

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

**Komisja
Administracji
i Spraw
Wewnętrznych**

■ **PODKOMISJI STAŁEJ DO SPRAW
FUNKCJONOWANIA ZARZĄDZANIA
KRYZYSOWEGO
(NR 11)
z dnia 23 kwietnia 2025 r.**

Pełny zapis przebiegu posiedzenia Komisji Administracji i Spraw Wewnętrznych – podkomisji stałej do spraw funkcjonowania zarządzania kryzysowego (nr 11)

23 kwietnia 2025 r.

Podkomisja stała do spraw funkcjonowania zarządzania kryzysowego, obradująca pod przewodnictwem posła **Konrada Fryszta (KO)**, przewodniczącego podkomisji, zrealizowała następujący porządek dzienny:

– informacja ministra spraw wewnętrznych i administracji w sprawie organizacji systemu bezpiecznej łączności.

W posiedzeniu udział wzięli: **Krzysztof Bondaryk** pełnomocnik ministra spraw wewnętrznych i administracji do spraw organizacji Systemu Bezpečnej Łączności Państwowej, dyrektor Departamentu Bezpečczeństwa Ministerstwa Spraw Wewnętrznych i Administracji, **Dariusz Nowak-Nova** dyrektor Departamentu Teleinformatyki Ministerstwa Spraw Wewnętrznych i Administracji wraz ze współpracownikiem oraz **Monika Pieniek** zastępcą dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji wraz ze współpracownikiem.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Anna Ornat i Kamila Pawluczuk** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł **Konrad Fryszak (KO)**:

Dzień dobry. Witam państwa bardzo serdecznie. Przepraszam za kilkunastominutowe opóźnienie, ale czekaliśmy na kworum, a dzisiaj było dużo obowiązków parlamentarnych po exposé ministra Sikorskiego.

Szanowni państwo, otwieram posiedzenie podkomisji stałej do spraw funkcjonowania zarządzania kryzysowego z porządkiem dziennym: informacja ministra spraw wewnętrznych i administracji w sprawie organizacji systemu bezpiecznej łączności.

Szanowni państwo, chciałbym powitać pana generała Krzysztofa Bondaryka, pełnomocnika ministra spraw wewnętrznych i administracji do spraw organizacji Systemu Bezpečnej Łączności Państwowej, dyrektora Departamentu Bezpečczeństwa Ministerstwa Spraw Wewnętrznych i Administracji. Witam również pana Dariusza Grabarczyka, zastępcę dyrektora Departamentu Teleinformatyki Ministerstwa Spraw Wewnętrznych i Administracji oraz pana Marcina Kondratowicza, radcę w Departamencie Cyberbezpieczeństwa Ministerstwa Cyfryzacji, pana Andrzeja Krzyżanka, kierownika zespołu do spraw SKR w NASK, pana Dariusza Nowaka-Nova, dyrektora Departamentu Teleinformatyki Ministerstwa Spraw Wewnętrznych i Administracji i panią Monikę Pieniek, zastępcę dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji. Szanowni państwo, witam państwa bardzo serdecznie. Witam oczywiście posłanki i posłów przybyłych na posiedzenie podkomisji.

Na wstępie chciałbym oddać głos panu dyrektorowi generałowi Krzysztofowi Bondarykowi. Bardzo proszę, panie dyrektorze.

Pełnomocnik ministra spraw wewnętrznych i administracji do spraw organizacji Systemu Bezpečnej Łączności Państwowej, dyrektor Departamentu Bezpečczeństwa Ministerstwa Spraw Wewnętrznych i Administracji gen. **Krzysztof Bondaryk**:

Dziękuję bardzo, panie przewodniczący. Szanowni państwo, w skrócie można powiedzieć, że przez ostatnie 10 lat do roku obecnego, do 1 stycznia 2025 r., tematyka łączności państwowej, rządowej była rozproszona i Ministerstwo Spraw Wewnętrznych i Administracji, które odpowiadało kiedyś za łączność rządową, pozbywało się w tym zakresie kompetencji, uprawnień i zdolności.

Ustawodawca powziął wolę wyposażenia ministra spraw wewnętrznych w takie zadanie i opatrzył go także funkcją operatora Systemu Bezpečnej Łączności Państwowej. W ustawie

z dnia 5 grudnia ubiegłego roku został zapisany rozdział 8, w którym sformułowano System Bezpiecznej Łączności Państwowej jako ogólnopolski system, który obejmuje Ministerstwo Spraw Wewnętrznych i Administracji, organy państwowe, organy konstytucyjne oraz organy ochrony ludności w wymiarze bezpiecznej łączności państwowej.

