania informacji: niektóre państwa członkowskie były niechętne komunikowaniu się ze swoimi odpowiednikami, traktując nazwy operatorów jako informacje niejawne;
- wysoka liczba istniejących zależności transgranicznych, która powodowała potrzebę nawiązania kontaktu ze znaczą liczbą zainteresowanych państw członkowskich, zwłaszcza w przypadku operatorów ogólnoeuropejskich;
- brak jednolitego sposobu rozumienia celów i zakresu konsultacji transgranicznych: niektóre państwa członkowskie uważają je wyłącznie za narzędzie wzajemnego informowania się o identyfikacji OUK mających wpływ transgraniczny, natomiast inne uznają, że konsultacje mają na celu dostosowanie progów i wymogów regulacyjnych. W motywie 24 dyrektywy zasugerowano, że jest to przede wszystkim procedura mająca na celu wspólną ocenę krytycznego charakteru operatora na potrzeby procesu identyfikacji;
- inny problem pojawia się, gdy dwa inne państwa członkowskie kontaktują się z państwem członkowskim w sprawie tego samego operatora. W takim przypadku dane państwo członkowskie może nie być w stanie dostosować swoich przepisów jednocześnie do przepisów obu państw członkowskich. W tym celu w motywie 24 przewidziano wielostronne rozmowy. Państwa członkowskie powinny korzystać z tej możliwości w celu zapewnienia spójności.

2.7 Uwzględnienie zasady stosowania przepisów szczególnych w procesie identyfikacji

Komisja zidentyfikowała pewien poziom niespójności wśród państw członkowskich w odniesieniu do stosowania zasady *lex specialis*. Doprowadziło to do niejednolitego stosowania dyrektywy, którego skutkiem jest z jednej strony identyfikacja OUK w przypadku stosowania zasad sektorowych, a z drugiej strony niewystarczający zakres identyfikacji OUK w niektórych sektorach uwzględnionych w załączniku II.

Art. 1 ust. 3 stanowi, że dyrektywa w sprawie bezpieczeństwa sieci i informacji nie ma zastosowania do przedsiębiorstw, które podlegają wymogom dyrektywy ramowej w sprawie łączności elektronicznej[16]. Wydaje się jednak, że niektóre państwa członkowskie zidentyfikowały OUK świadczące usługi, które w rzeczywistości powinny podlegać przepisom dyrektywy ramowej w sprawie łączności elektronicznej, takie jak usługi dostępu do internetu i telefonii.

Ponadto zgodnie z art. 1 ust. 7 przepisy dyrektywy w sprawie bezpieczeństwa sieci i informacji dotyczące wymogów bezpieczeństwa i zgłaszania incydentów nie mają zastosowania do operatorów, którzy podlegają już przepisom sektorowych aktów prawnych Unii, w których określono co najmniej równoważne obowiązki.

Chociaż większość państw członkowskich zidentyfikowała OUK w sektorach bankowym i rynków finansowych, kilka państw członkowskich nie zidentyfikowało OUK, twierdząc, że operatorzy świadczą usługi podlegające zasadom szczególnym.

Komisja nadal jest w trakcie gromadzenia szczegółowych informacji na temat stosowania zasady *lex specialis* określonej w dyrektywie w sprawie bezpieczeństwa sieci i informacji. Komisja przeprowadza obecnie szczegółowe kontrole prawodawstwa krajowego oraz wizyty kontrolne w państwach, aby ocenić obecny poziom transpozycji i wdrożenia, m.in. w odniesieniu do przepisów *lex specialis*. Na podstawie tych informacji Komisja zamierza dokładniej omówić zasadę *lex specialis* w ramach grupy współpracy, aby osiągnąć większą spójność między państwami członkowskimi.

[16] Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej.

3. Wnioski

W niniejszym sprawozdaniu oceniono podejścia, które państwa członkowskie wybrały w celu identyfikacji operatorów usług kluczowych (OUK) na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji. Ma ono na celu ocenę spójności praktyk stosowanych przez państwa członkowskie w świetle możliwego wpływu obecnych ram na funkcjonowanie rynku wewnętrznego i zarządzania zagrożeniami związanymi z cyberprzestępstwem.

