

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

**Komisja
Administracji
i Spraw
Wewnętrznych**

■ **PODKOMISJI STAŁEJ DO SPRAW
FUNKCJONOWANIA ZARZĄDZANIA
KRYZYSOWEGO
(NR 3)
z dnia 25 kwietnia 2024 r.**

Pełny zapis przebiegu posiedzenia

Komisji Administracji i Spraw Wewnętrznych

– podkomisji stałej do spraw funkcjonowania zarządzania kryzysowego (nr 3)

25 kwietnia 2024 r.

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

– informacja na temat wyznaczenia i ochrony infrastruktury krytycznej, wzmocnienia odporności kluczowych elementów zabezpieczenia przed efektem kaskadowym, w szczególności w sektorze energetyki i transportu.

W posiedzeniu udział wzięli: **Maciej Bando** podsekretarz stanu w Ministerstwie Klimatu i Środowiska wraz ze współpracownikami, **Bartosz Pelk** zastępca dyrektora Departamentu Zarządzania Kryzysowego i Bezpieczeństwa Ministerstwa Aktywów Państwowych, **Zbigniew Kręcis** dyrektor Biura Zarządzania Kryzysowego w Ministerstwie Infrastruktury, **Marcin Wysocki** zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji, **Dariusz Marczyński** dyrektor Departamentu Ochrony Ludności i Zarządzania Kryzysowego Ministerstwa Spraw Wewnętrznych i Administracji, **Józef Galica** zastępca komendanta głównego Państwowej Straży Pożarnej, **Jakub Mierzejewski** zastępca dyrektora Głównego Sztabu Policji w Komendzie Głównej Policji, **Piotr Stasiak** zastępca komendanta Centralnego Biura Śledczego Policji, **Zbigniew Muszyński** dyrektor Rządowego Centrum Bezpieczeństwa wraz ze współpracownikami, **Jacek Wysokiński** zastępca dyrektora Zarządu Granicznego w Komendzie Głównej Straży Granicznej, **Jerzy Płókarz** prezes Krajowego Sztabu Ratownictwa Społecznej Sieci Ratunkowej.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Andrzej Kniaziewicz**, **Anna Ornat** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

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

Dzień dobry. Witam państwa bardzo serdecznie na posiedzeniu podkomisji stałej do spraw funkcjonowania zarządzania kryzysowego. Jest punktualnie godzina 17.00. Witam bardzo serdecznie zaproszonych gości. Pozwólcie państwo, że przeczytam dzisiaj bardzo szeroki skład. Jesteśmy zaszczycony obecnością państwa. Witam pana podsekretarza stanu w Ministerstwie Klimatu i Środowiska, pełnomocnika rządu do spraw strategicznej infrastruktury energetycznej pana Macieja Bando, panią dyrektor Departamentu Elektroenergetyki i Gazu w Ministerstwie Klimatu i Środowiska Aleksandrę Świdorską, pana Ireneusza Panka zastępcę dyrektora Departamentu do Spraw Obronnych, Zarządzania Kryzysowego i Bezpieczeństwa w Ministerstwie Klimatu i Środowiska, panią Izabelę Walczak naczelnik Wydziału Zarządzania Kryzysowego w Departamencie Spraw Obronnych, Zarządzania Kryzysowego i Bezpieczeństwa w Ministerstwie Klimatu i Środowiska. Witam pana ministra Roberta Kropiwnickiego, którego nie widzę, pana Bartosza Pelka dyrektora Departamentu Zarządzania Kryzysowego w Ministerstwie Aktywów Państwowych, pana dyrektora Zbigniewa Kręcisa dyrektora Biura Zarządzania Kryzysowego w Ministerstwie Infrastruktury, naczelnika Wydziału Zarządzania Kryzysowego w Ministerstwie Infrastruktury pana Wojciecha Gajkowskiego. Witam pana Marcina Wysockiego zastępcę dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, pana Marcina Kondratowicza radcę w Wydziale

Funkcjonowania Krajowego Systemu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, pana Andrzeja Sowińskiego doradcę ekonomicznego w Departamencie Gospodarki, Skarbu Państwa i Prywatyzacji Najwyższej Izby Kontroli, pana Dominika Zimnego doradcę technicznego w Departamencie Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli, pana Pawła Kostkiewicza dyrektora do spraw certyfikacji w Naukowej i Akademickiej Sieci Komputerowej. Witam dyrektora Departamentu Ochrony Ludności i Zarządzania Kryzysowego w Ministerstwie Spraw Wewnętrznych i Administracji pana Dariusza Marczyńskiego. Witam pana Józefa Galicę zastępcę Komendanta Głównego Państwowej Straży Pożarnej, dzień dobry panie generale. Witam pana Mariusza Lenartowicza dyrektora Biura Ochrony Ludności w Komendzie Głównej Państwowej Straży Pożarnej. Witam pana Marka Wnęka naczelnika wydziału w Komendzie Głównej Państwowej Straży Pożarnej. Witam zastępcę dyrektora Głównego Sztabu Policji w Komendzie Głównej Policji pana Jakuba Mierzejewskiego. Witam naczelnika Wydziału Zarządzania Kryzysowego i Przygotowań Obronnych Policji w Komendzie Głównej Policji pana Przemysława Stachurę. Witam pana Piotra Stasiaka zastępcę komendanta Centralnego Biura Śledczego Policji. Witam pana Przemysława Majewskiego naczelnika Wydziału do Spraw Zwalczenia Aktów Terroru w Centralnym Biurze Śledczym Policji. Witam pana Zbigniewa Muszyńskiego dyrektora Rządowego Centrum Bezpieczeństwa. Witam pana Witolda Skomrę doradcę w Rządowym Centrum Bezpieczeństwa. Witam pana Jacka Wysokińskiego zastępcę dyrektora Zarządu Granicznego w Komendzie Głównej Straży Granicznej i pana Jerzego Płókarza prezesa Krajowego Sztabu Ratownictwa Społecznej Sieci Ratunkowej.

