

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

- **KOMISJI CYFRYZACJI, INNOWACYJNOŚCI
I NOWOCZESNYCH TECHNOLOGII
(NR 134)
z dnia 15 września 2026 r.**

Pełny zapis przebiegu posiedzenia Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 134)

15 września 2026 r.

Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, obradująca pod przewodnictwem posła **Bartłomieja Pejo (Konfederacja)**, przewodniczącego Komisji, rozpatrzyła:

– informację na temat funkcjonowania systemów łączności służb.

W posiedzeniu udział wzięli: **Tomasz Szymański** sekretarz stanu w Ministerstwie Spraw Wewnętrznych i Administracyjnych wraz z współpracownikiem, **Łukasz Wojewoda** dyrektor Departamentu Bezpieczeństwa w Ministerstwie Cyfryzacji, **Krzysztof Dyl** zastępca prezesa Urzędu Komunikacji Elektronicznej wraz ze współpracownikiem, **Michał Kanownik** prezes Związku Cyfrowa Polska, **Wojciech Maciejczak** przewodniczący Grupy Bezpieczeństwa Operatorów Telekomunikacyjnych Polskiej Izby Informatyki i Telekomunikacji wraz ze współpracowniczką, **Piotr Mieczkowski** członek zarządu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji oraz **Joanna Karczewska** członkini Stowarzyszenia @ELKApw.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Leszek Jasiński**, **Magdalena Krzymowska** i **Adam Maćkiewicz** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dzień dobry. Otwieram posiedzenie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, stwierdzając jednocześnie kworum. Witam panie i panów posłów. Bardzo serdecznie witam pana ministra Tomasza Szymańskiego, sekretarza stanu w Ministerstwie Spraw Wewnętrznych i Administracji wraz z zespołem. Witam pana Łukasza Wojewodę, Dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji. Witam serdecznie zastępcę prezesa Urzędu Komunikacji Elektronicznej, pana Krzysztofa Dyla wraz ze współpracownikami. Witam serdecznie przedstawiciela ministra spraw zagranicznych pana Michała Gocha.

Przepraszam jednocześnie za opóźnienie, ale mieliśmy bardzo ważną komisję, gdzie wybieraliśmy panią przewodniczącą, więc stąd to opóźnienie z uwagi na dużą ilość pytań i dyskusję. Witam również reprezentację strony społecznej Związku Cyfrowa Polska, Polskiej Izby Informatyki i Telekomunikacji, Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, AUTO PAY SA oraz Stowarzyszenia @ELKApw. Witam serdecznie wszystkich państwa. Porządek dzisiejszego posiedzenia przewiduje zapoznanie się z informacją na temat funkcjonowania systemów łączności służb. Czy są uwagi do porządku obrad? Nie widzę.

Przechodzimy zatem do jego realizacji. Bardzo proszę o zabranie głosu pana ministra Tomasza Szymańskiego. Bardzo proszę, panie ministrze.

Sekretarz stanu w Ministerstwie Spraw Wewnętrznych i Administracji Tomasz Szymański:

Dziękuję bardzo. Panie przewodniczący, Wysoka Komisjo, bardzo dziękuję za wybranie tej tematyki i tego problemu na posiedzenie Komisji, ponieważ problematyka związana z łącznością państwową do tej pory była traktowana drugorzędnie, jak nie trzeciorzędnie, mając na uwadze nawet raport Najwyższej Izby Kontroli, który oceniał stan i proces wdrażania poszczególnych elementów łączności państwowej, szczególnie w okresie kontrolowanym, czyli między 2016 r. a 2023 r.

Mając na uwadze niezwykle ważny element, jaki spełnia łączność państwowa, będąca jednym z kluczowych filarów funkcjonowania państwa i zarządzania kryzysowego, gdzie właśnie w dzisiejszych czasach jest to teraz niezbędny element do tego, żeby służby w sposób skoordynowany mogły używać systemów, które faktycznie zadziałają w sytuacji kryzysowej, nie tylko związanej oczywiście z działaniami zbrojnymi. Mamy tutaj również głównie przykład dobrego funkcjonowania i koordynacji w przypadku wystąpienia zjawisk atmosferycznych, na przykład powodzi, która miała miejsce na Dolnym Śląsku.

Szanowni państwo, został państwu przedstawiony materiał, który, mam nadzieję, został przez państwa przeanalizowany. Tutaj są opisane wszystkie elementy składowe. Opieraliśmy się głównie na TETRZE, czyli na tym systemie trackingowym wraz z rozpisaniem zasad funkcjonalności. Krótko opiszę państwu ten system. Potem oddam głos panu dyrektorowi Departamentu Teleinformatyki w Ministerstwie Spraw Wewnętrznych i Administracji.

Tak jak powiedziałem, do tej pory mieliśmy taką sytuację, że to wszystko było niezorganizowane. Każda służba podlegała resortowi spraw wewnętrznych miała swój niezależny system, który nie był interoperacyjny z innymi. Mieliśmy systemy TETRA, na których operowała policja, mieliśmy *Digital Mobile Radio* (DMR-y), mieliśmy inne systemy, które były w kompetencji poszczególnych służb. Każdy rozbudowywał je na własną modłę. Nie było organu spinającego, nie było jednego organizatora, nie było jednego podmiotu spinającego. To się zmieniło i oczywiście na kanwie tych działań każdy po prostu realizował plany inwestycyjne, każdy miał specjalne komórki wykonawcze, każdy dublował niekiedy zakupy. Na końcu było tak, że nikt siebie nie słyszał, ponieważ każdy działał na oddzielnych systemach i nie widzieli oni siebie w sieci. Państwo nieraz mogliście widzieć, jak funkcjonariusze policji rozmawiali między sobą za pomocą prywatnych telefonów komórkowych. Nie mogli w sposób skuteczny, bezpieczny skontaktować się podczas jednej akcji ratowniczej na przykład w przypadku pożaru czy też zdarzenia drogowego.

