

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

**Komisja
Administracji
i Spraw
Wewnętrznych**

- **PODKOMISJI DO SPRAW MODERNIZACJI
I ROZWOJU POLICJI,
STRAŻY GRANICZNEJ,
PAŃSTWOWEJ STRAŻY POŻARNEJ
I SŁUŻBY OCHRONY PAŃSTWA
(NR 16)
z dnia 3 grudnia 2025 r.**

Pełny zapis przebiegu posiedzenia Komisji Administracji i Spraw Wewnętrznych – podkomisji stałej do spraw modernizacji i rozwoju Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa (nr 16)

3 grudnia 2025 r.

Podkomisja stała do spraw modernizacji i rozwoju Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa, obradująca pod przewodnictwem posła **Wojciecha Króla (KO)**, przewodniczącego podkomisji, rozpatrzyła:

– **informację ministra spraw wewnętrznych i administracji na temat oceny stanu obecnych systemów łączności w Polsce.**

W posiedzeniu udział wzięli: **Dariusz Nowak-Nova** dyrektor Departamentu Teleinformatyki w Ministerstwie Spraw Wewnętrznych i Administracji wraz ze współpracownikami, insp. **Przemysław Więclaw** dyrektor Biura Łączności i Informatyki w Komendzie Głównej Policji, płk SG **Mariusz Kijowski** dyrektor Biura Łączności i Informatyki w Komendzie Głównej Straży Granicznej, płk SOP **Michał Majek** zastępca dyrektora Zarządu Łączności i Informatyki w Służbie Ochrony Państwa, st. bryg. **Kazimierz Gogacz** naczelnik w Komendzie Głównej Państwowej Straży Pożarnej oraz **Marek Wójcik** pełnomocnik Zarządu Związku Miast Polskich.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Igor Amarowicz** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Wojciech Król (KO):

Dzień dobrym, otwieram posiedzenie podkomisji stałej do spraw modernizacji i rozwoju Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa.

Porządek dzienny obejmuje informację ministra spraw wewnętrznych i administracji na temat oceny stanu obecnych systemów łączności w Polsce. Bardzo ważny temat, związany ponieważ z nową ustawą modernizacyjną, ponieważ również środki finansowe na kolejne 4 lata z tych 13 mld przeznaczonych, dedykowanych modernizacji, przeznaczone są także na środki łączności, na inwestycje w cyberbezpieczeństwo, bezpieczeństwo informatyczne, teleinformatyczne.

Bardzo miło mi powitać naszych gości na posiedzeniu podkomisji. A jest z nami pan Dariusz Nowak-Nova, dyrektor Departamentu Teleinformatyki w Ministerstwie Spraw Wewnętrznych i Administracji. Witam serdecznie i przepraszam za pomyłkę w nazwisku. Jest z nami insp. Przemysław Więclaw, dyrektor Biura Łączności i Informatyki w Komendzie Głównej Policji. Dzień dobry, witam serdecznie. Jest z nami płk Mariusz Kijowski, dyrektor Biura Łączności i Informatyki w Komendzie Głównej Straży Granicznej. Dzień dobry, witam serdecznie. Jest z nami płk Michał Majek, zastępca dyrektora Zarządu Łączności i Informatyki w Służbie Ochrony Państwa. Dzień dobry panu. Jest z nami Kazimierz Gogacz, naczelnik z Państwowej Straży Pożarnej. Dzień dobry, witamy pana. I jest z nami pani Maria Skarzyńska, naczelnik wydziału z Krajowego Centrum Monitorowania Systemu Powiadamiania Ratunkowego w Departamencie Ochrony Ludności i Zarządzania Kryzysowego w Ministerstwie Spraw Wewnętrznych i Administracji.

Myślę, że tytułem wstępu, jeżeli państwo na to przystaną, pozwolę sobie oddać głos przedstawicielowi ministra, panu dyrektorowi, który wprowadziłby nas w tę informację ministra, ponieważ porządek dzienny obejmuje informacje ministra dotyczące obecnych systemów łączności oraz planowanych inwestycji. Następnie poproszę, jeżeli oczywiście pan dyrektor zgadza się z moim planem posiedzenia naszej podkomisji, żeby przedstawiciel każdej służby opowiedział o swoich systemach, używanych w służbie, którą reprezentuje, a także o planowanych inwestycjach,

z nastawieniem również na te inwestycje, które są przewidziane w programie modernizacji. Bardzo proszę, oddaję głos panu dyrektorowi.

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

Dziękuję, panie przewodniczący. Szanowni państwo, minister przedłożył państwu informację na temat oceny stanu obecnych systemów łączności w Polsce. Ta informacja jest stosunkowo rozbudowana. Ja pozwolę sobie krótko przedstawić clou informacji, które są tam zawarte, a potem przejdziemy do zagadnień, o których pan przewodniczący powiedział.

Przedmiotem informacji są rozwiązania obejmujące łączność resortu spraw wewnętrznych i administracji oraz systemy mające znaczenie dla funkcjonowania państwa w zakresie bezpieczeństwa, ochrony ludności i obrony cywilnej. W informacji uwzględniono również działania podejmowane w związku z ustanowieniem przepisami ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej systemu bezpiecznej łączności państwowej, zakładanymi kierunkami rozbudowy tego systemu oraz integracji i wykorzystania na poziomie krajowym. Zapewnienie sprawnego, bezpiecznego oraz odpornego na zakłócenie obiegu informacji pomiędzy organami administracji publicznej, służbami odpowiedzialnymi za bezpieczeństwo państwa, podmiotami ratowniczymi oraz strukturami reagowania kryzysowego jest warunkiem prawidłowego wykonywania zadań państwa zarówno w czasie pokoju, jak i w sytuacjach nadzwyczajnych. Tak spoglądamy na te systemy. Systemy łączności stanowią jeden z kluczowych filarów funkcjonowania państwa, szczególnie w obszarze bezpieczeństwa wewnętrznego, ochrony ludności oraz obrony cywilnej. Znaczenie tych systemów w ostatnich latach uległo znacznemu wzmocnieniu, co jest ściśle związane z rosnącym poziomem zagrożeń o charakterze hybrydowym, cybernetycznym, informatycznym oraz militarnym. W tym kontekście systemy łączności muszą gwarantować nieprzerwaną zdolność wymiany informacji przy jednoczesnym zapewnieniu poufności, integralności oraz dostępności przesyłanych danych. Szczególnego znaczenia nabrała kwestia interoperacyjności. Interoperacyjność to zdolność różnych systemów, służb i podmiotów do współdziałania, co jest najistotniejsze, poprzez wykorzystywanie kompatybilnych rozwiązań komunikacyjnych. Informacja zawiera opis systemów, kategoryzując je na cztery główne grupy. Wyróżniamy tam systemy łączności stacjonarnej i tutaj pozwolę sobie państwu trochę więcej powiedzieć, jak w kontekście informacji interpretujemy te cztery rodzaje łączności.