Oprócz ustawy podstawy prawne dają nam dwa rozporządzenia. Jedno – Rady Ministrów w sprawie określenia zakresu i sposobu działania służb i pozostałych podmiotów w budowie, utrzymaniu, rozwoju SBŁP, szczegółowe warunki świadczenia usług telekomunikacyjnych w ramach SBŁP w celu zapewnienia ciągłości funkcjonowania administracji państwowej oraz ochrony ludności w czasie pokoju i obrony cywilnej w czasie wojny. Drugie – rozporządzenie Rady Ministrów w sprawie określenia sposobu korzystania z Systemu Bezpiecznej Łączności Państwowej przez użytkowników oraz minimalnych warunków technicznych i funkcjonalnych, jakie musi spełniać SBŁP oraz minimalny poziom bezpieczeństwa usług, transmisji danych, połączeń głosowych oraz wiadomości tekstowych mających na względzie konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa komunikacji oraz aktualny poziom wiedzy naukowo-technicznej.

Te dwa rozporządzenia prezesa Rady Ministrów i Rady Ministrów są w trakcie legislacji. Ich wejście w życie przewidywane jest na dzień 24 grudnia tego roku. Procedowane jest również zarządzenie prezesa Rady Ministrów w sprawie powołania pełnomocnika rządu do spraw Systemu Bezpiecznej Łączności Państwowej i określenia szczegółowego zakresu działania. To rozporządzenie jest także w trakcie legislacji. W ustawie, oczywiście oprócz Systemu Bezpiecznej Łączności Państwowej, istnieją pojęcia organizator podsystemu i system łączności. Generalnie System Bezpiecznej Łączności Państwowej staje się też częścią systemu kierowania bezpieczeństwem narodowym, ponieważ minister spraw wewnętrznych jest obarczony zadaniem dostarczenia tegoż Systemu Bezpiecznej Łączności Państwowej na rzecz systemu kierowania bezpieczeństwem narodowym, który jest określony w ustawie o obronie ojczyzny.

Jak wygląda architektura systemu zdefiniowana w ustawie? Jest jawna łączność stacjonarna, niejawna łączność stacjonarna, wielopunktowa wideokonferencja, bezpieczna radiowa łączność mobilna, w tym niejawna komórkowa, bezpieczna radiowa łączność trunkingowa i bezpieczna łączność satelitarna, w tym również niejawna. Ustawodawca określił beneficjentów systemu, można powiedzieć, że cały system administracji państwowej, naczelne organy państwowe, Wojsko Polskie, Siły Zbrojne i wszystkie organy, które są właściwe dla bezpieczeństwa państwa, ochrony porządku publicznego, ratownictwa, ochrony ludności, obrony cywilnej oraz zarządzania kryzysowego. System ma również wspomóc i działać w zakresie ostrzegania, powiadamiania, alarmowania ludności o zagrożeniach przekazywanych w ramach systemu ostrzegania, powiadamiania i alarmowania.

Organy jednostek organizacyjnych Sił Zbrojnych Rzeczypospolitej i podmioty ochrony ludności mogą korzystać z usług telekomunikacyjnych świadczonych przez operatora SBŁP w zakresie niezbędnym do zapewnienia tym podmiotom ciągłości działania. Ustawodawca określił zadania bardzo precyzyjnie i szeroko, mówiąc o ciągłości bezpieczeństwa funkcjonowania administracji państwowej, ochrony ludności i obrony cywilnej. Dlatego minister spraw wewnętrznych zarządza siecią łączności państwowej, w tym z wchodzącymi w jej skład urządzeniami, infrastrukturą telekomunikacyjną, w tym wydzielonymi bezpiecznymi sieciami teletransmisyjnym pozostającymi we właściwości ministra właściwego do spraw wewnętrznych. Minister określa te minimalne warunki techniczne, zapewnia możliwość szyfrowania komunikacji między użytkownikami i instytucjami indywidualnymi z wykorzystaniem urządzeń i narzędzi kryptograficznych certyfikowanych i dostarczanych przez ABW lub Służbę Kontrwywiadu Wojskowego, zapewnia rozliczalność użytkowników instytucjonalnych, zapewnia utrzymanie i rozwój Systemu Bezpiecznej Łączności Państwowej i zarządza bezpieczeństwem tegoż systemu.