To wszystko zmieniło się w momencie, kiedy została przyjęta ustawa o ochronie ludności i obronie cywilnej, która na powrót przywróciła w ogóle zarządzanie kryzysowe, przywróciła wykreśloną ustawę o obronie ojczyzny na powrót przywróciła ochronę ludności, ale również przywróciła system bezpiecznej łączności państwowej, która ustanowiła organizatora tej łączności w postaci ministra spraw wewnętrznych i administracji. Na podstawie tej ustawy powstał system i powstał zespół do spraw łączności państwowej, który wyodrębnił poszczególne podzespoły zajmujące się poszczególnymi elementami. Na tę chwilę, tak jak powiedziałem państwu na początku, system TETRA, którego organizatorem jest komendant główny policji, od teraz organizuje ten cały system łączności w Polsce. To on odpowiada za budowę infrastruktury. To on odpowiada na realizację zapotrzebowania poszczególnych służb podległych ministrowi spraw wewnętrznych i administracji, a także innych służb, które występują. Na kanwie, na przykład, wydarzeń pożarowych w województwie lubelskim widzimy, na przykład, że Lasy Państwowe są również tym podmiotem, który powinien być wyposażony w ten system, ze względu na zapewnienie dobrej komunikacji między poszczególnymi służbami.

Oprócz tego oczywiście są inne systemy i inne podzespoły łączności, mając na uwadze dostęp do sieci GOVNET. Mamy też coś, o czym należy mówić, co do tej pory było abstrakcyjne. Państwo przed chwileczką rozmawialiście o AI-u, możemy teraz mówić o łączności satelitarnej z prawdziwego zdarzenia. Powołutku będziemy się opierać na instrumentach europejskich, nie tylko na amerykańskim Starlinku. Jak państwo wiecie, została podpisana pomiędzy MSWiA a Komisją Europejską umowa w sprawie budowy IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite), czyli takiej kompilacji satelitarnej, której operatorem będą służby podległe ministrowi spraw wewnętrznych i administracji, dzięki czemu uzyskujemy niezawodną, zwielokrotnioną przepustowość w sytuacjach kryzysowych, na tyle dużą, że możemy dzielić się z innymi podmiotami na rynku krajowym, ale za pomocą *gateway*'a, który będzie umieszczony w Polsce, również możemy być operatorem satelitarnym dla państw nordyckich, dla państw Europy, krajów nadbałtyckich, ale również Holandii, o ile się nie mylę.

Tak że to są te rzeczy, które tak naprawdę od 2023 r. wdrożyliśmy w sposób błyskawiczny. Szanowni państwo, również to, co jest najważniejsze, zapewniliśmy finansowanie w tym obszarze. Do tej pory był to projekt doposażający służby mundurowe, ale tam oczywiście najważniejsze sprawy były w postaci wozów, radiowozów, komend, budowy, utrzymania obiektów technicznych. Łączność była traktowana pobocznie. Wraz z nowym programem ochrony ludności i obrony cywilnej, w obszarze piątym, zarezerwowanym wyłącznie na kwestie łączności państwowej, są przeznaczone na to pieniądze. Z tych pieniędzy, oprócz oczywiście kwestii łączności, będzie obsługiwany również... Pracujemy tutaj wspólnie z operatorami sieci telefonii komórkowej, nad systemem Cell Broadcast, o którym państwo również słyszeliście, żeby wdrożyć rozwiązania techniczne, które również będą jakimś komponentem, tutaj może bardziej w systemie ostrzegania i alarmowania. Tutaj mieliśmy bardzo dużo do zrobienia. De facto nic nie funkcjonowało.

To może tyle na początek. Panie dyrektorze, oddałbym głos celem uzupełnienia mojej wypowiedzi. Dziękuję.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję, panie ministrze.

Proszę, panie dyrektorze.

Dyrektor Departamentu Teleinformatyki w Ministerstwie Spraw Wewnętrznych i Administracji Dariusz Nowak-Nova:

Panie przewodniczący, państwo posłowie, pan minister praktycznie wyczerpał treść sprawozdania, które państwu składa Ministerstwo Spraw Wewnętrznych i Administracji. Szczegóły są w sprawozdaniu. Pan minister bardzo dobrze scharakteryzował, podsumował całe wystąpienie, więc nie pozostaje mi nic do dodania. Dziękuję.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję bardzo.

Bardzo proszę teraz o zabranie głosu pana dyrektora Łukasza Wojewodę.

Dyrektor Departamentu Bezpieczeństwa w Ministerstwie Cyfryzacji Łukasz Wojewoda:

Panie przewodniczący, szanowna Komisjo, w ramach uzupełnienia tak naprawdę tego, co zostało powiedziane przez pana ministra i pana dyrektora z MSWiA, w ramach systemu bezpiecznej łączności państwowej, Ministerstwo Cyfryzacji przygotowało jeden z podsystemów tego systemu. Świetnie się składa, że akurat to posiedzenie Komisji jest dzisiaj, ponieważ udało nam się dość niedawno zawrzeć również stosowne porozumienie i już oficjalnie system System Komunikacji Rządowej – Zastrzeżonej (SKR-Z), który jest budowany przez Ministerstwo Cyfryzacji, stał się jednym z elementów Systemu Bezpečnej Łączności Państwowej.