Otóż łączność stacjonarna to są głównie systemy łączności wykorzystujące infrastrukturę przewodową i światłowody. Druga grupa to jest łączność radiowa i tutaj mówimy o łączności specjalistycznej, wykorzystywanej przez służby, niezależnej od systemów publicznych. Mówimy tam o łączności mobilnej i to są systemy, które wykorzystują publiczne czy powszechnie funkcjonujące sieci komórkowe. Mówimy także o łączności satelitarnej i w kontekście sprawozdania na dzień dzisiejszy opisujemy usługi świadczone przez komercyjne podmioty oferujące taką łączność. Oczywiście jest to duże uproszczenie, natomiast w takim kontekście dużo łatwiej opowiadać o samej łączności. Sprawozdanie przedstawia szczegółowy opis w poszczególnych typach łączności. Dużo uwagi poświęcone jest podstawowej sieci stacjonarnej, która jest zarządzana przez ministra spraw wewnętrznych, czyli sieci GovNet. Jest to sieć, która łączy instytucje centralne, urzędy wojewódzkie, ministerstwa, schodzi aż do powiatów i na tej sieci jako sieci podkładowej realizowane są usługi, w tym także usługi łączności, także łączności specjalnej. To nie dotyczy tylko obiegu informacji wewnątrz naszego kraju, ale również dzięki tej sieci jesteśmy połączeni z systemami Unii Europejskiej i są przesyłane także usługi istotne dla bezpieczeństwa państwa pomiędzy krajami unijnymi. Na tej sieci również działa taka specjalistyczna łączność, system łączności rządowej, łącząca najważniejsze organy państwowe. To jest sieć, która nie jest siecią jawną, nie jest siecią publiczną, służy do komunikowania się. Oczywiście policja wykorzystuje bardzo rozbudowaną sieć OST 112. To jest sieć, która powstała w celu obsługi numeru alarmowego 112 – oczywiście to jest podstawowy jej cel. Natomiast od strony praktycznej policja wykorzystuje również tę łączność do realizacji swoich zadań i usług, które bezpośrednio funkcjonują w policji.

Drugą dużą grupą jest łączność radiowa. Koncentrując się na opisie łączności radiowej duży nacisk kładziemy na łączność trunkingową. Myślę, że państwo macie w pamięci raport Najwyższej Izby Kontroli z 2024 r., który dosyć krytycznie opisywał systemy łączności służb podległych ministrowi spraw wewnętrznych i administracji. Wskazano tam na wieloletnie zaniedbania, jeśli chodzi o stworzenie jednego, jednorodnego systemu łączności. Wskazywano na to, że rozwój

systemów w poszczególnych służbach odbywał się poza kontrolą ministra. Wskazywano na to, że systemy były rozwijane w odseparowaniu od innych systemów, że nie zastanawiano się nad wymianą informacji, nad interoperacyjnością właśnie. Ten raport stanowił taki... nie powiem, że kamień milowy, ale pewnego rodzaju game changer, ponieważ minister spraw wewnętrznych i administracji postanowił w ramach ustawy o ochronie ludności i obronie cywilnej powołać system bezpiecznej łączności państwowej. Opisany tam system koncentruje się na współdziałaniu wszystkich służb odpowiedzialnych za porządek, ratownictwo i ochronę służb, które są zarówno zarządzane, nadzorowane przez ministra spraw wewnętrznych i administracji, jak i współpracujące z ministrem organem. W ramach tego systemu SBŁP wyodrębniono kilka podsystemów, już takich dedykowanych pod poszczególne technologie i jednym z podsystemów jest system łączności trankingowej SBŁP-T. To jest właśnie ten element łączności, który opisujemy w sprawozdaniu. Minister podjął decyzję, żeby jako system ogólnokrajowy wykorzystać system trankingowy, który był budowany wcześniej przez Komendanta Głównego Policji. Ten system umożliwi w sposób szyfrowany komunikowanie się służb, jednocześnie ma już dzisiaj zapewniony dosyć szeroki zasięg. Dzięki inwestycjom i takiej dosyć kontrolowanej rozbudowie obejmuje już dzisiaj ponad 60% pokrycia kraju. Dążymy do tego, żeby kraj był pokryty całkowicie systemami łączności, żeby służby, wykorzystując system trankingowy, niezależnie od tego, w którym są miejscu, mogły ze sobą się specjalnie komunikować. Jest on budowany przez Policję, bo Policja została wyznaczona przez ministra na organizatora tego podsystemu i ta rozbudowa odbywa się we współdziałaniu ze wszystkimi naszymi służbami. Jeśli będą państwo zainteresowani szczegółami, to oczywiście będziemy mogli szczegółowo odpowiadać na pytania. Tu oczywiście też mamy zabezpieczone finansowanie na ten system trankingowy, dlatego że on jest finansowany z programu obrony cywilnej i ochrony ludności. W momencie, w którym weszła w życie ustawa, to wprowadziła też nakaz tworzenia programu ochrony ludności i obrony cywilnej i tym programie są zawarte środki finansowe. Obecny program obejmuje lata 2025–2026 i w takim cyklu mamy zaplanowane wydatkowanie środków.

Następną grupą są systemy łączności mobilnej. Dzisiaj, jeśli mówilibyśmy o systemach łączności mobilnej, to z punktu widzenia SBŁP jest to kategoria SBŁP-M. Dzisiaj mówimy o systemach wykorzystujących sieci komórkowe, które nie są systemami jawnymi. One funkcjonują i jest planowany ich dalszy rozwój, one są zintegrowane, ale szczegółowe informacje w tym zakresie nie są na tę Komisję, natomiast taki mechanizm również funkcjonuje.

Ostatnia grupa – łączność satelitarna – duże, rozwojowe zagadnienie. Dzisiaj ta łączność służy jako łączność zapasowa, w momencie, w którym brak jest tradycyjnych połączeń, wykorzystywana jest łączność satelitarna i to głównie oferowana przez jednego z komercyjnych dostawców takiej łączności. Natomiast UE od kilku lat przygotowuje się do uruchomienia dużego systemu łączności satelitarnej, który będzie takim paneuropejskim systemem i jednocześnie będzie działał w oparciu o całkowicie europejskie satelity, po to, żeby uniezależnić się od jednego komercyjnego dostawcy. Jako Polska uczestniczymy w tym programie. Minister spraw wewnętrznych i administracji jest odpowiedzialny za program GOVSATCOM i jego część Secure Connectivity. Jesteśmy bardzo mocno zaangażowani w budowę programu łączności satelitarnej o nazwie IRIS Square, trwają już takie prace. Komisja Europejska powołała konsorcjum, które odpowiada za budowę. Finalnie uruchomienie tych systemów jest planowane na 2027 r., ale już dzisiaj, funkcjonując w IRIS Square, otrzymujemy możliwość dostępu do łączności satelitarnej oferowanej przez część satelitów, które w tym programie będą funkcjonowały. Z naszego punktu widzenia – myślę, że to będzie wspólne zdanie dyrektorów pionów odpowiedzialnych za IT w służbach – najpoważniejszym problemem, który dzisiaj postrzegamy, są rosnące koszty i to lawinowo rosnące koszty utrzymywania takich systemów. O ile udaje się pozyskiwać środki na inwestycje, chociażby dzięki programowi ochrony ludności i obrony cywilnej, to stoją przed nami kolosalnie duże wyzwania związane z utrzymywaniem systemów, które już są, z podniesieniem tych technologii, z wymianą starych urządzeń na nowe. Z uwagi na to, że te obszary były niedofinansowane przez wiele lat, teraz mamy taki problem. Odrębnym zagadnieniem, ale równie istotnym są kadry. Jako sfera publiczna nie jesteśmy w stanie zapewnić tak samo wysokich stawek jak podmioty komercyjne, więc też mamy dużo mniejszy dostęp do specjalistów. Staramy się, jak możemy, żeby temu przeciwdziałać, ale to są problemy i braki, z którymi się na co dzień borykamy. To jest taka nasza wspólna konkluzja.

Generalnie w opinii MSWiA, jeśli chodzi o łączność pomiędzy służbami, to dzisiaj sytuacja jest opanowana, kontrolowana i w tych podstawowych elementach mamy zapewnioną komunikację,

głównie bazując na systemach łączności stacjonarnej. Ten moduł łączności radiowej jest bardzo dynamicznie rozwijany i tak naprawdę z dnia na dzień dostępność się zmienia. Nad pozostałymi elementami pracujemy i te prace odbywają się w ramach SBŁP, czyli Systemu Bezpiecznej Łączności Państwowej.

To chyba tyle krótkiego podsumowania tej informacji. Oczywiście jesteśmy gotowi na udzielenie odpowiedzi na szczegółowe pytania, jeśli państwo posłowie będziecie zainteresowani.