Te funkcjonalności Systemu Bezpiecznej Łączności Państwowej mówią przede wszystkim o zapewnieniu i zbudowaniu interoperacyjności między systemami łączności, komunikacji w administracji, służbach podległych ministrowi właściwemu do spraw wewnętrznych oraz innymi wydzielonymi systemami łączności, w tym systemami pozostającymi we właściwości ministra obrony narodowej. System Bezpiecznej Łączności Państwowej ma zadanie i możliwość przekazywania informacji o zagrożeniach między elementami systemu wykrywania zagrożeń, ostrzegania, powiadamiania, alarmowania ludności oraz dostarczenia i funkcjonowania bezpiecznych kanałów łączności w sieciach telekomunikacyjnych z uwzględnieniem wszystkich segmentów w wymiarze bezpieczeństwa i niejawności.

Jak wspomniałem, beneficjentami tego systemu są konstytucyjne organy Rzeczypospolitej Polskiej, organy publicznej administracji państwowej, których zadania związane są z bezpieczeństwem państwa i ochroną ludności, Siły Zbrojne Rzeczypospolitej Polskiej oraz podmioty wykonujące na rzecz administracji rządowej zadania z zakresu ochrony ludności. Oczywiście na wniosek tych podmiotów mogą być dołączone do Systemu Bezpiecznej Łączności Państwowej.

Jeśli chodzi o przygotowanie działalności SBŁP i o tym, czym już dzisiaj dysponujemy powie pan dyrektor Nowak. Natomiast możemy tylko stwierdzić, że przygotowując się do tych zadań, minister spraw wewnętrznych i administracji powołał w MSWiA pełnomocnika do spraw SBŁP, powierzył mi tę funkcję z zadaniem zinventaryzowania zasobów, kosztów i systemów MSWiA podlegających integracji w ramach SBŁP. Oczywiście w ramach ustawy ustawodawca zobowiązał podmioty, takie jak Służby Specjalne, Straż Graniczną, Państwową Straż Pożarną, SOP, Policję oraz ministra do spraw informatyzacji, wskazane przez MON jednostki wojskowe do udzielania pomocy operatorowi. Tu chodzi o wsparcie techniczne przy realizacji jego zadań ustawowych z uwzględnieniem prac badawczo-rozwojowych dotyczących nowoczesnych systemów łączności.

Minister będzie mógł zlecać zadania podmiotom, które w ustawie mają możliwość wykonania usług i dają rękojmię zachowania tajemnicy państwowej. Oczywiście główną rolę w państwie oprócz MSWiA będzie pełnił pełnomocnik rządu do spraw Systemu Bezpiecznej Łączności Państwowej. Jego kandydaturę i zadania ustala minister spraw wewnętrznych z ministrem obrony narodowej i przedstawia premierowi do akceptacji.

Jeśli można, to pan dyrektor Nowak uzupełni stan obecny.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo proszę, panie dyrektorze. Dziękuję, panie generale.

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

Projektując SBŁP podjęto decyzję o wykorzystaniu infrastruktury telekomunikacyjnej, w tym sieci dostępnych dla organów jednostek organizacyjnych podległych ministrowi spraw wewnętrznych i administracji lub przez niego nadzorowanych. Uczyniono tak z kilku istotnych powodów. Ewidentne są oszczędności finansowe, ponieważ w przypadku identyfikacji odpowiedniej lokalizacji do instalowania stacji bazowej lub punktu dystrybucyjnego posadowienie w takim miejscu przyczyni się do znacznych oszczędności finansowych, ponieważ nie będzie trzeba komercyjnie wynajmować takiej powierzchni dla takiej lokalizacji.

Wzmocniona ochrona – wybór tych lokalizacji wiąże się z zapewnieniem wyższej ochrony, ponieważ miejsca takie znajdują się zwykle w zamkniętych obiektach, do których dostęp mają jedynie osoby uprawnione. Dostęp do zasobów – tego rodzaju lokalizacje często dysponują całodobową służbą dyżurną, która może stanowić pierwszą linię kontaktu w przypadku problemów lub awarii, umożliwiając reagowanie i naprawy. W końcu potencjał rozwoju takiej lokalizacji, współpraca różnych segmentów sieci w takich punktach przy rozwoju infrastruktury może zapewnić w sposób naturalny współdziałanie zasobów.