Natomiast czym jest system SKR-Z? System SKR-Z będzie tym podsystemem, który zapewnia łączność mobilną w tym niejawną. Mieliśmy do tej pory takie wyzwanie, to wyzwanie zaczęło narastać w chwili inwazji Federacji Rosyjskiej na Ukrainę: Jak w sposób bezpieczny, szybki i sprawny wymieniać się informacją niejawną? Bardzo często wystarcza informacja o klauzuli zastrzeżonej, nie jest potrzebna informacja wyżej klauzulowana. Jak bezpiecznie, skutecznie wymieniać się tą informacją, ale nie tylko przez wybrane podmioty administracji publicznej, ale szerzej, pomiędzy służbami i nie tylko tymi, które są w portfolio ministra spraw wewnętrznych, ale również służbami będącymi w zasobach ministra obrony narodowej? Wiedzieliśmy, że takim systemem mobilnym dysponuje Agencja Bezpieczeństwa Wewnętrznego i rozpoczęliśmy projekt, który na podstawie tego systemu mogłby zbudować coś szerszego dla całej administracji publicznej. Tak powstał system SKR-Z, czyli system komunikacji rządowej klauzuli zastrzeżonej oparty o sieć komórkową, w którym można wykorzystać do komunikacji dwa rodzaje urządzeń: urządzenie mobilne w postaci smartfona oraz komputer. Jest to system w pełni mobilny, z aktualnie obowiązującą dokumentacją, również możliwy do użytkowania w postaci telefonu i komputera poza strefami bezpieczeństwa, tak aby tworzyć z niego jak najbardziej elastyczny element do komunikowania się. System umożliwia nie tylko połączenia głosowe i nie tylko połączenia wideo, stosownie zbudowanego na potrzeby tego systemu komunikatora, ale również wymianę wiadomości e-mail, nie tylko w ramach systemu SKR-Z, ale również w ramach połączenia międzysystemowego z wojskowym systemem MIL-NAD-Z, jak również z systemem CATEL Agencji Bezpieczeństwa Wewnętrznego. Tym samym zbudowaliśmy funkcjonujący, interoperacyjny system, w którym nie tylko wojsko, nie tylko służba specjalna odpowiedzialna za bezpieczeństwo wewnętrzne, ale również reszta administracji publicznej w sposób bezpieczny, sprawny i szybki może przekazywać między sobą informację klauzulowaną.

Wiemy, że informacja klauzulowana w niektórych przypadkach nie jest niezbędna, aby informacji tej nadawać klauzulę, dlatego też Ministerstwo Cyfryzacji w ramach przedsięwzięcia, które realizuje pod nazwą SKR-Z, przygotowało również przedsięwzięcie pod nazwą komunikator do wykorzystania w środowisku jawnym, ale zabezpieczonym, odpowiednio przygotowanym, w odpowiedniej infrastrukturze. Tak powstał projekt czy aplikacja mSzyfr, którą w tej chwili rozwijamy w Ministerstwie Cyfryzacji z aspiracją na to, że będzie to administracja, która może skutecznie wyrugować wykorzystywanie komercyjnych rozwiązań do celów służbowych. Czyli to jest to, o czym wspominał pan minister, wykorzystywanie prywatnych telefonów do celów służbowych, które będzie obowiązywało nie tylko w tym wymiarze takiego formalnego zakazu, ale to będzie nasza potrzeba użytkowa. Czyli funkcjonariusz, urzędnik państwowy nie będzie nawet miał potrzeby korzystania z urządzenia prywatnego, ponieważ wszystkie funkcjonalności, takie jakie są dostarczane w środowisku biznesowym, będzie można znaleźć również

w rozwiązaniu, jakie dostarczamy w ramach połączonego systemu SKR-Z wraz z komponentem komunikatora mSzyfr.

Mało tego, jako podmiot odpowiedzialny za skonstruowanie, przygotowanie, utrzymywanie, rozwój systemu SKR-Z, słuchamy również potrzeb, jakie są po stronie innych interesariuszy. Tym sposobem również pomagamy w spełnieniu wymagań na przykład w zakresie zorganizowania Centralnej Ewidencji Obiektów Zbiorowej Ochrony. Na tej podstawie podpisaliśmy odpowiednie porozumienie z komendantem Państwowej Straży Pożarnej, tak aby również nie dublować różnych rodzajów systemów, tylko tak jak pan minister Szymański dobrze wspomniał: zrobimy coś wspólnego, skonsolidowanego, tak aby, po pierwsze, optymalnie wykorzystywać zasoby, jakie są w administracji publicznej, ale również nie pozostawiać po stronie użytkownika systemu – przepraszam za kolokwializm – tego kombinowania, co ja mam zrobić, żeby skutecznie i bezpiecznie wymienić się informacją.

Powiedziałem, że system SKR-Z i mSzyfr są oczywiście oparte o komunikację w sieciach mobilnych, komunikację na naszej komórce, z użyciem odpowiedniej karty SIM w laptopie, ale tu się nie zamknęliśmy. Też wychodząc naprzeciw potrzebom, że czasem nie będzie dostępu do sieci komórkowej, przygotowaliśmy, przetestowaliśmy takie rozwiązanie i taką konfigurację terminali systemu SKR-Z, że można to zrobić na przykład z wykorzystaniem systemu GovNet. Mało tego, rozwijamy się, aby ta komunikacja była możliwa również z wykorzystaniem przygotowywanych systemów komunikacji satelitarnej. Na pierwszy test oczywiście poszła dostępna w Ministerstwie Cyfryzacji komunikacja wykorzystująca terminale Starlink. Rozumiemy i widzimy tę potrzebę, że musimy być tak elastyczni, jak biznes tego potrzebuje, a biznesem dla nas są użytkownicy ekosystemu.

Żeby nie opierać się tylko na tym, że mamy tam głos i wideo do wymieniania się informacją, że mamy tam maila, wiemy, że skuteczna wymiana informacji niejawniej również wymaga dobrego systemu do zarządzania tą dokumentacją, więc w ramach kolejnej inicjatywy w projekcie SKR-Z rozpoczęliśmy przygotowanie odpowiednio skonstruowanego elektronicznego zarządzania dokumentami właśnie dla systemu niejawnego, który będzie odpowiadał potrzebom wynikającym z ustawy o ochronie informacji niejawnych.