Przewodniczący poseł Wojciech Król (KO):

Oczywiście, bardzo dziękuję. Dziękuję również za informację, którą otrzymaliśmy, bardzo szczegółową.

Dziękuję za zwrócenie też uwagi na wyniki kontroli NIK. Tych zagrożeń dzisiaj dostrzegamy coraz więcej i jednym z takich słabych elementów była łączność. Dobrze, że te inwestycje mają miejsce, ale technologia też się nieustannie zmienia i rozwija. Nie tylko jednorazowe inwestycje, choćby nawet duże, tak jak teraz są czynione, ale również stały rozwój tych systemów i zabezpieczeń jest potrzebny, więc nie tylko utrzymanie, które jest drogie, ale również bieżące inwestycje w rozwijające się systemy i to też musimy uwzględniać. Nowe systemy powstają, powstają też nowe narzędzia do tego, żeby je rozszyfrowywać, w związku z tym ta technologia musi nieustannie się zmieniać. Jeszcze raz dziękuję za informację. Poproszę teraz naszych gości, przedstawicieli różnych służb, o chociażby kilkudzaniowe uzupełnienie, z nastawieniem właśnie na specyfikację swojej służby. Zdaję sobie sprawę, że pewnie w policji jest najwięcej wyzwań związanych z łącznością bieżącą. Sam też rozmawiałem z policjantami i wiem, że jest to taki słaby punkt, który wymaga inwestycji, dlatego pozwolę sobie zacząć od policji. Bardzo proszę pana inspektora o zabranie głosu.

Dyrektor Biura Łączności i Informatyki w Komendzie Głównej Policji insp. Przemysław Więclaw:

Bardzo dziękuję, panie przewodniczący. Szanowni państwo, mam przyjemność przedstawić przed państwem informację, tak jak pan przewodniczący powiedział, bardzo skrótową na temat środowiska teleinformatycznego, za które odpowiada Policja.

Celowo używam słów „za które odpowiada Policja”, ponieważ usługi, które są generowane w przestrzeni teleinformatycznej Policji, są wykorzystywane, tak jak pan dyrektor powiedział, przez wiele tysięcy instytucji w naszym kraju. Otóż policja na dzień dzisiejszy na poziomie centralnym realizuje swoje zadania w oparciu o 79 systemów centralnych. Na poziomie komend wojewódzkich jest to ponad 360 systemów różnego rodzaju w zakresie różnych technologii. Jeżeli chodzi o kwestie obszarów, w których się poruszamy, są to obszary zarówno jawne, niejawne, międzynarodowe i krajowe. I tutaj pozwolę sobie przytoczyć takie przykładowe obszary, które być może państwu są znane, jednak są istotne z punktu widzenia funkcjonowania naszego państwa – oczywiście to, o czym mogę mówić w postaci informacji jawnej. Mówimy tutaj chociażby o tym, że komendant główny Policji jest dzisiaj centralnym organem technicznym Krajowego Systemu Informatycznego, więc Policja odpowiada dzisiaj tak naprawdę za centralną infrastrukturę, która umożliwia nam korzystanie z dobrodziejstw strefy Schengen, a więc korzystanie z ruchu bezgranicznego, co dotyczy zarówno osób, jak i towarów. W ramach KSI utrzymywany jest i rozwijany Schengen Information System, wizowy system informacyjny, jak również Eurodac. Policja dzisiaj również odpowiada za największy w tym kraju niejawny system, to jest system Krajowego Centrum Informacji Kryminalnych i tutaj z punktu widzenia samej ustawy właściwie wszystkie instytucje, z uwagi na to, że są zobowiązane do udzielania odpowiedzi szefowi KCIK, są użytkownikami tego systemu.

Kolejnym dużym systemem, za który odpowiada dzisiaj Policja, oczywiście tak jak pan dyrektor powiedział, wspólnie z MSWiA, jest kwestia utrzymania i rozwijania OST 112, a więc systemu, który stanowi KOR, jeżeli mówimy dzisiaj o chociażby ratownictwie medycznym. Ale tak jak było wspomniane, na bazie tej sieci wykorzystywane są również inne usługi dla różnych instytucji, jak chociażby łączność przewodowa. Państwo zapewne o tym wiecie, że Policja jest operatorem wyróżnika AB=47, więc mamy swoją sieć komunikacyjną, z której korzystają praktycznie wszystkie instytucje rządowe w naszym państwie.

Następny system, z którego państwo zapewne korzystacie, to policyjny system wideo, który stał się od pandemii podstawowym systemem komunikacji w ramach administracji rządowej. Mógłbym wymieniać tych systemów dużo i skala odpowiedzialności za te systemy jest oczywiście ogromna, ale chętnie odpowiem na szczegółowe pytania dotyczące każdego z nich. Natomiast

chciałbym zaznaczyć kwestie globalne, które dotyczą utrzymania tak rozległej infrastruktury teleinformatycznej. Otóż z punktu widzenia zasobów, którymi dysponuje Policja, na dzień dzisiejszy obserwujemy zjawisko powiększania się tzw. długu technologicznego. To jest to, o czym wspomniał pan przewodniczący, a więc tak naprawdę technologia się rozwija, musimy dbać o to, aby ta technologia, którą wykorzystujemy, odpowiadała naszym potrzebom z punktu widzenia cyberbezpieczeństwa, z punktu widzenia bezpieczeństwa teleinformatycznego, jak również funkcjonalnego. My szacujemy na dzień dzisiejszy, że tak jak w przypadku OST 112, dzisiejszy budżet, którym dysponujemy rocznie, to jest około 40 mln zł, a nam dzisiaj potrzeba tylko na tę sieć około 100 mln zł rocznie. Budżet teleinformatyki policyjnej średnio to jest około 300 mln zł w ciągu roku, z czego znowu szacujemy, że około 1/3 jest przeznaczona na usługi, z których korzystają instytucje zewnętrzne. Na dzień dzisiejszy aktywnych kont w naszych systemach, z których korzystają różni użytkownicy, jest ponad 800 tys. i my też musimy je utrzymywać. Dodatkowo w środowisku teleinformatycznym, za które odpowiada Policja, jest coś, co nazywamy długiem informacyjnym i z punktu widzenia długu informacyjnego my szacujemy, że na dzień dzisiejszy potrzeba około 400 osób – nie mówię o etatach, bo etaty mogą się znaleźć, ale osób. Nawiązuję tutaj do tego, o czym powiedział pan dyrektor na temat możliwości pozyskania takich osób do pracy w teleinformatyce, nie tylko policyjnej, ale również innych służb, że jest to bardzo utrudnione. Stąd ten dług technologiczny w połączeniu z długiem informacyjnym, który stale rośnie, powoduje zagrożenie i powoduje zagrożenie nie tylko dlatego, że nie możemy wdrażać funkcjonalności, które są potrzebne dzisiaj na rynku administracji rządowej czy administracji samorządowej, ale nie możemy też powiedzieć, że bezpieczeństwo, za które odpowiadamy, jest na poziomie ryzyka, który jest dla nas odpowiedni, więc na pewno w tym przypadku są to zagrożenia, które występują w postaci różnego rodzaju podatności.