Z przeprowadzonej analizy wynika, że w wielu państwach członkowskich dyrektywa w sprawie bezpieczeństwa sieci i informacji stanowiła katalizator, torując drogę dla rzeczywistej zmiany systemu instytucjonalnego i regulacyjnego w zakresie cyberbezpieczeństwa. Ponadto w związku z obowiązkiem identyfikacji operatorów usług kluczowych przeprowadzono kompleksową ocenę zagrożeń związanych z operatorami prowadzącymi działania kluczowe oraz nowoczesnych sieci i systemów informatycznych w niemal wszystkich państwach członkowskich. Można uznać to za osiągnięcie całej Unii zgodnie z celami dyrektywy.

Do celów niniejszego sprawozdania Komisja przeanalizowała krajowe metody identyfikacji, usługi, jakie organy krajowe uznają za kluczowe, progi identyfikacji oraz liczby OUK zidentyfikowanych w różnych sektorach uwzględnionych w dyrektywie:

- **państwa członkowskie opracowały zróżnicowane metody**, jeżeli chodzi o ogólne podejście do identyfikacji OUK (sekcja 2.1), ale również w odniesieniu do definicji usług kluczowych i ustalania progów. Może mieć to negatywny wpływ na spójne stosowanie przepisów dotyczących bezpieczeństwa sieci i informacji w całej Unii oraz możliwe konsekwencje dla prawidłowego funkcjonowania rynku wewnętrznego i skutecznego radzenia sobie z kwestiami zależności cybernetycznych;

- ponadto wydaje się, że **interpretacje państw członkowskich dotyczące tego, co stanowi usługę kluczową zgodnie z dyrektywą w sprawie bezpieczeństwa sieci i informacji, są rozbieżne**, ponieważ państwa członkowskie stosują różne poziomy szczegółowości (zob. sekcja 2.2). Utrudnia to porównanie wykazów usług kluczowych. Ponadto **istnieje ryzyko okrojenia zakresu dyrektywy** z uwagi na fakt, że niektórzy operatorzy podlegają dodatkowym regulacjom (ponieważ zostali zidentyfikowani przez odpowiednie państwo członkowskie), a inni świadczący podobne usługi pozostają wyłączeni z jej zakresu (ponieważ nie zostali zidentyfikowani). Aby zlikwidować te niespójności, należy

podjąć dodatkowe wysiłki na podstawie doświadczenia państw członkowskich, które mogłyby doprowadzić do bardziej spójnego wykazu usług kluczowych;

- ponadto w sprawozdaniu wykryto znaczne niespójności dotyczące sposobu stosowania progów przez państwa członkowskie (sekcja 2.3). Dalsze **ujednolicenie progów na poziomie UE** mogłoby przyczynić się do rozwiązania tego problemu. Takie prace można by prowadzić na przykład na forum sektorowych grup roboczych w ramach grupy współpracy, z uwzględnieniem specyfiki krajowej, m.in. szczególnych wymogów małych państw członkowskich;

- skorzystanie przez niektóre państwa z możliwości identyfikacji usług kluczowych w dodatkowych sektorach lub podsektorach nieuwzględnionych w załączniku II **wskazuje, że istnieją sektory potencjalnie narażone na cyberincydenty inne niż sektory określone w dyrektywie w sprawie bezpieczeństwa sieci i informacji** (sekcja 2.5). Identyfikacja OUK w sektorach takich jak infrastruktura informacyjna, usługi finansowe niewchodzące w zakres działalności podmiotów wymienionych w załączniku II oraz usługi publiczne może doprowadzić do poprawy cyberodporności organizacji w takich sektorach. Jednak w przypadku gdy tylko niektóre państwa członkowskie zidentyfikują OUK w takich sektorach, działanie to może mieć negatywne konsekwencje dla rynku wewnętrznego i równych szans, które powinno zapewniać.

Wiele metod i najlepszych praktyk, które opracowały organy krajowe, ma szczególną wartość i należy je wziąć pod uwagę w przyszłości, na przykład w ramach prac grupy współpracy i w procesie ciągłej identyfikacji OUK przez państwa członkowskie. Obecny poziom zróżnicowania może mieć jednak negatywny wpływ na osiągnięcie celów dyrektywy.

Komisja doszła do wstępnego wniosku, że chociaż dyrektywa w sprawie bezpieczeństwa sieci i informacji doprowadziła do rozpoczęcia kluczowego procesu w celu ulepszenia i poprawy praktyk związanych z zarządzaniem ryzykiem operatorów w sektorach krytycznych, istnieje znaczne rozdrobnienie praktyk w Unii, jeżeli chodzi o identyfikację OUK. Wynika to częściowo z konstrukcji dyrektywy, a częściowo z poszczególnych metod wdrażania stosowanych przez państwa członkowskie.