Wszystkie te elementy systemu są posadowione w znanej nam infrastrukturze i bazują na takich rozwiązaniach, w których zapewniamy swoich specjalistów. Mało tego, idąc z duchem właśnie zapewniania pewnego rodzaju suwerenności technologicznej w rozwiązaniach mSzyfr, poszliśmy w stronę wykorzystania chociażby oprogramowania, które jest oprogramowaniem otwartokodowym, tak aby znów nie zamykać się technologicznie na konkretne rozwiązanie. W tym zakresie mieliśmy swoje doświadczenia, ponieważ zanim zaczęliśmy wykorzystywać oprogramowanie, system mSzyfr, korzystaliśmy z komercyjnego rozwiązania Threema On-Prem, które też było bezpiecznym narzędziem do wymiany informacji szyfrowanej w środowisku jawnym, wynikającym z potrzeby zapewnienia odpowiedniego, szybkiego i sprawnego komunikowania się wszystkich interesariuszy krajowego systemu cyberbezpieczeństwa po inwazji Federacji Rosyjskiej na Ukrainę.

Podsumowując, w tej chwili system SKR-Z i mSzyfr to są systemy działające operacyjnie. Liczba użytkowników stale się zwiększa, a dostarczane tam usługi również są umieszczone w takim cyklu rozwojowym. Nasze porozumienie, czyli pomiędzy ministrem cyfryzacji a ministrem spraw wewnętrznych i administracji też umożliwia nam lepsze słuchanie tego, co jest potrzebne w ramach ogólnie pojętej ochrony ludności i tego, co wynika z potrzeb samego Systemu Bezpiecznej Łączności Państwowej. Jeśli są dodatkowe pytania, chętnie na nie odpowiem. Dziękuję.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo serdecznie dziękuję.

Otwieram dyskusję. Czy ktoś z państwa posłów chciałby zabrać głos? Widzę. Ze swojej strony, bardzo dziękuję za tę informację. To oczywiście pozytywne, że państwo współdziałacie, że w porozumieniu ze sobą w tych kwestiach najważniejszych dla naszego państwa, a więc bezpieczeństwa przesyłania informacji, bezpieczeństwa komunikacji, działacie państwo w tym kierunku. Czy jest jeszcze pytanie, czy ktoś z państwa ze strony społecznej chciałby zabrać głos? Bardzo proszę.

Członek zarządu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji Piotr Mieczkowski:

Dzień dobry. Piotr Mieczkowski, Krajowa Izba Gospodarki Elektronicznej i Telekomunikacji. Chciałbym podnieść wątek budowy i stanu sieci dla służb we współpracy z sektorem prywatnym, dlatego że tak jak tutaj pan dyrektor, pan minister słusznie wskazał, Polska jest jedynym krajem, który nie ma kompleksowego systemu łączności dla służb z pokryciem całego kraju, tak dla jasności. Historycznie takie systemy były budowane jako wyspy, w szczególności największe kompetencje i największe wdrożenie sieci 2G, to jest tak naprawdę technologia sprzed 30 lat, czyli TETRA. Ma ją Policja, głównie w miastach wojewódzkich. Jeszcze za byłego premiera Leszka Millera były podejścia, żeby to rozbudować, ale one ugrzęzły. Dzisiaj mamy wojnę na granicy i jesteśmy jedynym krajem, który nie ma spójnego systemu dla wszystkich służb z pokryciem całego kraju. Jeśli dobrze pamiętam, to pokrycie siecią TETRA, czy tą siecią, którą operują służby – chodzi mi tu głównie o Policję i inne – to jest około 50–60 paru procent.

Pisałem na ten temat swego czasu, kilka lat temu książkę, robiąc przegląd właściwie większości krajów, które dokonały wdrożeń takich sieci. W większości tych krajów podstawą do budowy takiej komunikacji dla służb mundurowych jest współpraca z sektorem prywatnym. Ona jest w różnym modelu, ale jest głównie z sektorem prywatnym, gdzie sektor prywatny oferuje swoje częstotliwości lub nawet przede wszystkim sieci komercyjne i stacje bazowe w terenie, a państwo buduje rdzeń sieci, czyli tutaj MSWiA czy operator państwowy, taki jak EXATEL, mógłby zrealizować taką rzecz. Teraz w Stanach Zjednoczonych, w Wielkiej Brytanii i w wielu innych krajach operator komercyjny był właśnie wybierany w przetargu. W Wielkiej Brytanii to jest EE, dawny British Telecom, w Stanach Zjednoczonych jest sieć FirstNet, to jest operator AT&T. Tak jak powiedziałem, w większości krajów europejskich dzieje się podobnie, a największe kraje, które wdrożyły TETRĘ, czyli tę technologię, którą my się posługujemy, takie jak Niemcy – Niemcy mają chyba największe wdrożenie TETRY w Europie – migrują również, większość migruje do sieci 4G, a w tej chwili 5G. Teraz w Polsce mamy taką sytuację, że mamy kilka sektorów budujących osobno łączność dla państwa. Mamy sektor energetyczny. Mamy cztery spółki energetyczne, z czego PGE otrzymała kilka lat temu częstotliwości i buduje własną sieć LTE-M na 450 MHz. Buduje to samemu tylko i wyłącznie na własnym terenie. Poszczególne spółki energetyczne budują TETRĘ lub coś innego. Mamy kolejnictwo, które od 10 czy 15 lat nieskutecznie buduje łączność *Global System for Mobile Communications – Railway (GSM-R)*, czyli to jest odnoga 2G dla kolei, jako *railway* i mamy właśnie państwo, które też nieskutecznie, jako jedyne w Europie, nie buduje łączności dla służb. To, co robiły inne kraje, to na przykład w ramach przetargu albo konkursu na częstotliwości, najczęściej wskazywało jedno pasmo właśnie dla takiej łączności krytycznej, przykładowo blok sparowany 10 MHz i taki blok był oferowany czasami bezpłatnie, po to, żeby ten operator krajowy, kto wygra, musiał rozgłaszać tę sieć państwową w imieniu tak naprawdę dla państwa.