Z punktu widzenia technologii, którą stosujemy, na dzień dzisiejszy w naszym obszarze, czyli w obszarze technologii teleinformatycznych stosowanych na poziomie centralnym, szacujemy, że tych specjalizacji jest około 30. Czyli możemy tu zwrócić uwagę na to, że nie tylko ilość, ale jakość w różnych specjalizacjach jest niezbędna. Podam taki przykład, że osoba, która do nas trafia, która ma wykształcenie informatyczne, potrzebuje od 3 do 5 lat, aby poznać architekturę rozwiązań, poznać specyfikę funkcjonowania baz danych, specyfikę funkcjonowania sieci teleinformatycznych. Dla przykładu: w dwóch systemach, w tych podstawowych systemach policyjnych, czyli Krajowym Systemie Informacyjnym Policji oraz SWD (System Wspomagania Dowodzenia Policji) dziennie przetwarzamy około 5 petabajtów danych. Są to ogromne ilości danych na bazach, które liczą po kilka albo kilkanaście milionów obiektów, więc tym trzeba zarządzić. Tym trzeba zarządzić w sposób taki, że korzystamy oczywiście z firm zewnętrznych, ale przez ograniczenie finansowe nie możemy spowodować, aby to SLA, które utrzymujemy na odpowiednim poziomie, nas zadawała. Czyli z punktu widzenia korzystania przez użytkowników z naszych systemów widzimy, że jest możliwość uzupełnienia poprzez finansowanie i poprzez zabezpieczenie odpowiednich zasobów kadrowych.

Jeżeli mówimy o kwestiach przyszłości, to musimy mieć na uwadze nie tylko to, o czym dzisiaj wszyscy mówią, czyli o sztucznej inteligencji, a więc o tym, że musimy inwestować w nowe technologie, nie tylko te, które wykorzystujemy on-premowo, ale również technologie internetowe, czyli chmura, sztuczna inteligencja. To tu rzeczywiście obserwujemy, że w porównaniu do naszych kolegów z wojska policja jest traktowana troszeczkę inaczej. Pomimo tego, że mamy ogromne zadania, które są związane z obronnością naszego państwa, bo sama ustawa mówi o tym, że my podlegamy mobilizacji, więc na pewno te zadania realizujemy, ale realizujemy te zadania na co dzień. Jesteśmy dzisiaj na pierwszej linii, jeżeli chodzi o wojnę hybrydową w cyberprzestrzeni. Tutaj mogę podać taki przykład i to jest informacja absolutnie jawna, że wszelkie działania, które są prowadzone za wschodnią granicą, jak chociażby ćwiczenia „Zapad”, powodują, że my w naszych sieciach widzimy od razu, co się dzieje, czyli widzimy tak naprawdę wzrost aktywności naszych adversarzy w postaci chociażby zwiększonej liczby ataków DDoS. To jest tylko przykład, który pokazuje, że Policja nie tylko bierze udział w działaniach kinetycznych czy działaniach fizycznych, ale również w działaniach w cyberprzestrzeni i to jest komponent, który wymaga radykalnego uzupełnienia na dzień dzisiejszy. To, co mówimy o sztucznej inteligencji, to rzeczywiście trudno sobie dzisiaj wyobrazić, że w przyszłości bez sztucznej inteligencji będziemy mogli działać. Dzisiaj szczątkowo wykorzystujemy sztuczną inteligencję chociażby na naszych firewallach po to, żeby przeciwdziałać zagrożeniom sieci Internet. Natomiast potrzeby są ogromne, zarówno w specjalizacjach w ramach sztucznej inteligencji, jak

również w wykorzystaniu sztucznej inteligencji do naszej codziennej pracy, chociażby w analizach kryminalnych. To jest tylko jeden obszar, w którym możemy to wykorzystywać.

Jeżeli chodzi o technologie chmurowe, oczywiście nie ma na dzień dzisiejszy decyzji strategicznej naszego kraju, że taka instytucja jak nasza może wejść do chmury któregoś z operatorów. Wykorzystujemy technologie chmurowe prywatne, czyli wykorzystujemy tak naprawdę technologie na naszej infrastrukturze. I to jest obszar, który jest w coraz większym stopniu przez nas zagospodarowywany, a więc coś, co nazywamy MTN-ami, czyli mobilne terminale noszone, w które wyposażamy naszych policjantów, po to, aby odejść od kwestii papierowych. I na dzień dzisiejszy mogę powiedzieć, że już w tej chwili wykorzystanie MTN-ów jest na poziomie około 15 tysięcy. W tej chwili następna dostawa będzie w styczniu – to jest znów około 15 tys. i docelowo będzie to liczba około 45 tys. terminali. Te terminale mają dostęp do wszystkich systemów policyjnych, ale też mają dostęp do wszystkich niezbędnych baz danych w postaci rejestrów publicznych. Tu chciałem powiedzieć, panie przewodniczący, że oprócz tego, że mówimy w tej chwili głównie o funkcjonalnościach, bezpieczeństwie i o tym, co mamy, nie sposób nie wspomnieć, że my jako administracja rządowa niezwykle potrzebujemy infrastruktury serwerowej. To jest dla nas *core*, który w tej chwili się wyczerpuje. My mamy problemy w tej chwili we wdrażaniu nowych funkcjonalności z punktu widzenia wydajności, z punktu widzenia możliwości postawienia nowej infrastruktury teleinformatycznej w tych serwerach, które mamy. Takie samo ograniczenie dotyczy sieci, bo sieci też mają ograniczoną przepustowość, i włączenie nowych funkcjonalności, jak chociażby obrazu wideo z kamer nasobnych policjantów w sposób scentralizowany – ta infrastruktura na dziś na to nie pozwala. Niemniej jednak, tak jak wspominałem wcześniej, jeżeli stawiamy sobie za cel odpowiednie SLA, odpowiednią ciągłość działania poszczególnych systemów, ona jest na dzień dzisiejszy utrzymywana i mogę powiedzieć, że nasza infrastruktura teleinformatyczna na dziś jest bezpieczna. Dziękuję bardzo.

Przewodniczący poseł Wojciech Król (KO):

Bardzo dziękuję za wszystkie przekazane informacje. Wspomniał pan o sztucznej inteligencji w kryminalistyce. Mówi się, że rozwój sztucznej inteligencji będzie w Policji miał tak przełomowe znaczenie jak badania DNA, które zmieniły wykrywalność przestępstw. Bardzo jeszcze raz dziękuję za informację. I poproszę teraz Państwową Straż Pożarną, pana naczelnika, żeby ze swojego punktu widzenia i specyfiki służby opowiedział o systemach łączności i inwestycjach. Bardzo proszę.

Naczelnik w Komendzie Głównej Państwowej Straży Pożarnej st. bryg. Kazimierz Gogacz:

Panie przewodniczący, szanowni państwo, PSP wykorzystuje systemy łączności zarówno stacjonarnej, mobilnej, radiowej, wideokonferencyjnej, jak i satelitarnej.

Stan obecny, w którym zgodnie z ustawą o ochronie ludności i obronie cywilnej narzucono nam systemy w zakresie łączności trunkingowej, radiowej, jest na etapie przygotowania i rozbudowy. Łączność telefoniczna w PSP stacjonarna stanowi podstawowy element infrastruktury komunikacyjnej wykorzystywany w codziennej pracy administracyjnej, jak i w działaniach operacyjnych. Natomiast w zakresie łączności radiowej, łączność mobilna wykorzystywana jest jako kanał komunikacyjny dodatkowy wspierający działania operacyjne, jak i koordynacyjne oraz administracyjne. Łączność ta oparta jest na infrastrukturze komercyjnych operatorów w sieci telefonii mobilnej. Kolejnym elementem systemów łączności radiowej PSP są analogowe systemy łączności w paśmie VHF, jak i systemy DMR oraz systemy TETRA. Są to podstawowe systemy do realizacji działań operacyjnych PSP. Każdy z wymienionych systemów pełni odrębną rolę w organizacji, znajduje zastosowanie na różnych poziomach dowodzenia i współdziałania, od lokalnego, poprzez wojewódzki, aż po centralne. W oparciu o systemy łączności analogowej i radiowej funkcjonują również jednostki ochotniczych straży pożarnych. Jest około 16 tys. takich jednostek, z czego ponad 5 tys. znajduje się w Krajowym Systemie Ratowniczo-Gaśniczym. W związku z tym każda modernizacja systemów łączności PSP wiąże się z uwzględnieniem potrzeb również ochotniczych straży pożarnych, gdzie w strukturach łączności znajduje się około 100 tys. radiotelefonów. Jest to duże wyzwanie w celu zabezpieczenia tak dużej liczby sprzętu łączności, żeby zapewnić odpowiedni poziom bezpieczeństwa czy szyfrowania komunikacji. W związku z powyższym ustawa modernizacyjna, która nakłada nowe kierunki w zakresie wyposażenia i rozbudowy tych systemów, jest obecnie kluczowym elementem, aby tym wyzwaniom w zakresie łączności sprostać.