Opisując zadania interoperacyjności, o których wspomniał pan generał, dodam, że określając architekturę SBŁP postanowiono skoncentrować się na bezpiecznym przepływie informacji, a nie na konkretnych mediach. To jest zgodne z podejściem mówiącym o chronionym systemie dystrybucyjnym. Taki chroniony system dystrybucyjny zapewnia przesył informacji, korespondencję od punktu A, która jest źródłem, do punktu Z, do odbiorcy z wykorzystaniem różnorodnych mediów – sieci stacjonarnych, radiowych, komórkowych, satelitarnych. Tak interpretujemy zapis interoperacyjności, która jest zapisana w ustawie.

Podejście takie jest zgodne z zaleceniem odporności NATO, w szczególności z obszarem odporności nr 6, który nazywany jest odpornymi systemami łączności cywilnej. Celem takiego zakresu odporności NATO jest zapewnienie stałej dostępności i gwarantowanego dostępu do niezawodnych, bezpiecznych i solidnych usług komunikacyjnych w czasie pokoju, kryzysu i konfliktu, z uwzględnieniem potencjalnych zagrożeń, w tym cybernetycznych, fizycznych, personalnych, hybrydowych, zagrożeń spowodowanych przez człowieka lub z przyczyn naturalnych.

Jest to również spójne z unijnym podejściem do łączności o krytycznym znaczeniu. Na poziomie Unii Europejskiej od 2023 r. działa specjalna grupa do spraw łączności o krytycznym znaczeniu. Pracuje ona nad takim dużym europejskim systemem Critical Communications System. W 2024 r. Komisja Europejska podjęła decyzję o budowie takiego systemu. Minister spraw wewnętrznych i administracji również uczestniczy w tych pracach. System

Bezpiecznej Łączności Państwowej swym zakresem... To już pan generał wymieniał, jakie będą usługi.

Dzisiaj systemy, o których mówił pan generał, są systemami operacyjnymi. To znaczy one są, wymagają modyfikacji, integracji i rozwoju. Nie są to systemy, które powinny powstawać od zera. Infrastruktura techniczna będąca podstawą SBŁP jest cały czas infrastrukturą pozostającą w gestii resortu spraw wewnętrznych i administracji. Bazą do funkcjonowania będzie infrastruktura sieci teletransmisyjnej GovNet. To jest sieć, która była projektowana jako bezpieczne medium transmisyjne, odseparowane od internetu. Jest to wydzielona sieć. W tej chwili łączy ministerstwa, urzędy centralne i wojewódzkie. Mamy w sumie 345 powiatów, czyli tą bezpieczną siecią schodzimy do wszystkich powiatów. W tej chwili pracujemy nad rozwojem, nad rozbudową tej sieci do szpitali resortowych, do szpitali podległych ministrowi spraw wewnętrznych i administracji. W drugiej połowie roku będziemy także na wszystkich lotniskach, na części lotnisk już jesteśmy. Na przyszły rok mamy zaplanowane kupno urządzeń, które umożliwią nam uruchomienie 2800 punktów gminnych. Zakładamy, że na poziomie gmin będziemy mieli...

Jesteśmy też po rozmowach z Ministerstwem Obrony Narodowej. Ministerstwo Obrony Narodowej dysponuje swoją siecią IP RON. Pracujemy wspólnie nad integracją tych sieci i mamy zapewnienie, że z GovNet będziemy mogli wejść również do wszystkich jednostek, czyli w przyszłym roku sieć GovNet będzie praktycznie na terenie każdej gminy. Na poziomie GovNet uruchamiamy bardzo nowoczesną technologię MPLS, która umożliwia budowanie wirtualnych kanałów po to, żeby przysyłać informacje w sposób bezpieczny, szyfrowanych od punktu A do punktu Z. W ramach tej sieci działają również połączenia Polski z Unią Europejską. Na bazie sieci szkieletowej GovNet funkcjonuje sieć TESTA. Komunikują się z nią dzisiaj wszystkie służby odpowiedzialne za ochronę granic i bezpieczeństwo publiczne. Komisja Europejska chce również uruchomić ponad 700 punktów dostępowych do swojego wspólnego systemu wymiany informacji. Jesteśmy już na to przygotowani i od przyszłego roku zaczniemy to rozwijać.