Państwa członkowskie powinny dążyć do stosowania przepisów dyrektywy w sprawie bezpieczeństwa sieci i informacji w najbardziej spójny sposób, wykorzystując w pełni wytyczne opracowane przez Komisję i grupę współpracy. Komisja wskazała zatem kilka

działań do podjęcia na szczeblu krajowym, które mogłyby przyczynić się do rozwiązania problemów przedstawionych w niniejszym sprawozdaniu:

- wiele państw członkowskich nie zakończyło procesu identyfikacji OUK w terminie określonym w dyrektywie. Ponadto na dzień publikacji niniejszego sprawozdania 23 państwa członkowskie przekazały wszystkie dane wymagane zgodnie z art. 5 ust. 7. Kolejne 5 państw członkowskich przekazało informacje częściowe. Komisja **wzywa organy krajowe odpowiedzialne za identyfikację do zakończenia tego procesu** tak szybko, jak to możliwe, oraz do jak najszybszego przekazania Komisji niezbędnych informacji;

- właściwe organy powinny dokonywać regularnego przeglądu swoich wykazów usług kluczowych oraz **zapewniać identyfikację wszystkich istniejących usług kluczowych**, aby ograniczyć liczbę „luk w zakresie spójności" w odniesieniu do usług kluczowych na rynku wewnętrznym;

- państwa członkowskie powinny w miarę możliwości aktywniej **komunikować się ze sobą, aby ujednolicać progi**, zwłaszcza w sektorach mających znaczący wymiar transgraniczny takich jak sektor transportu lub sektor energetyczny. Można to osiągnąć za pośrednictwem procedury konsultacji transgranicznych, o której mowa w art. 5 ust. 4 dyrektywy w sprawie bezpieczeństwa sieci i informacji, ale również dzięki lepszemu wykorzystaniu istniejących struktur grupy współpracy;

- organy krajowe powinny konsultować się wzajemnie w celu zapewnienia, by transgraniczni operatorzy **musieli spełnić podobne wymogi w zakresie bezpieczeństwa i zgłaszania incydentów** na rynku wewnętrznym. Ponadto państwa członkowskie powinny kontaktować się z takimi operatorami, aby zebrać więcej informacji na temat rozbieżności przepisów. Lepsza cyberodporność nie powinna odbywać się kosztem rozdrobnienia przepisów. W stosownych przypadkach państwa członkowskie powinny również prowadzić wielostronne rozmowy, jak przewidziano w motywie 24 dyrektywy w sprawie bezpieczeństwa sieci i informacji.

Poza działaniami na szczeblu krajowym istnieje szereg środków, które można potencjalnie wprowadzić na szczeblu unijnym i które doprowadziłyby do większej spójności. Komisja zainicjuje rozmowy w celu ulepszenia niejednolitego i niekiedy rozdrobnionego systemu identyfikacji. Potencjalne środki są następujące:

- **rola grupy współpracy ds. bezpieczeństwa sieci i informacji powinna zostać wzmocniona**, aby promować jednolite zrozumienie sposobu bardziej spójnego wdrażania dyrektywy. W tym celu Komisja zaproponuje, by istniejąca osobna grupa robocza ds. identyfikacji OUK dokonała szybkiego przeglądu **wytycznych w celu lepszego wyeliminowania istniejących niespójności**. Grupa współpracy powinna również przeanalizować utworzenie dodatkowych sektorowych grup roboczych[17] w celu zwiększenia spójności między państwami członkowskimi oraz zbadać możliwość wykorzystania specjalnego narzędzia komunikacyjnego w celu zacieśnienia współpracy w ramach grupy;

- tylko niewielka liczba państw członkowskich korzysta obecnie z **procedury konsultacji transgranicznych** w przypadku identyfikacji operatorów świadczących usługi kluczowe w więcej niż jednym państwie członkowskim. Aby usprawnić wymianę informacji, grupa współpracy powinna dokonać przeglądu swojego dokumentu referencyjnego dotyczącego warunków procesu konsultacji w przypadkach mających wpływ transgraniczny i uzgodnić spójną interpretację zakresu, celów i procedur takiego procesu. Jednocześnie Komisja przeanalizuje rozwiązania umożliwiające **bezpieczną wymianę informacji między właściwymi organami**;

- można stwierdzić, że wśród państw członkowskich istnieje pewien stopień niespójności w stosowaniu przepisów dyrektywy dotyczących zasady *lex specialis*. W związku z tym Komisja wykorzysta struktury grupy współpracy w celu **omówienia przypadków, w których stosowanie zasady *lex specialis* może być nieprawidłowe**.