Kolejną rzeczą, przed którą stoi PSP, są ograniczenia systemu analogowego, który nie zapewnia standardów bezpieczeństwa. To jest właśnie koncepcja przyjęta w 2023 r. przez PSP w zakresie migracji na cyfrową łączność radiową, która umożliwi szyfrowanie komunikacji w sieciach łączności, natomiast jest też polem do integracji z łącznością używaną w jednostkach ochotniczych straży pożarnych. Jesteśmy na etapie i na przedpolu, żeby zapewnić możliwość całościowego zafunkcjonowania PSP w systemie TETRA, gdzie ten element jest uzależniony od centralnych rozwiązań, które nadzoruje policja. W ramach systemu TETRA PSP funkcjonuje w oparciu o wojewódzkie stanowiska kierowania, natomiast docelowy model zakłada, żeby PSP była w tym systemie łączności cyfrowej TETRA w całości wdrożona. Natomiast wyzwaniem jest taki model, gdzie wszystkie jednostki PSP, jak i wspierające działania ratowniczo-gaśnicze jednostki OSP były zabezpieczone systemami bezpiecznej łączności państwowej – mówię tu o systemie TETRA, który umożliwiłby zachowanie pełnego bezpieczeństwa. Systemy TETRA, które zapewniają nam pełne szyfrowanie i współdziałanie z innymi służbami, w tym z policją, podczas działań ratowniczo-gaśniczych są kluczowe, żeby je rozwijać i wdrażać.

Ponadto PSP wykorzystuje narzędzia wideokonferencyjne do prowadzenia bieżącej komunikacji, które zostały mocno rozwinięte podczas pandemii. Wdrożono rozwiązanie w zakresie wykorzystywania komunikacji wewnętrznej, m.in. rozwiązania Microsoftu MS-365, jak i systemy wideokonferencyjne działające w ramach resortowych systemów wideokonferencyjnych administrowanych przez policję.

Niezmierzalnym ważnym elementem w działaniach PSP jest sieć satelitarna, która zapewnia dostawę usług IT podczas kryzysu, szczególnie kiedy działania kryzysowe mają miejsce, kiedy infrastruktura komercyjna ulega awarii bądź jest skolejkowana i nie ma zapewnionej dostępności. Wtedy niezależne kanały satelitarne umożliwiają dostęp do baz danych czy komunikacji wewnątrz służb podczas działań operacyjnych. W strukturach PSP funkcjonuje łączność niejawną w oparciu o rozwiązania systemowe ABW, poza tym obecnie budowany i wdrażany jest system komunikacji rządowej SKRZ. Kolejnym elementem, który jest rozwijany i służy do integrowania systemów łączności, była rozbudowa systemu ostrzegania alarmowania i wdrożenie infrastruktury do sieci SD-WAN w PSP, obejmującej 553 lokalizacje PSP w celu połączenia systemami łączności i bezpiecznej komunikacji jednostek PSP. Rozwiązanie to zakłada redundancję, wysoką dostępność łączy i centralne zarządzanie oraz monitoring i zaawansowane mechanizmy bezpieczeństwa, to jest szyfrowanie, firewalle i elastyczne kształtowanie ruchu sieciowego oraz pełną kompatybilność z obecnymi systemami teleinformatycznymi.

PSP realizuje również projekt budowy ogólnokrajowego systemu ostrzegania alarmowania ludności, który jest kluczowym elementem w zakresie ustawy o ochronie ludności i obronie cywilnej. System ten ma docelowo umożliwiać uruchamianie i monitorowanie syren alarmowych w zakresie podniesienia bezpieczeństwa i alarmowania ludności. Ponadto na wyposażeniu PSP znajdują się samochody dowodzenia łączności stanowiące mobilne stanowiska kierowania oraz zaplecze teleinformatyczne. Obecnie jesteśmy na etapie zakupu i modernizacji takich wozów. Wyposażenie tych pojazdów musi być dostosowane do obecnych standardów bezpieczeństwa, jak i łączności, w tym wyposażenie w terminale łączności cyfrowej i TETRA.

Istotnym elementem w obszarze prawnym, który służy do rozwijania i modernizacji systemów łączności PSP, jest ustawa o ochronie ludności i obronie cywilnej, która między innymi ustanawia podstawy funkcjonowania systemu bezpiecznej łączności państwowej. Celem tego przedsięwzięcia jest zintegrowanie istniejących systemów teleinformatycznych, radiokomunikacyjnych służb w jeden spójny ekosystem. W zakresie obecnych zdolności sprzętowych, operacyjnych PSP technicznie jest przygotowana na rozwój i rozbudowę tych systemów, zwłaszcza że środki z programu modernizacji będą w głównej mierze spożytkowane na doposażenie systemu łączności, radiotelefony dla jednostek PSP. Natomiast w zakresie, który widzimy, który jest też problematyczny, PSP stara się o zwiększenie liczby etatów w zakresie kadry do systemów IT i łączności i tutaj kluczowa jest ścisła współpraca z ministerstwem, jak i służbami podległymi, nadzorowanymi przez resort. Stanowi to kluczowy element do modernizacji systemów łączności PSP. W związku z powyższym dalszym kierunek modernizacji systemów łączności PSP będzie realizowany zgodnie z opracowanymi wytycznymi, rozwojem systemu bezpiecznej łączności państwowej oraz własnymi potrzebami wynikającymi ze specyfikacji służby. Dziękuję za uwagę.

Przewodniczący poseł Wojciech Król (KO):

Dziękuję bardzo. Dziękuję, że zwrócił pan uwagę na współpracę i koordynację z ochotniczymi strażami pożarnymi, bo myślę, że ma to istotne znaczenie ze względu na ich uczestnictwo w akcjach ratunkowych. Poproszę o wyłączenie mikrofonu.

A teraz poproszę przedstawiciela Straży Granicznej, pana pułkownika, o przedstawienie informacji z uwzględnieniem problemów wynikających z kryzysu migracyjnego i działań hybrydowych na granicy polsko-białoruskiej. Wiem, że istotnym elementem jest właśnie bezpieczna łączność, zapewniająca bezpieczeństwo bezpośrednio osobom, które chronią granicę, ale proszę także o zwrócenie uwagi na koordynację z innymi służbami, które są na granicy, czyli z policją i wojskiem. I oczywiście proszę, aby pan również wspomniał o tej specyfice i planowanych inwestycjach. Bardzo proszę.