Z uwagi na to, że te sieci pełnią coraz większą rolę i przysyłają informacje również w obszarze zarządzania kryzysowego, planujemy uruchomienie takich specjalnych zespołów zajmujących się ochroną cyberbezpieczeństwa tej sieci oraz ich awaryjnością. Planujemy zbudowanie resortowego SOC – System Operations Center, które będzie od strony centralnej opiekowało się SBŁP, ale również chcemy stworzyć 16 wojewódzkich tak, żeby takie zespoły specjalistów również były dostępne na poziomie wojewódzkim.

Na poziomie GovNet działa sieć łączności rządowej. Jest to element infrastruktury krytycznej i jest wykorzystywana do zapewnienia łączności specjalnej między najważniejszymi osobami w państwie. Jest ona m.in. w KPRM, w Kancelarii Prezydenta, w Kancelarii Sejmu, Senatu, w ministerstwach, urzędach oraz organach administracji rządowej wykonujących zadania z zakresu ochrony, bezpieczeństwa i porządku publicznego, ochrony granic, sądownictwie i prokuraturze. Tę sieć będziemy rozwijali o komponenty video i unowocześniali te technologie video tak, żeby na poziomie wszystkich wojewódzkich centrów zarządzania kryzysowego możliwa była bezpieczna transmisja video. To są również działania, które mamy zaplanowane na przyszły rok. Modernizacje sieci i podnoszenie technologii z tej takiej zastalej, która od wielu lat była niemodernizowana, realizujemy teraz na bieżąco, nie czekając na zakończenie finalnych prac dotyczących projektowania CBŁP, bo tak jak mówiłem, ideą jest wykorzystywanie zasobów, które już państwo polskie posiada. Nie chodzi o to, żeby budować coś od sera, trzeba mądrze wykorzystać to, co mamy.

Osobnym tematem jest system łączności radiowej budowany w oparciu o standard TETRA. Po raporcie NIK minister spraw wewnętrznych i administracji powołał zespół złożony ze służb resortu, który ma opracować sposób rozbudowy tego systemu i funkcjonowania w ramach SBŁP. W przyszłym tygodniu w poniedziałek ma zostać przyjęty raport końcowy. Raport będzie niejawnym, więc już więcej na ten temat nie będę się wypowiadał.

Kolejnym takim segmentem, który będzie bardzo intensywnie eksploatowany w ramach SBŁP, będzie łączność satelitarna. Tutaj dzisiaj dla nikogo nie jest tajemnicą, że taka łączność może być organizowana ad hoc w różnych miejscach i doskonale spełnia ona swoją funkcję transportową. Problemem może być własność terminali. Unia Europejska pracuje nad systemem europejskiej łączności satelitarnej. Realizuje to w ramach inicjatywy GOVSATCOM. Polskę w ramach GOVSATCOM reprezentuje minister spraw wewnętrznych, jest on krajowym CGA, czyli Competent GOVSATCOM Authority i również jako ministerstwo uczestniczymy

w programie Secure Connectivity. To jest oczywiście też wspólne i uzupełnia się z inicjatywą DG HOME tego unijnego systemu komunikacji kryzysowej.

Jeśli chodzi o GOVSATCOM stan gry jest w tej chwili taki, że niesłuchanie przyspieszyły prace nad europejskimi systemami satelitarnymi. Inicjatywa GOVSATCOM zakłada, że w drugiej połowie roku będzie już można korzystać z takiej sieci przez państwa uczestniczące. W drugiej połowie maja ma się zakończyć przetarg na takie usługi. Po zakończeniu przetargu zostaną określone usługi i wtedy zostaną przydzielone państwom uczestniczącym w tej inicjatywie odpowiednie zasoby. Jako Polska w tym uczestniczymy od długiego czasu, więc też w sposób naturalny będziemy mieli dostęp do bezpiecznej łączności satelitarnej, której nie będziemy musieli kupować od podmiotów komercyjnych.

Mógłbym jeszcze powiedzieć, jakie mamy zaplanowane działania w ramach programu ochrony ludności i obrony cywilnej, ale to już jest opisane w programie, więc tam mogą państwo sięgnąć do źródła i przeczytać, co będzie realizowane, łącznie z budżetami. Dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Zatem przechodzimy do... Chyba, że państwo z Ministerstwa Cyfryzacji chcą coś dodać. Nie? Dziękuję. Zatem przechodzimy do pytań parlamentarzystek, parlamentarzystów, do pań posłanek i panów posłów. Czy są pytania? Bardzo proszę, pan poseł Ściebiorowski.