Czyli moje pytanie brzmi... Po tym wstępie, żeby wyjaśnić, jak to wygląda na świecie, czyli czy to mowa o Stanach Zjednoczonych, Wielkiej Brytanii, Finlandii, Szwecji i tak jak powiedziałem większość krajów europejskich, korzysta, czy to na bazie przetargu, czy na bazie wybrania pasma 700–800 MHz w konkursie i współpracuje z sektorem prywatnym. Moje pytanie brzmi: Czy nasze państwo przewiduje współpracę z sektorem prywatnym w zakresie chociażby łączności 5G i zbudowania takiej synergii, że sektor prywatny oferuje stacje bazowe i zasięg w całym kraju, szczególnie że w ostatnich aukcjach został zobligowany do zapewnienia zasięgu na powierzchni całego kraju z dużą przepływnością, a państwo korzysta z rdzenia, oferuje rdzeń sieci i zarządza użytkownikami? To jest pytanie pierwsze o tę współpracę Partnerstwo Publiczno-Prywatne (PPP), czy nasze państwo przewiduje tutaj jakąś współpracę.

Mam drugie pytanie o ten *self-broadcast*, który padł w przemówieniu. Jaki jest pomysł na sfinansowanie tego? Czy na przykład jakaś ulga dla operatorów za to, że będą oferować taką funkcjonalność, czyli na przykład pomniejszona opłata za numerację lub coś innego? To znaczy, to są moje dwa pytania. Jedno dotyczy PPP, a drugie sfinansowania *self-broadcast*. Dziękuję bardzo.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję.

Bardzo proszę, panie ministrze.

Sekretarz stanu w MSWiA Tomasz Szymański:

Dziękuję bardzo. Szanowni państwo, zacznę od drugiego pytania, bo wydaje się prostsze. Mając na uwadze nasz powołany zespół, tak go nazwę, roboczy, problemowy, poświęcony właśnie tematyce, między innymi *self-broadcast*'u. Ona tu jest wiodąca, również rozszerzamy ją o usługę Rządowego Centrum Bezpieczeństwa, będąc jakby w interoperacyjności systemu alarmowania i ostrzegania, na tę chwilę jesteśmy właśnie w dialogu. Kolejne spotkanie w przyszłym tygodniu, które mamy z operatorami, na pewno przybliży nas o kolejny krok w kontekście finansowania niezbędnych nakładów, zarówno po stronie operatorów, jak i strony rządowej, ponieważ doskonale wiemy, że to wymaga spójnej... To znaczy, najpierw spójnego zdiagnozowania potrzeb, operacyjnego, technologicznego podejścia. Na to trzeba nałożyć kalendarium. To znaczy, mam nadzieję, że to chyba będzie jedno z najszybszych wdrożeń *self-broadcast*'u przynajmniej, jeżeli chodzi o Europę. Tak, na to liczymy. Tak że tutaj jesteśmy dopiero w dialogu i jakby opracowujemy ten model finansowania.

Zanim oddam głos panu dyrektorowi, bo już sobie zrobił notatki, żeby również udzielić odpowiedzi. To znaczy, może nas cieszyć to, że w momencie, kiedy obejmowaliśmy władzę w 2023 r., jak pan doskonale wie, pokrycie TETRA przekraczało ledwo ponad 20%. Na koniec 2025 r. wynosiło 57%, a teraz już wynosi blisko ponad 70%. Tak że idziemy w dobrym kierunku, mając na uwadze te wieloletnie zapóźnienia i jakby doposażanie i zinwentaryzowanie stanu zastalego. Zespół, który powołaliśmy, którego jestem szefem, dokładnie bada te wszystkie nurty: między innymi infrastrukturę, zdiagnozowanie, paszportyzację oraz inwentaryzację poszczególnych systemów, kto co ma, jakie zasoby, czym się zajmuje. Zaczęliśmy to robić, zlecieliśmy to zadanie. Pan dyrektor może powie o szczegółach.

Dyrektor departamentu w MSWiA Dariusz Nowak-Nova:

Tak. Tak jak pan minister powiedział, sytuacja, o której pan opowiedział, którą opisał, rzeczywistość była w kraju. Pan minister również wspominał o raporcie NIK, który dosyć krytycznie, mówiąc kolokwialnie, czy tak chyba bardzo lekko, opisał stan łączności służb. Dużo jednak się zmieniło od tego czasu. W ciągu ostatnich dwóch lat, jeśli mówimy o łączności dla służb, rzeczywistość postawił na łączność tetrową. To nie jest tak, że to jest technologia, z której kraje europejskie się wycofują. Jest wręcz odwrotnie. Szacuje się, że w skali Europy ta technologia będzie dalej rozwijana przez około 15 lat. Ona oczywiście przejdzie w następny rodzaj, w następną wersję technologii tetrowej, TETRA+, będzie to korelowane z łącznością satelitarną. Jako MSWiA uczestniczymy w budowie takiego dużego europejskiego systemu łączności kryzysowej, więc na bieżąco wiemy, jak wyglądają te trendy i też to, co robimy w kraju, odzwierciedla dokładnie trendy europejskie czy trendy światowe.