Dyrektor Biura Łączności i Informatyki w Komendzie Głównej Straży Granicznej płk SG Mariusz Kijowski:

Dziękuję. Panie przewodniczący, szanowni państwo, może rzeczywiście najpierw od kwestii łączności radiowej zacznę, która w kontekście presji migracyjnej na granicy z Białorusią stanowi podstawowe narzędzie, jeśli chodzi o komunikację między patrolami, w tym patrolami łączonymi z wojskiem, z policją. Nasz system łączności radiowej jest oparty o DMR. Jest to łączność cyfrowa, w pełni szyfrowana. System łączności radiowej, który funkcjonuje na granicy z Białorusią, przeszedł swój test podczas kontroli NIK, która oceniła ten system bardzo dobrze. Ale tym najistotniejszym elementem jest oczywiście jego odporność na bardzo wysoką presję migracyjną i oczywiście konieczność obsłużenia, zapewnienia komunikacji wszystkim patrolom, które na granicy były. Przytoczę tutaj jedną liczbę: w kryzysie, w takim najbardziej obciążonym okresie wystawiliśmy wspólnie, my od strony łączności radiowej, ponad 1700 patroli. Ten system wytrzymał to, choć w założeniach nie powinien to być system do aż tak dużego obciążenia. W ramach tego systemu łączności radiowej wszystkie nasze patrole są na bieżąco monitorowane. One są jakby w trybie online i ich położenie jest prezentowane w Systemie Wspomagania Kierowania, który został wykonany siłami własnymi funkcjonariuszy, także mamy taką mapę zarządczą i na każdym poziomie placówki, komendy oddziału oraz komendy głównej można zobaczyć, jak te patrole samochodowe czy też patrole piesze się przemieszczają. Oprócz zwiększenia możliwości zarządzania siłami, środkami to jest kluczowy element, jak pan przewodniczący powiedział, bezpieczeństwa funkcjonariuszy, dzięki któremu wiemy, gdzie funkcjonariusze się znajdują.

Przechodząc do kwestii presji migracyjnej, podobnie jak koledzy z Policji, widzimy zbieżność działań..., gdy obserwujemy działania kinetyczne bądź pewne incydenty związane w tej sferze rzeczywistej, ma to odzwierciedlenie w atakach na infrastrukturę służb. My jako SG w 2015 r., już po aneksji Krymu, zbudowaliśmy pierwsze struktury Security Operations Center, tj. zespołu do szybkiego reagowania, i rozwijamy je sukcesywnie. Oczywiście siła ataków, ich częstotliwość jest coraz większa i my to obserwujemy. Co więcej, w ostatnim czasie obserwujemy ataki, które są przygotowywane pod instytucje, to już nie są zwykłe ataki paraliżujące, tylko są to ataki, w których widać, że pewne schematy logowania czy też schematy zachowania użytkowników są wykorzystywane do tego typu przedsięwzięć.

Dlaczego dla nas cyberbezpieczeństwo jest tak ważne? I tutaj przejdę już właśnie do zadań, które na bieżąco realizujemy. Otóż SG ma kilka trudnych zadań, które wymagają olbrzymich przedsięwzięć, jeśli chodzi o bezpieczeństwo i łączność. Pierwszym jest krajowy system informacji PNR, czyli system przeciwdziałania zagrożeniom terrorystycznym oraz poważnym przestępstwom. Dzięki temu systemowi pozyskujemy informacje o pasażerach linii lotniczych z systemów rezerwacyjnych przewoźników lotniczych. Otrzymujemy listy pasażerów i na bazie tych informacji, wysyłanych na 48 godzin przed przylotem, dokonujemy analiz, w tym analiz kryminalistycznych w odniesieniu do tych osób, czy nie stanowią one istotnego zagrożenia dla bezpieczeństwa na pokładach statków, bezpieczeństwa państwa. Ten system jest o tyle istotny, że z jednej strony mamy połączenie z Internetem, a z drugiej strony musimy dostarczyć te informacje do służb, w tym służb specjalnych, czyli systemów niejawnych. Z tego punktu widzenia dla nas jest to otwarcie, które wynika z realizacji zadań ustawowych, natomiast wymaga szczególnej ochrony.

Kolejnym elementem istotnym z punktu widzenia bezpieczeństwa jest oczywiście fakt, że wszystkie nasze patrole są wyposażone w rozwiązania teleinformatyczne, ponieważ wszystkie

procesy zarówno migracyjne, jak i związane z wydawaniem decyzji są w pełni scyfryzowane. Te zadania zostały też wykonane siłami własnymi funkcjonariuszy Biura Łączności i Informatyki.

Teraz z mojej jakby perspektywy, w związku z tym, że realizujemy szereg zadań związanych z kodeksem granicznym Schengen, to też jesteśmy oceniani od strony informatycznej. Takie dwa parametry, które nam przyświecają, to jest niezawodność systemów na poziomie 99,99%, to znaczy niedostępność ich przez około 52 minuty w skali roku oraz zapewnienie odpowiedzi systemów na poziomie poniżej 5 sekund. I teraz odniosę się do tych elementów. Otóż najistotniejszym oczywiście systemem SG, najtrudniejszym, jest system odpraw granicznych. Każdej doby placówki SG przetwarzają, obsługują 100 tys., czasem też do 180–200 tys. osób dziennie. To oznacza, że każdy pasażer, każda osoba odprawiana jest sprawdzana w kilkunastu bazach. Te bazy są rozlokowane w Unii Europejskiej, w Interpolu, są to bazy krajowe. Te bazy są dostępne dla nas w przedziale czasowym poniżej 1 sekundy. Jeżeli system działa, to po dokonaniu odczytu funkcjonariusz w takim czasie dostaje pełną informację o osobie, o dokumentach, które on prezentuje, czy też o pojazdach, którymi się przemieszcza. Średnio 8 mln zapytań i odpowiedzi każdej doby przetwarzamy przed wdrożeniem systemu, o którym powiem za chwilę. Stąd agregacja tych informacji wymaga niezawodnej łączności stacjonarnej, ale również mobilnej. Olbrzymim wyzwaniem dla nas jest drugi system unijny, który wdrażamy właśnie w chwili obecnej. To jest system, który podnosi bezpieczeństwo państwa w skali dotąd niespotykanej. Otóż od 12 października SG wdraża w całej administracji rządowej system Entry-Exit. To jest taka nowoczesna odprawa graniczna, która jest oparta o biometrię. Każdemu cudzoziemcowi, co do zasady, z pewnymi wyjątkami, w ramach pobytów krótkoterminowych będzie zrobione zdjęcie na żywo oraz pobrane odciski czterech palców. Te dane służą następnie zaawansowanej identyfikacji cudzoziemców. Chodzi o to, że w państwach ościennych czy też w państwach trzecich istnieje możliwość posługiwania się dokumentami na zmienione dane, i to jakby w świetle prawa. Można zmienić imię, nazwisko, a w niektórych państwach nawet datę urodzenia. To są sytuacje, których chcemy oczywiście unikać i tutaj system Entry-Exit będzie tym narzędziem, ponieważ biometria to są unikalne cechy, które powodują, że osoby są jednoznacznie zidentyfikowane. W tym ujęciu dostarczyliśmy do wszystkich instytucji, w tym urzędów wojewódzkich, możliwość korzystania z tego systemu na bazie uprawnień, o których mówi dedykowana ustawa. Innym obszarem, który jest dla nas niezwykle istotny, to jest kwestia zapewnienia weryfikacji cudzoziemców w kontekście różnych benefitów, które państwo polskie im oferuje. Niedawno weszła ustawa o weryfikacji cudzoziemców i na bazie tego rozbudowujemy nasz Krajowy Rejestr Cudzoziemców, dzięki czemu zapewniamy identyfikację cudzoziemców dla służb, które wypłacają benefity. Są to olbrzymie środki i uczestniczymy w tym procesie uszczelnienia. Jeśli chodzi o łączność jako taką, to oczywiście tak jak wspominałem, wszystkie patrole w związku z tym, że muszą pobierać biometrię, wykonują też czynności administracyjne, korzystamy z zabezpieczonej sieci komórkowej. W niektórych miejscach, gdzie jest to potrzebne w związku z przywróceniem kontroli granicznej, wykorzystujemy łączność satelitarną.