Poseł Łukasz Ściebiorowski (KO):

Dziękuję. Panie przewodniczący, szanowni państwo, mam pytanie, bo tych systemów jest dość dużo. Widzę, że pan wymieniał różne i te analogowe, jak dobrze domniemam, nie jestem tutaj specjalistą od cyfryzacji, ale tak to odebrałem, i te cyfrowe. Na ile one są też ze sobą kompatybilne, czyli współpracują w różnych sytuacjach zagrożenia? To jest jedno pytanie.

Drugie, czy ministerstwo ma bazę, ewentualnie lokalnie korzysta z informacji w różnych powiatowych centrach zarządzania kryzysowego odnośnie do krótkofalowców, bo często to są pasjonaci w różnych strukturach. Na przykład na moim przykładzie wiem, że w Piekarach Śląskich na przykład jest harcerstwo, ci pasjonaci w harcerstwie działają też na różnych obozach, gdzie uczą tych młodszych zasad krótkofalowców. Czy te systemy, takie typowo jeszcze analogowe, też są wykorzystywane? Bo gdy zawiodą te cyfrowe, nie daj Boże, gdyby miał się odbyć atak to pewnie na te cyfrowe pójdzie pierwszy i na ile można wykorzystać wtedy właśnie zasoby krótkofalowców, pasjonatów? Czy jest to robione? Czy jest taka baza, czy państwo w ogóle wiecie, macie rozeznanie, ilu ich jest w Polsce, w jakich klubach są zrzeszeni i gdzie można do nich szybko dotrzeć w razie potrzeby i ewentualnie ich wykorzystać? Dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Dziękuję. Pan dyrektor odpowie? Bardzo proszę.

Dyrektor departamentu MSWiA Dariusz Nowak-Nova:

Tak. Jeśli chodzi o pierwsze pytanie to, że mamy dużo systemów w Polsce i to, że one są niekompatybilne i ze sobą nie rozmawiają, to już wielokrotnie znajdowało swoje odzwierciedlenie w raportach NIK. Najwyższa Izba Kontroli wprost pisała, że jako Polska nie mamy takiego systemu i różne służby wykorzystują różne systemy. Żeby temu przeciwdziałać zaczęliśmy właśnie pracować nad Systemem Bezpiecznej Łączności Państwowej, który został opisany jako forma organizacyjna, a nie technologiczna. Jednym z pierwszych wyzwań jest zbudowanie interfejsów między systemami po to, żeby nie miało znaczenia, po jakim medium komunikat przesyłany jest, tylko żeby on przechodził. Odpowiadając krótko – jesteśmy przed wyzwaniem zbudowania interfejsów, ale to się już dzieje i mamy też takie bardzo konkretne plany, a częściowo już mamy takie rozwiązania, które są rozwiązaniami wielosystemowymi.

Natomiast, jeśli chodzi o ten element fal krótkich, to mamy taki komponent również wpisany w SBŁP i może na tym poprzestaną.

Dyrektor departamentu MSWiA gen. Krzysztof Bondaryk:

Możemy tylko dodać, panie przewodniczący, panie pośle, że temat krótkofalowy czy krótkich fal jest w naszym zainteresowaniu. Nie jest to tylko kwestia jawnej komunikacji. Natomiast oczywiście te rejestry ma Urząd Komunikacji Elektronicznej, tych indywidualnie działających w tym obszarze, bo muszą mieć identyfikację i rejestrację.

Co do tematu fal krótkich, zawsze uważałem to za pożądany element rozwoju i myśląc o zapasowej łączności szeroko rozumianej, żebyśmy nie wchodzili w szczegóły, ten element jest rozważany.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Jakies dodatkowe pytania? Pan przewodniczący? Bardzo proszę, pan przewodniczący Lachowicz.