Działania podjęte na szczeblu unijnym powinny gwarantować spójne ramy, uwzględniające zarówno działania sektorowe przewidujące szczególne lub wyższe wymogi w zakresie cyberbezpieczeństwa, jak i inne europejskie przepisy.

[17] Grupy robocze ds. energii i infrastruktury cyfrowej utworzono w czerwcu 2018 r. i lipcu 2019 r.

4. Załączniki

4.1 Przegląd dostępnych danych w podziale na państwa członkowskie

Państwo członkowskie	Data przekazania informacji	Wykaz usług	Liczby OUK	Progi
AT	Po terminie	Dostarczono	BRAK DANYCH	Dostarczono
BE	Po terminie	Dostarczono	BRAK DANYCH	BRAK DANYCH
BG	Po terminie	Dostarczono	Dostarczono	Dostarczono
CY	W terminie	Dostarczono	Dostarczono	Dostarczono
CZ	Po terminie	Dostarczono	Dostarczono	Dostarczono
DE	W terminie	Dostarczono	Dostarczono	Dostarczono
DK	W terminie	Dostarczono	Dostarczono	Dostarczono
EE	W terminie	Dostarczono	Dostarczono	Dostarczono
EL	Po terminie	Dostarczono	Dostarczono	Dostarczono
ES	W terminie	Dostarczono	Dostarczono	Dostarczono
FI	W terminie	Dostarczono	Dostarczono	Dostarczono
FR	W terminie	Dostarczono	Dostarczono	Brak oficjalnych progów
HR	W terminie	Dostarczono	Dostarczono	Dostarczono
HU	W terminie	Dostarczono częściowo	Dostarczono częściowo	Dostarczono częściowo
IE	Po terminie	Dostarczono	Dostarczono	Dostarczono
IT	Po terminie	Dostarczono	Dostarczono	Dostarczono
LT	W terminie	Dostarczono	Dostarczono	Dostarczono
LU	Po terminie	Dostarczono	Dostarczono	Dostarczono
LV	Po terminie	Dostarczono	Dostarczono	Dostarczono
MT	Po terminie	Dostarczono	Dostarczono	Dostarczono
NL	Po terminie	Dostarczono	Dostarczono	Dostarczono
PL	W terminie	Dostarczono	Dostarczono	Dostarczono
PT	W terminie	Dostarczono	Dostarczono	Dostarczono
RO	Po terminie	Dostarczono	Dostarczono częściowo	BRAK DANYCH
SE	W terminie	Dostarczono	Dostarczono	Dostarczono
SI	Po terminie	Dostarczono	BRAK DANYCH	Dostarczono
SK	W terminie	Dostarczono	Dostarczono	Dostarczono
UK	W terminie	Dostarczono	Dostarczono	Dostarczono

4.2 Liczba usług i OUK zidentyfikowanych przez każde państwo członkowskie

Państwo członkowskie	Zidentyfikowane OUK	Usługi uwzględnione w załączniku II	Usługi dodatkowe
AT	0	46	0
BE	0	31	0
BG	185	30	3
CY	20	29	17
CZ	50	31	12
DE	573	15	12
DK	128	39	0
EE	137	18	6
EL	67	30	0
ES	132	55	18
FI	10 897[18]	20	0
FR	127	70	20
HR	85	49	2
HU	42	12	0
IE	64	26	0
IT	553	37	0
LT	22	37	0
LU	49	21	0
LV	66	18	0
MT	36	29	2
NL	42	12	0
PL	142	87	0
PT	1 250	26	0
RO	86	77	0
SE	326	27	0
SI	0	34	2
SK	273	28	7
UK	470	34	0

[18] Ze względu na metodę identyfikacji stosowaną przez Finlandię w sektorze opieki zdrowotnej zidentyfikowano bardzo dużą liczbę OUK.