Panowie dyrektorzy wspominali o kwestiach osobowych. Co do zasady u nas wszystkie systemy kluczowe, jeśli chodzi o infrastrukturę krytyczną, budujemy siłami własnymi, nie tylko dlatego, że to jest bardziej efektywne kosztowo, ale dlatego, że od 2012 r. przyjęliśmy określoną strategię i te 52 minuty, o których mówiłem, były przy rozwiązaniach komercyjnych często przekraczane, co było dla nas niesatysfakcjonujące. W związku z tym wybudowaliśmy nowoczesny system odpraw granicznych, rozbudowujemy go do dzisiaj. W związku z tym struktury biura łączności są niezwykle istotne dla operacyjnego funkcjonowania SG. Dostrzegamy oczywiście coraz większe potrzeby osobowe, staramy się z tym sobie radzić. Niedawno rozpoczęliśmy – choć nie jest to związane z łącznością – taką kampanię „Informatyka w mundurze”. Bardzo istotnym elementem – i myślę, że będę wyrazicielem opinii wszystkich tu obecnych panów dyrektorów – bardzo istotnym elementem jest doświadczenie teleinformatyczne, które pozwala nam rzeczywiście konkurować i pozyskiwać osoby. Była dzisiaj mowa o sztucznej inteligencji – oczywiście my też ją wykorzystujemy troszkę w analizie danych, i to jest jakby jeden element, ale mogę tu też zdradzić, oczywiście to jest informacja jawna, że w jednym z oddziałów, dokładnie w podlaskim, sztuczna inteligencja jest wykorzystywana do rozpoznawania, czy to jest osoba, czy to jest zwierzę, czy to jest jakiś ruch gałęzi. I rzeczywiście to ma bardzo wysoką skuteczność, jesteśmy po kilkuletnich testach.

Wracając jeszcze do tego elementu: doświadczenie teleinformatyczne jest kluczowym czynnikiem motywacyjnym dla utrzymania kadr, ale też ich rozwoju. Musimy pamiętać, że w obliczu

zagrożeń, o jakich tu była mowa, o cyberbezpieczeństwie, cyberterroryzmie, który nas wszystkich dotyka, szczególnie w sferze cywilnej jesteśmy bardzo mocno narażeni. Podobnie jak koledzy z policji, my przez całą dobę wykonujemy zadania i te zadania często są oparte na informacji. Brak informacji bądź jakakolwiek zmiana informacji powoduje, że przestajemy być skuteczni bądź też nasza skuteczność jest znacznie ograniczona. Dlatego silne piony łączności, informatyki, które budują systemy, które wspierają nasze działania ustawowe, to kluczowy element bezpieczeństwa państwa. Dziękuję, panie przewodniczący, dziękuję państwu.

Przewodniczący poseł Wojciech Król (KO):

Bardzo dziękuję za tę szczegółową informację. Przejdziemy teraz do Służby Ochrony Państwa – formacji, która może nie ma takiego bezpośredniego kontaktu z obywatelami jak formacje, które wcześniej prezentowały swoje stanowiska, ale o strategicznym znaczeniu dla bezpieczeństwa instytucji państwowych, bezpieczeństwa struktur państwa. I również tutaj poproszę w tym zakresie jawnym o informację dotyczącą planowanych inwestycji i specyfiki służby. Bardzo proszę, panie pułkowniku.

Zastępca dyrektora Zarządu Łączności i Informatyki w Służbie Ochrony Państwa płk SOP Michał Majek:

Panie przewodniczący, szanowni państwo, w SOP ze względu na specyfikę w szczególności wykorzystujemy łączność radiową bezpośrednią. Jest to rozwiązanie na tę chwilę oparte na technologii NXDN.

W zakresie dalszego kierunku rozwoju łączności radiowej bierzemy udział w rozwoju sieci SBLP-T w celu zwiększenia interoperacyjności z pozostałymi służbami i myślę, że to jest bardzo dobry kierunek. Na pewno będą z tego dodatkowe korzyści, takie jak polepszona wymiana informacji pomiędzy SOP a pozostałymi służbami, z którymi na co dzień współpracujemy. Łączność mobilna w SOP traktowana jest jako łączność alternatywna podczas wykonywanych zadań. Opieramy się w głównej mierze na operatorach telekomunikacyjnych publicznych, zabezpieczając dodatkowo urządzenia, wykorzystując narzędzia typu wirtualne sieci prywatne, komunikatory bezpieczne. Jeżeli chodzi o łączność stacjonarną, realizujemy ją przede wszystkim we współpracy z Policją. Jest to oparte na sieci GovNet, jak również na operatorach sieci publicznej. W miejscach, gdzie na przykład brak dostępności łączności mobilnej wykorzystujemy łączność satelitarną, również opartą na rozwiązaniach komercyjnych. W zakresie systemów własnych, w zakresie jawnym mogę powiedzieć, że są to systemy wykorzystywane na nasze potrzeby z celu realizacji ustawowych zadań. I tyle z tego zakresu mogę dodać. Jeżeli chodzi o inwestycje, to przede wszystkim inwestycja w kierunku zwiększenia tej interoperacyjności ze służbami. Dziękuję.

Przewodniczący poseł Wojciech Król (KO):

Bardzo dziękuję panu pułkownikowi. Przejdziemy teraz do Krajowego Centrum Monitorowania Systemu Powiadomienia Ratunkowego, systemu, który jest kluczowy dla życia i zdrowia. Dlatego bardzo proszę, oddaję teraz głos pani naczelnik.

Naczelnik wydziału w Krajowym Centrum Monitorowania Systemu Powiadomienia Ratunkowego w Departamencie Ochrony Ludności i Zarządzania Kryzysowego w MSWiA Maria Skarzyńska:

Bardzo dziękuję, panie przewodniczący. Ja będę krótko się odnosiła, ponieważ nasz temat wiąże się z tematem dzisiaj poruszonym, właściwie głównie, jeśli chodzi o sieć OST 112, której jesteśmy głównym beneficjentem.

Dla naszego systemu ta sieć została zbudowana i jest absolutnie kluczowa, jeżeli chodzi o komunikację zarówno między centrami powiadamiania ratunkowego, których jest 17 w całym kraju, jak i między centrami powiadamiania ratunkowego a dyspozytorniami wszystkich trzech służb, z którymi współpracujemy. To jest ten zakres, który, jeżeli chodzi o działanie policji w kontekście dzisiejszego posiedzenia, najbardziej nas interesuje. Mogę też pokrótce przedstawić, jeżeli to pana przewodniczącego interesuje, jak funkcjonuje nasz system, jeżeli chodzi o stronę techniczną. Realizujemy to siłami MSWiA, nie siłami służb resortu, a siłami naszego ministerstwa, oczywiście ze wsparciem firm zewnętrznych, dlatego że Krajowe Centrum Monitorowania Systemu Powiadomienia Ratunkowego liczy zbyt mało osób, żeby móc sobie poradzić z utrzymaniem systemu, który musi działać w trybie ciągłym. Właściwie nie może przestać działać, ponieważ jego zatrzymanie powodowałoby ogromne perturbacje, jeżeli chodzi

o możliwość wezwania pomocy przez każdą osobę, która korzysta z numerów alarmowych 112, 997 i 998. Mamy w swoim zespole właśnie personel techniczny, który zajmuje się utrzymaniem technicznym tego systemu na zasadzie pierwszej i drugiej linii wsparcia. Jeśli chodzi o trzecią linię wsparcia, to korzystamy z firm zewnętrznych. Nasz system teleinformatyczny Centrum Powiadamiania Ratunkowego jest jednym systemem dla wszystkich centrów, łączy wszystkie centra i z wykorzystaniem interfejsu łączy się z systemami wspomagania dowodzenia Policji, Państwowego Ratownictwa Medycznego i z Systemem Wspomagania Decyzji Państwowej Straży Pożarnej. To tyle, jeśli chodzi o krótką architekturę naszego systemu. Jeżeli są jakieś pytania, to oczywiście bardzo chętnie odpowiem.

Przewodniczący poseł Wojciech Król (KO):

Bardzo dziękuję wszystkim państwu za informację, w całości bardzo szczegółową. Ale jest z nami również przedstawiciel Związku Miast Polskich pan Marek Wójcik i wiem, że chciał zabrać głos, dlatego bardzo proszę.