Poseł Piotr Lachowicz (KO):

Panie dyrektorze, w ramach tworzonego Systemu Bezpiecznej Łączności Państwowej pan słusznie podkreślił, że skupiacie się na formie organizacyjnej, a nie technologicznej. Natomiast, jeśli chodzi o technologie, to rozumiem, że poszczególne technologie, bo to nie musi być jedna czy nawet nie będzie, rozumiem, że będą stosowne przetargi. Wiemy, że takie technologie współcześnie tworzy na przykład Motorola. Pan zresztą lepiej się orientuje, jakie firmy się zajmują właśnie takimi systemami wielozakresowymi. To będzie podlegało normalnym komercyjnym przetargom czy będziemy starali się to robić też własnymi siłami tylko i wyłącznie? Jeśli to pytanie nie wykracza poza ochronę informacji niejawnych oczywiście, bo jak tak, to je cofam.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo proszę, pan dyrektor.

Dyrektor departamentu MSWiA Dariusz Nowak-Nova:

Panie przewodniczący, firma, której nazwę pan wymienił, jest dostawcą urządzeń, a nie technologii, ta technologia jest oparta na standardzie. Jesteśmy zwolennikami kupowania w postępowaniach przetargowych na zasadach absolutnie konkurencyjnych rozwiązań. Nie wyklucza to tego, że takie postępowania konkurencyjne są realizowane dla kilku podmiotów, które mają odpowiednie poświadczenia bezpieczeństwa. Będziemy kupowali i tak, i tak.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Zatem ja mam jeszcze kilka pytań. Szanowni państwo, pamiętacie doskonale, mówiliśmy o tym, rozmawialiśmy krótko przed rozpoczęciem posiedzenia o ubiegłorocznej powodzi, która nawiedziła południową część naszego kraju. Pamiętam jedno z wystąpień, gdzie skarżono się na brak komunikacji, na brak łączności. Nie pamiętam dokładnie. Może pani posłanka Czernow wsparłaby mnie wiedzą, w którym dokładnie to było miejscu, ale to chyba chodziło o tamę, która pękła. Był brak przekazu informacji, bo zerwana została wszelka łączność. W związku z tym mam pytanie, oczywiście trochę odpływając od ochrony cywilnej, obrony ludności, a łącząc tę kwestię Systemu Bezpiecznej Łączności Państwowej na czas „P”, czyli na czas pokoju, mówiąc wprost – zarządzania kryzysowego. Czy ta budowana bezpieczna łączność będzie pozwalała, oczywiście z wyłączeniem jawności prowadzonej korespondencji, na to, by ją wykorzystywać, uwzględnić jej funkcjonowanie w warunkach awarii technicznych, w tym braku zasilania w energię elektryczną i braku sygnału internetowego ze źródeł powszechnie dostępnych? To pierwsze.

Drugie, czy budowana bezpieczna łączność obejmuje integrację z istniejącymi sieciami łączności, na przykład z sieciami radiowymi pozostającymi w dyspozycji wojewodów?

Trzecie, czy w sieć bezpiecznej łączności zostaną włączone jednostki samorządu terytorialnego? Mam na myśli przede wszystkim centra zarządzania kryzysowego stanowiące pierwszy element reagowania w przypadku sytuacji kryzysowej. To są moje pytania.

Pan dyrektor, bardzo proszę.

Dyrektor departamentu MSWiA gen. Krzysztof Bondaryk:

Od końca. Oczywiście podmioty i organy ochrony ludności będą ujęte w sieci SBŁP. Natomiast podmioty ochrony ludności na wniosek tych podmiotów mogą być ujęte przez operatora w tym systemie.

Co do centrów powiatowych zarządzania kryzysowego – system ochrony ludności opiera się de facto o Państwową Straż Pożarną, która ma strukturę państwowej formacji mundurowej oraz na Krajowym Systemie Ratowniczo-Gaśniczym, czyli mamy ochotniczo kolejne tysiące osób. Oczywiście OSP, która nie jest KSRG, jest kolejnym etapem siły żywej, także strażnice OSP – tych organizacji w Polsce jest ok. 16 tys. – i są one takim elementem podstawowym do doposażenia i do działania ochrony ludności. Temat łączności tych instytucji będzie także przedmiotem rozwoju i pracy SBŁP. Natomiast chcemy zacząć od integracji resortu i instytucji państwowych

na początku, z rozwojem dostępności na poziomie gmin, bezpiecznej, wydzielonej łączności transportowej, transmisyjnej GovNet. Poszczególne urządzenia czy rozwiązania będą dostosowane i do możliwości finansowych, i do tego stanu, który jest dzisiaj, ponieważ chcemy wykorzystać, o ile to jest możliwe, infrastrukturę, także państwową, a także podmioty państwowe czy spółki Skarbu Państwa, które mogą nam udostępnić pewnego rodzaju możliwości, jeśli chodzi o sieć, czy to sieć światłowodową, czy to sieć radiową.