Dużo się mówi o tym, że łączność służb... Zresztą sam pan powiedział, że istnieje kilka dużych systemów, które są budowane i które mają zajmować się łącznością. Natomiast chciałem zwrócić uwagę, że to jest łączność innego rodzaju. Trudno porównywać nawet łączność radiową budowaną przez PGE z wykorzystaniem innych częstotliwości. Tam te kanały głównie będą służyły do zarządzania maszynami. Tam jest ruch maszyna-maszyna. To samo dotyczy łączności, którą budują Polskie Koleje Państwowe. Te pasma 420 MHz też służą do czegoś innego.

Czy warto budować łączność w kooperacji publiczno-prywatnej? Sytuacja podczas wojny w Ukrainie pokazała, że państwo nie może tracić kontroli nad łącznością. Państwo nie może sobie pozwolić na to, że prywatny właściciel któregoś dnia powie, że nie będzie dostarczał łączności, bo coś tam. Stąd zapadła decyzja, że łączność, która jest budowana dla służb, ta łączność kryzysowa, będzie w 100% oparta na infrastrukturze kontrolowanej przez państwo.

W pierwszym kroku zaczęliśmy budować tę łączność, rozwijając policyjny system tetrowy. Pan minister powiedział, jakiego rodzaju zasięgi już dzisiaj mamy. Mamy też takie projekcje, które mówią, że w 2027 r. to będzie 90% kraju ze stacjonarnymi *Base Transceiver Station* (BTS-ami). Nie mówimy tutaj o takich mobilnych BTS-ach, które się poruszają i które mogą dojechać w każde miejsce.

Sekretarz stanu w MSWiA Tomasz Szymański:

Też mamy, można powiedzieć, bardzo duże zaawansowanie, zakupione mobilne węzły, które są jakby kolportowane do komend powiatowych, zarówno straży, jak i Policji.

Dyrektor departamentu w MSWiA Dariusz Nowak-Nova:

To jest taki dodatkowy element rozszerzający łączność tetrową, natomiast łączność dla służb resortu to jest jedna łączność dla wszystkich służb. Obejmujemy tym także Wojewódzkie Centra Zarządzania Kryzysowego. Będziemy schodzili do powiatów. To nie jest tak, że państwo nie buduje łączności, że nie ma łączności i że musi ją budować z wykorzystaniem podmiotów prywatnych. Łączność, o której mówił pan dyrektor Łukasz, ta łączność mobilna, to jest ten obszar, który mógłby być potraktowany jako *Public Protection and Disaster Relief (PPDR)*, bo to do tego się sprowadza, ale łączność Systemu Komunikacji Rządowej – Zastrzeżone (SKR-Z-owa) jest jednym z podsystemów Systemu Bezpiecznej Łączności Państwowej (SBŁP). Tak naprawdę budując łączność, podchodzimy do tego wielosystemowo. Mamy kilka kanałów komunikacyjnych, które rozwijamy równolegle. Wydaje się, że na razie idzie nam to w miarę... Nie chcę się chwalić, ale możemy w pełni świadomie powiedzieć, że służby resortu MSWiA są w pełni skomunikowane. Też robimy dalsze kroki, które umożliwią nam bardzo aktywne korzystanie z łączności satelitarnej, ze schodzeniem do jak najniższego poziomu, do poziomu powiatów, do poziomu gmin, nie tylko z głosem, ale także z obrazem, z dźwiękiem, z danymi.

Członek zarządu KIGeIT Piotr Mieczkowski:

Mam tylko jedno pytanie. Wspomniał pan o służbach w MSWiA, a ta łączność *PPDR*, ta łączność dla służb, ona dotyczy ratownictwa, Straży Pożarnej, Policji i tak dalej. Jest pytanie. Ten system, te 90%, czy tam te 70% pokrycia, to dobrze się posuwa, ale pytanie brzmi: Czy ono pokrywa wszystkie te służby między sobą? One też są wyposażone jakby w urządzenia mobilne, żeby móc się skomunikować, załóżmy, jak jest powódź, prawda, czy jest pożar, gdy jest jakieś zdarzenie.

Wiadomo, że historycznie był problem przy wielkiej powodzi we Wrocławiu, kiedy właśnie zjechały się służby ratownicze i każdy miał telefon z innej parafii, nikt nie mógł rozmawiać. Cieszy mnie to, że jest pewien postęp, ale pytanie brzmi, czy właśnie wszyscy otrzymają ten aparat do wykonywania takich połączeń.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Ja jeszcze uzupełnię to pytanie. Czy w tych 70% bierzecie państwo pod uwagę wszystkie służby? W jaki sposób mierzycie te 70%?

Dyrektor departamentu w MSWiA Dariusz Nowak-Nova:

To będzie wspólna odpowiedź na pytanie à propos służb, które uczestniczą w systemie. Tak, wszystkie służby, które są odpowiedzialne za zarządzanie kryzysowe, za bezpieczeństwo, za ratownictwo, łącznie z ratownictwem górskim i tak dalej – te wszystkie służby są objęte jednym systemem łączności radiowej Bezpieczna Radiowa Łączność Trankingowa (SBŁP-T), budowanym w oparciu o urządzenia, o technologię TETRA.

W tej chwili realizowaliśmy dwa takie duże nurty zakupowe. Z jednej strony budowaliśmy nowe stacje nadawcze, nowe BTS-y. W tej chwili trwają postępowania na zakup słuchawek, czyli radiotelefonów, urządzeń dla służb. Mamy odpowiedni algorytm rozdziału. Służby zgłaszały nam zapotrzebowania. Także wchodzimy z TETRĄ na poziom administracji publicznej, czyli do Centrum Zarządzania Kryzysowego. Mamy już podpisanych sporo licencji, bo TETRA może być rozdzielana tylko w wypadku, jeśli użytkownik otrzyma licencję. Dużo licencji daliśmy wojewodom. Wojewodowie przekazują te urządzenia powiatom, tak że – tak, wszystkie służby. I 70%...