4.3 Usługi zidentyfikowane przez państwa członkowskie w podsektorze energii elektrycznej

Państwo członkowskie	Zidentyfikowane usługi
AT	– Zakłady produkcji energii elektrycznej – Systemy kontroli w zakładach produkcji – Sieci dystrybucyjne – Sieci przesyłowe
BE	– Przedsiębiorstwa zajmujące produkcją, transportem i dystrybucją – Dystrybucja energii elektrycznej – Transport energii elektrycznej
BG	– Produkcja energii elektrycznej – Przesył energii elektrycznej – Eksploatacja, utrzymywanie oraz rozbudowa sieci przesyłowej energii elektrycznej – Dystrybucja energii elektrycznej – Zapewnienie funkcjonowania i utrzymania systemu dystrybucji energii elektrycznej – Rynek energii elektrycznej
CY	– Produkcja/dostawa – Dystrybucja/przesył – Usługi na rynku energii elektrycznej
CZ	– Produkcja energii elektrycznej – Sprzedaż energii elektrycznej – Eksploatacja sieci przesyłowej – Eksploatacja sieci dystrybucyjnej
DE	– Zasilanie
DK	– Przesył energii elektrycznej – Dystrybucja energii elektrycznej – Produkcja energii elektrycznej
EE	– Dostawy energii elektrycznej
EL	– Dostawy energii elektrycznej – Dystrybucja energii elektrycznej – Przesył energii elektrycznej
ES	– Wytwarzanie energii elektrycznej – Przesył energii elektrycznej – Dystrybucja energii elektrycznej – Ośrodki obsługi i kontroli systemów elektroenergetycznych
FI	– Usługa przesyłu – Dystrybucja energii elektrycznej w ramach sieci dystrybucyjnej – Dostawy energii elektrycznej za pośrednictwem sieci dystrybucyjnej wysokiego napięcia
FR	– Sprzedaż lub odsprzedaż energii elektrycznej klientom hurtowym i końcowym – Dystrybucja energii elektrycznej – Przesył energii elektrycznej
HR	– Produkcja energii elektrycznej – Przesył energii elektrycznej – Dystrybucja energii elektrycznej
HU	– Energia elektryczna
IE	– Operatorzy systemu dystrybucyjnego – Przedsiębiorstwa energetyczne

	– Operatorzy systemu przesyłowego
IT	– Wytwarzanie – Obrót – Przesył – Dystrybucja
LT	– Usługa produkcji energii elektrycznej – Usługa przesyłu energii elektrycznej – Usługa dystrybucji energii elektrycznej – Usługa dostarczania energii elektrycznej
LU	– Dostawy energii elektrycznej – Dystrybucja energii elektrycznej – Przesył energii elektrycznej
LV	– Wytwarzanie energii elektrycznej – Dystrybucja energii elektrycznej – Przesył energii elektrycznej
MT	– Dostarczanie energii elektrycznej do konsumentów – Przesył energii elektrycznej do konsumentów lub dystrybucja energii elektrycznej na potrzeby konsumentów – Wytwarzanie energii elektrycznej na potrzeby konsumentów
NL	– Przesył i dystrybucja energii elektrycznej
PL	– Wytwarzanie energii elektrycznej – Przesył energii elektrycznej – Dystrybucja energii elektrycznej – Handel energią elektryczną – Magazynowanie energii elektrycznej – Usługi zapewniania jakości i zarządzanie infrastrukturą energetyczną
PT	– Operatorzy systemu dystrybucyjnego – Operatorzy systemu przesyłowego
RO	– Produkcja energii elektrycznej – Dostarczanie energii elektrycznej do konsumentów – Funkcjonowanie scentralizowanych rynków energii elektrycznej – Transport energii elektrycznej – Funkcjonowanie systemu energetycznego – Dystrybucja energii elektrycznej
SE	– Operator systemu przesyłowego – Operator systemu dystrybucyjnego – Produkcja – Sprzedaż hurtowa
SI	– Produkcja energii elektrycznej w elektrowniach wodnych – Produkcja energii elektrycznej w elektrowniach cieplnych, elektrowniach jądrowych – Przesył energii elektrycznej – Dystrybucja energii elektrycznej – Handel energią elektryczną
SK	– Przedsiębiorstwo energetyczne – Operator systemu przesyłowego – Operator systemu dystrybucyjnego
UK	– Dostawy energii elektrycznej – Przesył energii elektrycznej – Dystrybucja energii elektrycznej