Pełnomocnik Zarządu Związku Miast Polskich Marek Wójcik:

Bardzo dziękuję. Panie przewodniczący, państwo posłowie, szanowni państwo, Marek Wójcik, Związek Miast Polskich.

Nieprzypadkowo jestem na spotkaniu z państwem, bowiem jednostki samorządu terytorialnego, jak słusznie zresztą państwo podnosicie w tej informacji – tutaj patrzę na pana dyrektora – mają zarówno w przypadku połączeń stabilnych stacjonarnych, jak i mobilnych, problem dotarcia na poziom lokalny, najniższy. Na bazie naszych doświadczeń i kontaktów z naszymi przyjaciółmi i samorządowcami z Ukrainy. Chcę bardzo wyraźnie podkreślić, że bardzo prosimy o to, abyście państwo uwzględnili możliwość, po pierwsze, włączenia administracji samorządowej w jak najszerszym zakresie we wszystkie możliwe systemy. Po drugie, pozwolili nam budować systemy wewnętrzne, które będą służyły nam do ograniczenia skutków zjawisk kryzysowych wtedy, kiedy grozi nam na przykład niemożliwość korzystania z sieci mobilnej. Ja przypominam sobie taką bardzo tragiczną sytuację z wichury na Kujawach, kiedy okazało się, że w momencie, kiedy braknie energii elektrycznej, to w całym powiecie nie można korzystać z sieci komórkowej, stają stacje benzynowe itd. My chcielibyśmy mieć możliwość działania w sytuacjach kryzysowych wtedy, kiedy mamy potrzebę kontaktowania się z naszymi służbami z perspektywy samorządów terytorialnych, ze służbami komunalnymi zajmującymi się oczyszczaniem miasta, dostarczaniem wody, transportu zbiorowego i szerzej, naszymi jednostkami organizacyjnymi. Stąd też chcieliśmy prosić o to, aby włączyć nas we wszystkie działania, w te projekty, które służą dofinansowaniu budowy systemów alternatywnych do tych, którymi dysponujemy dzisiaj.

Ja powiedziałem o Ukrainie, ale nasi przyjaciele w Ukrainie mówią wyraźnie: najbardziej potrzebne w sytuacji kryzysowej są środki transportu i komunikacja, i to komunikacja alternatywna. I to mówią wyraźnie, to nie jest pojedyncze doświadczenie. Właściwie za każdym razem, jak pytaliśmy się, co powinniśmy zrobić, to słyszeliśmy o tym. Zarówno w programie zbudowanym na bazie ustawy o ochronie ludności i obronie cywilnej, jak i w funduszu pożyczkowym, który się teraz buduje, w oparciu o środki, którymi będzie dysponował Bank Gospodarstwa Krajowego, prosimy o to, aby nas włączyć, żebyśmy byli systemowym partnerem. I raczej nie na tej zasadzie, że będą się o to dopominały pojedyncze samorządy, które mają np. zasoby kadrowe, żeby przygotować projekty, tylko systemowo włączać wszystkie jednostki samorządu terytorialnego, a przede wszystkim samorządy gminne we wszystkie możliwe systemy komunikacji, przekazywania sobie informacji. My mamy sporo doświadczeń w tej sprawie i żeby nie przedłużać, powiem jeszcze o jednym, dotyczącym klęsk powodzi. Tutaj też sprawa szybkiego przekazania informacji, łączności między poszczególnymi podmiotami, inspekcjami, służbami, strażami, administracją szczebla powiatowego, np. z gminą i naszymi jednostkami, była kluczowa i działać trzeba było szybko. Dlatego raz jeszcze proszę państwa o to, aby pojawiły się konkretne narzędzia potrzebne dla nas w takich sytuacjach. Potrzebne nam wszystkim, szerzej, administracji publicznej – to trzeba bardzo wyraźnie podkreślić. I dziękuję za to, że państwo zauważacie w tej informacji tego typu potrzeby. Dziękuję.

Przewodniczący poseł Wojciech Król (KO):

Dziękuję bardzo. Pytania nie było, więc nie będę oddawał głosu, chyba że pan dyrektor chce, tak? Bardzo proszę.

Dyrektor departamentu w MSWiA Dariusz Nowak-Nova:

Tak, mogę krótko odpowiedzieć. Z punktu widzenia ustawy o obronie ludności i ochronie cywilnej każdy samorząd, który realizuje zadania związane z zarządzaniem kryzysowym czy z ochroną ludności, z definicji jest podmiotem uprawnionym do korzystania z SBŁP, czyli z Systemu Bezpiecznej Łączności Państwowej. My też, kierując się taką zasadą, myślimy o tym, żeby z systemami komunikacyjnymi czy zapewniającymi komunikację zejść jak najniżej. Mamy zaplanowane końcówki systemu we wszystkich gminach, jak i również od przyszłego roku będziemy dostarczali do punktów, które sobie wypracujemy, takie mobilne systemy, węzły łączności, które będą umożliwiały łączność w sytuacjach, o których słyszeliśmy, że zakłócona jest możliwość łączności stacjonarnej z uwagi na powódź, wichurę itd. Wiemy więc o tym i pracujemy nad tym, żeby zejść jak najniżej. Od przyszłego roku już pewnie będą pierwsze efekty. Dziękuję.

Przewodniczący poseł Wojciech Król (KO):

Dziękuję bardzo, panie dyrektorze. Pan poseł Łukasz Ściebiorowski ma pytanie – proszę o wskazanie adresata.

Poseł Łukasz Ściebiorowski (KO):

Dziękuję. Panie przewodniczący, panowie dyrektorzy, naczelnicy, szanowna podkomisjo, pytanie o współpracę z systemami cywilnymi, jeżeli tak to mogę nazwać, ale również z systemami w harcerstwie, w różnych hufcach, które są ulokowane w większości miast i gmin. Czy też państwo z tego korzystacie? To pytanie może do pana dyrektora: czy jest taka współpraca, wykorzystanie tego systemu i wiedza, jakie w ogóle systemy tam są i czy one są przydatne w sytuacjach, nazwijmy to, zagrożenia? Dziękuję.

Przewodniczący poseł Wojciech Król (KO):

Pan dyrektor, bardzo proszę.

Dyrektor departamentu w MSWiA Dariusz Nowak-Nova:

Z punktu widzenia teleinformatyki nie przyglądaliśmy się systemom, które funkcjonują w związkach młodzieżowych, harcerskich, skautowskich. Wiem, że te organizacje pełnią swoje role w ramach obrony cywilnej i ochrony ludności, ale nie analizowaliśmy ich systemów teleinformatycznych.

Przewodniczący poseł Wojciech Król (KO):

Pan poseł, bardzo proszę.

Poseł Łukasz Ściebiorowski (KO):

Tam jest też wielu pasjonatów tych systemów łączności. Wiem, że do nauki młodych kadr ich używają, więc myślę, że mógłby to być taki kierunek, który warto byłoby zdiagnozować. Dziękuję.

Przewodniczący poseł Wojciech Król (KO):

Pan dyrektor, bardzo proszę.

Dyrektor departamentu w MSWiA Dariusz Nowak-Nova:

Tak, być może w kontekście wszelkiego rodzaju łączności krótkofalowej itd., itd. Tu rzeczywiście jest spore grono pasjonatów, które korzysta czy do dzisiaj kultywuje tego rodzaju łączność. My również o niej myślimy w trochę innym kontekście, więc niewykluczone, że pojawi się taki punkt styku.

Przewodniczący poseł Wojciech Król (KO):

Dziękuję bardzo. Myślę, że na tym wyczerpaliśmy dzisiejszy temat. Dziękuję wszystkim państwu za obecność i wzięcie udziału w posiedzeniu podkomisji, za przekazane informacje. Jeszcze raz dziękuję ministerstwu za przesłanie szczegółowych materiałów.

Zamykam posiedzenie podkomisji, dziękuję bardzo.