Sekretarz stanu w MSWiA Tomasz Szymański:

Tak, to będzie to rozwinięcie samych stacji bazowych, stałych. Na koniec roku, to znaczy, do 2023 r., było ich kilkadziesiąt. W samym tylko 2025 r. przyrosło ponad 106 stacji stałych. Czyli można powiedzieć, że na początku roku było 220 stałych stacji bazowych. Jaki mamy przyrost w tym roku?

Dyrektor departamentu w MSWiA Dariusz Nowak-Nova:

145.

Sekretarz stanu w MSWiA Tomasz Szymański:

145 stacji bazowych. To tak celem uzupełnienia intensyfikacji prac w poszczególnych systemach. Dzięki.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję bardzo.

Czy są jeszcze jakieś pytania? Bardzo proszę.

Ekspert Polskiej Izby Informatyki i Telekomunikacji Katarzyna Cyrbus:

Dzień dobry, Katarzyna Cyrbus, Polska Izba Informatyki i Telekomunikacji, Cellnex Poland. Chciałabym troszeczkę dodać parę słów pytania do pytania kolegi z krajowej izby. Państwo mówią o systemie SBŁP-T. Sądzę, że należy w pierwszej kolejności pogratulować tej inicjatywy rozszerzania systemu TETRA na wszystkie służby jako pierwszego kroku. To, o co Piotr pytał, to o migrację do nowszych technologii, które będą umożliwiały, to o czym pan też wspominał, komunikowanie się maszyn czy na przykład przesył wideo między służbami. Z tego, co pan dyrektor Wojewoda mówił, rozumiem, że ten rozwój systemu SKRZ nie ma na celu wypełnienia tego podsystemu opisanego w ustawie o ochronie ludności, podsystemu bezpiecznej radiowej łączności mobilnej SBŁP-M. To jest potencjalnie ten obszar, którego rozwój zostanie jeszcze zaplanowany w kolejnych latach jego przez ministerstwo. Chciałabym to doprecyzować. Dziękuję.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Jeśli można, to proszę o odpowiedź.

Pan dyrektor.

Dyrektor departamentu w MC Łukasz Wojewoda:

Oczywiście. Jeśli chodzi o podsystem, jeden z podsystemów systemu SBŁP, na chwilę obecną system komunikacji mobilnej, w tym niejawnej, dostarczany jest właśnie poprzez system Systemem Komunikacji Rządowej – Zastrzeżone (SKR-Z). System SKR-Z opiera się o komunikację sieci GSM jednego z operatorów. To à propos współpracy administracji publicznej i biznesu. Tak, potrafimy współpracować i robimy to od wielu lat, nie tylko my jako Ministerstwo Cyfryzacji, ale są również inni, którzy korzystają z podobnych systemów, tak samo jak chociażby Agencja Bezpieczeństwa Wewnętrznego i system CATEL. Na obecną chwilę te potrzeby, jakie stoją za komunikacją mobilną z wykorzystaniem systemu SKR-Z, w naszej ocenie wyczerpują te potrzeby. Żebyśmy się rozumieli, jakby co my potrzebujemy...

Co my chcemy osiągnąć przez ten system? Chcemy osiągnąć właściwą dla danych czasów komunikację jawną i niejawną pomiędzy wieloma interesariuszami. To nie jest tak, że wystarczy nam tylko krótka wiadomość tekstowa. W tej chwili, biorąc dla przykładu wydarzenia z Odry z kilku lat wstecz, chociażby dobrej jakości zdjęcia, które by pokazywały skalę problemu, też zanim zostaną przekazane w sposób niewłaściwy, też powinny być odpowiednio chronione. Po to powstają systemy. Zgodnie z klasyfikacją informacji, jaka została zawarta w ustawie o ochronie informacji niejawnych, administracja publiczna jest też zobowiązana do tego, żeby nadawać taką klasyfikację tej informacji. Taki system chcemy dostarczyć. Z jednej strony wygodny, mobilny, elastyczny, z drugiej strony spełniający wymagania ustawy o ochronie informacji niejawnych. Te wymagania dotyczą systemów teleinformatycznych. Przypomnę, zgodnie z ustawą akredytujemy systemy teleinformatyczne, więc te wszystkie wymagania zostały złożone w jedną całość i stąd mamy system SKR-Z.

Natomiast widząc, że w tym podsystemie łączności mobilnej, jest dopisek „w tym niejawnej”, widzimy też potrzeby bezpiecznej łączności, ale dla których być może nie ma potrzeby nadawania klauzuli. Tu powstał komunikator mSzyfr, który jest bardzo szeroko dostępny. Jest dostępny w sklepie Play. Jest dostępny na rozwiązania firmy Apple. Jest dostępny również przez interfejsy webowe. Tak jak użytkownicy zgłaszali potrzebę, tak staramy się dostosować, nie schodząc z poziomu bezpieczeństwa, bo to jest istotne. Ten system jawny jest też systemem szyfrowanym, klasy *end-to-end encryption*, z wykorzystaniem aktualnie dostępnych protokołów, które też są w tym otwarto kodowym trybie, dzięki czemu my, dopisując się do społeczności, która pracuje nad tym systemem, nad tymi rozwiązaniami, mamy też możliwość weryfikacji, co w naszym systemie później implementujemy fizycznie. Też, żeby nie było, że nie ma przykładów, jak historia pokazuje, jeden niezbyt przyjazny nam deweloper, który zapisał się do repozytorium i wspólnie pracuje nad kodem, dołożył coś, co później się pojawia w repozytorium. Po to budujemy zdolności również sprawdzania takiego rozwiązania, żebyśmy mieli tę świadomość, zanim trafi na tak zwaną produkcję, co później znalazło się w tym naszym rozwiązaniu. To jest ta składowa pod nazwą „mobilna, w tym niejawna”, oparta o aktualnie funkcjonujących operatorów komórkowych. Jaka to jest firma po naszej stronie, to już zostawię do węższego grona. Natomiast jeśli chodzi o to, że współpracujemy z biznesem, tak, współpracujemy i potrafimy to robić. Mało tego, potrafimy to robić od już wielu, wielu lat.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję bardzo. Czy jeszcze ktoś z państwa chciałby zabrać głos?
Bardzo proszę, panie Piotrze.