4.4 Usługi zidentyfikowane przez państwa członkowskie w podsektorze transportu kolejowego

Państwo członkowskie	Zidentyfikowane usługi
AT	– Infrastruktura kolejowa – Transport kolejowy towarów – Transport kolejowy pasażerów – Stacje kolejowe
BE	– Zarządcy infrastruktury – Przedsiębiorstwa kolejowe
BG	– Zapewnianie i utrzymanie obiektów infrastruktury usługowej oraz zarządzanie takimi obiektami – Transport kolejowy realizowany przez przewoźników kolejowych – Przedstawianie wytycznych dotyczących transportu kolejowego
CY	Brak zidentyfikowanych usług w tym podsektorze
CZ	– Funkcjonowanie kolei – Funkcjonowanie transportu kolejowego lub obiektu infrastruktury usługowej
DE	– Kolej
DK	– Zarządzanie infrastrukturą kolejową – Transport kolejowy
EE	– Zarządca infrastruktury kolejowej – Usługa transportu kolejowego
EL	– Zarządzanie infrastrukturą kolejową – Przewozy kolejowe
ES	– Zarządzanie usługami kolejowymi – Zarządzanie transportem kolejowym – Usługi sieci kolejowej – Zarządzanie informacją i telekomunikacją kolejową
FI	– Zarządzanie infrastrukturą państwową – Usługi zarządzania ruchem
FR	– Przewozy kolejowe – Kontrola ruchu kolejowego i zarządzanie ruchem kolejowym – Utrzymanie infrastruktury – Przewóz towarów i materiałów niebezpiecznych – Przewóz pasażerów – Utrzymanie taboru kolejowego – Metro, tramwaje i inne przewozy lekkimi pojazdami szynowymi (w tym koleje podziemne)
HR	– Zarządzanie infrastrukturą kolejową, m.in. zarządzanie ruchem i podsystem „Sterowanie”, oraz utrzymanie tej infrastruktury – Usługi transportu kolejowego towarów lub pasażerów – Zarządzanie obiektami infrastruktury usługowej i świadczenie usług w obiektach infrastruktury usługowej – Świadczenie dodatkowych usług niezbędnych do transportu kolejowego towarów lub pasażerów
HU	Brak zidentyfikowanych usług w tym podsektorze
IE	– Zarządcy infrastruktury – Przedsiębiorstwa kolejowe

IT	Brak zidentyfikowanych usług w tym podsektorze
LT	– Przewóz osób i bagażu koleją – Usługi kolejowych przewozów towarowych – Rozwój infrastruktury kolejowej, zarządzanie tą infrastrukturą i jej utrzymanie
LU	– Zarządzanie infrastrukturą kolejową – Transport kolejowy towarów i pasażerów
LV	ND.
MT	ND.
NL	Brak zidentyfikowanych usług w tym podsektorze
PL	– Przygotowywanie rozkładów jazdy pociągów – Transport kolejowy pasażerów – Transport kolejowy towarów
PT	– Zarządcy infrastruktury zgodnie z definicją w art. 3 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2012/34/UE. – Przedsiębiorstwa kolejowe zgodnie z definicją w art. 3 pkt 1 dyrektywy 2012/34/UE, w tym operatorzy obiektów infrastruktury usługowej zgodnie z definicją w art. 3 pkt 12 dyrektywy 2012/34/UE.
RO	– Kontrola ruchu i zarządzanie nim – Transport towarowy – Transport materiałów niebezpiecznych – Przewóz pasażerów – Metro, tramwaje i inne przewozy lekkimi pojazdami szynowymi – Utrzymanie infrastruktury kolejowej – Utrzymanie taboru
SE	– Zarządzanie infrastrukturą – Transport PAX – Transport ładunku
SI	– Transport kolejowy pasażerski, międzymiastowy – Transport kolejowy towarów – Uboczna działalność usługowa związana z transportem lądowym (funkcjonowanie stacji kolejowych itp.)
SK	– Operatorzy infrastruktury – Przedsiębiorstwa kolejowe
UK	– Przewozy kolejowe – Usługi kolei dużych prędkości – Metro, tramwaje i inne przewozy lekkimi pojazdami szynowymi (w tym koleje podziemne) – Międzynarodowe przewozy kolejowe