W Polsce jest bardzo dużo światłowodów, bardzo dużo masztów, duża ich część jest także w podmiotach, gdzie Skarb Państwa ma znaczące udziały, na przykład energetyka. Płynnie więc moglibyśmy przejść do drugiego pytania – odporność takiej sieci komunikacyjnej a brak prądu. Jeżeli patrzymy na sieci energetyczne, wieże transmisyjne, BTS, światłowody, których odporność na brak prądu jest różna u różnych operatorów i ten standard jest u operatorów komercyjnych, to BTS bez zasilania może działać 4 godziny, ważniejsze – 24 godziny, 48 godzin i 72 godziny. Niektóre firmy energetyczne posiadają te standardy, więc pytanie czy ich wieże transmisyjne wszystkie mają mieć standard do 48 godzin czy 72 godzin i wykorzystanie tej infrastruktury daje nam z automatu takie zdolności. Czy musimy budować doraźne kwestie to jest kwestia do rozstrzygnięcia. Jeżeli się uda zintegrować zasoby także państwowych spółek energetycznych i innych posiadających sieci teletransmisyjne i zasoby teleinformatyczne, to budowa takiej zdolności, o którą pan przewodniczący pyta, mogłaby być szybsza i skończona w ciągu 2 lat, także mniejszym kosztem oczywiście, bo ta integracja pozwala według naszej oceny zmniejszyć wydatki co najmniej o jedną czwartą dotychczasowych rozmiarów.

Tam było jeszcze jedno pytanie?

Dyrektor departamentu MSWiA Dariusz Nowak-Nova:

Tak, jeszcze jedno pytanie – brak łączności w trakcie powodzi i brak możliwości poinformowania o nawale wody, który uszkodził tamę. Tu chyba o ten kontekst chodziło. Z informacji, które były w mediach wiemy, że rzeczywiście nie było łączności komórkowej, ponieważ w BTS zabrakło prądu i nie działały już agregaty. Natomiast służby, które działały w terenie dysponowały łącznością, taką stałą bieżącą, którą mają. Oprócz tego były instalowane takie moduły łączności satelitarnej. Natomiast problemem być może było to, że takie miejsca, jak zapory, które ewidentnie są obiektami infrastruktury krytycznej, nie miały połączenia GovNet. Gdyby był GovNet, to zaręczam panu przewodniczącemu, że odpowiedni komunikat byłby w stanie dotrzeć do odpowiednich osób i zrobimy wszystko, żeby do tego doprowadzić, żeby skomunikować takie miejsca i nie dopuścić do takich sytuacji, w których jesteśmy uzależnieni tylko od LTE, GSM i jak tego nie ma, to nie ma nic.

Przewodniczący poseł Konrad Fryszak (KO):

Reasumując, żeby to wybrzmiało i zostało zaprotokołowane – pan dyrektor, panowie dyrektorzy chcecie zrobić wszystko, żeby System Bezpiecznej Łączności Państwowej mógł być użytkowany nie tylko w sytuacji „W”, ale również w sytuacji pokoju przez zarządzanie kryzysowe, żeby był kompatybilny i mógł być wykorzystywany. Można tak zerojedynkowo to uprościć?

Dyrektor departamentu MSWiA gen. Krzysztof Bondaryk:

Jeżeli nie będzie działać w czasie pokoju, to nie będzie działać w czasie wojny.

Przewodniczący poseł Konrad Fryszak (KO):

To oczywiście. To już logika. OK, ale będziemy mogli go wykorzystywać w sytuacji zarządzania kryzysowego, takich zdarzeń, które były dotychczas i które mamy nadzieję, że tylko takie nasz kraj mogą dotykać. Dziękuję.

Dyrektor departamentu MSWiA Dariusz Nowak-Nova:

Tak. Tak jest on opisany w ustawie, bo to jest system do zarządzania na czasy kryzysu.

Przewodniczący poseł Konrad Fryszak (KO):

Tak, tak. Super. Szanowni państwo, czy są jeszcze jakieś pytania? Nie widzę. Nie słyszę. Zatem dziękuję wszystkim państwu za obecność i zamykam posiedzenie podkomisji.