Członek zarządu KIGEiT Piotr Mieczkowski:

Pytam o jedną rzecz związaną z tymi 70%, bardziej o perspektywę. To znaczy, jak to państwo planują. Czy w ogóle są plany zapewnienia 100% pokrycia? W szczególności myślę o tym programie „Tarcza Wschód” i po tej ścianie wschodniej. Jakie są perspektywy pokrycia całościowego i jaki pan dyrektor przewiduje, że będzie procent pokrycia tymi radiotelefonami w poszczególnych służbach? Czy na przykład będzie to cała policja, w sensie cała policja w Polsce, głównie drogówka i tak dalej, czy również służby ratownicze, strażacy, którzy dzisiaj często korzystają też z różnych telefonii, czy nawet prywatnych? Jak to będzie wyglądało w przyszłości? Jakie są perspektywy tak ogólnie, to będzie 2030 r., 2035 r.? I może ile będzie masztów, jaka jest też tego perspektywa? Tutaj też była o tym mowa.

Dyrektor departamentu w MSWiA Dariusz Nowak-Nova:

Na chwilę dzisiejszą mamy 367 masztów stacji bazowych. Mamy także zawartą umowę na 521 kolejnych masztów. To jest taka... Szacunki kilka lat temu mówiły o tym, że pokrycie w całym kraju powinno być zapewnione w liczbie między 1800 a 2200 masztów. Takie były szacunki. Tylko tu też... Być może to nie jest miejsce na taką dyskusję, ale bardzo interesującym rozwiązaniem, czy takim zagadnieniem, jest pokrycie w górach. Pytanie brzmi, jak często w górach powinien być maszt, żeby powinien być zasięg. Koledzy z Austrii mówią: „Ale po co wam maszty? Damy wam słuchawki, które są dwusystemowe. Jak nie ma TETRY, to jest LTE.” Tak że pójdziemy raczej w tę stronę. To jest odpowiedź à propos pokrycia.

Planujemy, że do końca przyszłego roku będziemy mieli pokryte pełnym zasięgiem 90% kraju. Oczywiście najtrudniejsza będzie ta końcówka, czyli tych 10%. To są często rejony gęsto zaludnione, w których budynki są taką naturalną przeszkodą, ale nie będziemy mieli problemu z ciągami komunikacyjnymi. Tam wszędzie będą mogły być węzły mobilne, stacje mobilne, także stacje uruchamiane bezpośrednio w radiowozach czy w wozach służb. Generalnie na przyszły rok będziemy mieli 90% i będziemy dogęszczać.

Jeśli chodzi o standard komunikacji między służbami, on został wskazany. Standardem komunikacji służb resortu MSWiA jest system TETRA, co oznacza, że docelowo wszyscy policjanci będą korzystali z radia tetrowego. Co oznacza, że Straż Graniczna w 100% przejdzie na system tetrowy. Tam były poczynione dosyć duże inwestycje w systemy DMR-owe. Te systemy DMR-owe będą traktowane jako systemy backupowe, więc Straż Graniczna przechodzi na system tetrowy. Służba Ochrony Państwa również jest włączona w system tetrowy. On jest na tyle mały, że odbędzie się to z zachowaniem własnych radiostacji, które potrzebują do innych zadań. Dużym wyzwaniem jest PSP, czyli straż pożarna. O ile jesteśmy w stanie zagwarantować, że Państwowa Straż Pożarna zostanie wyposażona w końcówki, w terminale tetrowe, to jest problem licencyjny z ochotniczymi strażami. Niestety system tetrowy rządzi się swoimi prawami związanymi z szyfrowaniem, licencjonowaniem i tak dalej, stąd nie ma takiego prostego mechanizmu przekazywania tych urządzeń tetrowych każdemu, kto o nie poprosi. Tu ustaliliśmy, że w zakresie ochotniczych straży pożarnych na pewno wszystkie komendy czy wszystkie oddziały, które wchodzi w skład Krajowego Systemu Ratowniczo-Gaśniczego, w KSRG będą wyposażone w te urządzenia. On się składa zarówno ze straży państwowych, jak i ochotniczych, natomiast pracuje w rygorach KSRG i w tym zakresie będziemy działali. Również system tetrowy będzie obejmował ratownictwo, w tym Lotnicze Pogotowie Ratunkowe, ratownictwo medyczne, również ratownictwo górskie i inne organizacje, które nie są organizacjami społecznymi, a realizują zadania związane z ochroną ludności i mogą się mieścić w katalogu podmiotów uprawnionych zgodnie z ustawą o obronie cywilnej i ochronie ludności. Dziękuję bardzo.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję. Rozumiem, że już nie ma głosów w dyskusji. Bardzo serdecznie dziękuję panom za wyjaśnienia, za przedstawienie tychże informacji. Na pewno będziemy wracać do sprawy, do tych tematów, bo one są niezwykle istotne. Raz jeszcze bardzo serdecznie wszystkim państwu dziękuję.

Zamykam dyskusję i zamykam posiedzenie Komisji. Dobrego popołudnia.