Po przywitaniu, szanowni państwo, porządek dzienny dzisiejszego posiedzenia, czyli „Informacja na temat wyznaczenia i ochrony infrastruktury krytycznej, wzmacniania odporności kluczowych elementów zabezpieczenia przed efektem kaskadowym, w szczególności w sektorze energetyki i transportu”.

Szanowni państwo, sytuacja za naszą wschodnią granicą oraz wojna hybrydowa nakazuje nam zająć się również sprawą odporności w strategicznych gałęziach naszego kraju. Stąd ten dzisiejszy punkt. Bardzo bym prosił państwa o przedstawienie, w jaki sposób jesteście przygotowani na takie akty destabilizacji. Oczywiście wiemy, że tym zajmuje się bezpośrednio Straż Pożarna. Czy pan generał zechce na początek zabrać głos? Czy ktoś z państwa ma jakąś inną propozycję? W takim razie, które ministerstwo jako pierwsze?

Zastępca dyrektora Departamentu Zarządzania Kryzysowego Ministerstwa Aktywów Państwowych Bartosz Pelk:

Dzień dobry. Bartosz Pelk, Ministerstwo Aktywów Państwowych. Może my zaczniemy. Jeśli chodzi o ministra aktywów państwowych, to minister aktywów państwowych jest umiejscowiony w dwóch sektorach infrastruktury krytycznej. Po pierwsze, oczywiście sektor energii surowców energetycznych i paliw. Tutaj jesteśmy współodpowiedzialni za ten sektor z ministrem klimatu i środowiska. Drugi sektor, to jest sektor łączności. Tutaj mamy współodpowiedzialność z ministrem cyfryzacji, ale tak naprawdę w zakresie łączności minister aktywów państwowych zajmuje się głównie sprawami infrastruktury krytycznej w Poczcie Polskiej SA.

Jeśli chodzi o ministra aktywów państwowych, to jest to jedyny minister nadzorujący infrastrukturę krytyczną, który posiada szczególne uprawnienia w odniesieniu do tej infrastruktury krytycznej, które określa ustawa o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych i grupach kapitałowych, które prowadzą działalność w sektorach energii elektrycznej, ropy naftowej i paliw gazowych. W każdym z tych trzech sektorów, w porozumieniu dyrektorów i Rządowego Centrum Bezpieczeństwa, już kilka lat temu została wytypowana infrastruktura krytyczna i tak naprawdę w ramach tych sektorów mamy 12 spółek sektora energii elektrycznej, 12 sektora ropy naftowej i 6 spółek sektora paliw gazowych. Są to między innymi takie spółki jak Orlen, jeśli chodzi o paliwa, Polskie Sieci Elektroenergetycznej, jeśli chodzi o przesył energii, Polskie Górnictwo Naftowe i Gazownictwo, które jest teraz w Grupie Orlen, Gaz-System, który odpowiada za przesył paliw. Tych spółek jest dużo i są to spółki kluczowe dla funkcjonowania gospo-

darki. Minister posiada takie uprawnienia, że w tych spółkach, wspólnie z dyrektorem Rządowego Centrum Bezpieczeństwa, opiniuje kandydatów na pełnomocników do spraw ochrony infrastruktury krytycznej, którzy po uzyskaniu pozytywnej opinii są powoływani przez zarządy. Taki pełnomocnik do spraw ochrony infrastruktury krytycznej jest łącznikiem dla ministra aktywów państwowych, dla ministra klimatu i środowiska, dla dyrektora Rządowego Centrum Bezpieczeństwa i dla innych podmiotów, które agregują zadania w zakresie zarządzania kryzysowego. On jest człowiekiem, który czuwa nad infrastrukturą krytyczną i co kwartał przekazuje raporty o stanie ochrony infrastruktury krytycznej oraz sprawozdania do tych wszystkich podmiotów. Każdy raport musi się odnosić do tak zwanego sześciopaku bezpieczeństwa, czyli do kwestii związanych z ochroną fizyczną, teleinformatyczną, prawną, osobową itd, infrastruktury krytycznej.

Ponadto szczególne uprawnienia ministra polegają na tym, że pełnomocnik przekazuje ministrowi wszystkie uchwały organów spółki, czy to jest rada nadzorcza, zarząd bądź walne zgromadzenie, które w jakikolwiek sposób odnoszą się do mienia infrastruktury krytycznej. Minister ma prawo zgłosić sprzeciw do uchwały, która według niego będzie zagrażała ciągłości działania integralności i funkcjonowaniu infrastruktury krytycznej. To jest takie zabezpieczenie prawne, które pozwala nam czuwać nad tym, żeby ta infrastruktura krytyczna nie była sprzedawana bez naszego nadzoru, czy jakiejś jej mienie nie było zaniechane, albo ktoś się wycofał z jego funkcjonowania itd. To realizujemy tak naprawdę od 2010 r. Już wcześniej realizował to minister właściwy do spraw energii i minister skarbu państwa.

Oczywiście jako minister aktywów państwowych jeszcze opiniujemy plany ochrony infrastruktury krytycznej tych wszystkich spółek z tych trzech sektorów. To opiniowanie też się odbywa we współpracy z ministrem klimatu i Rządowym Centrum Bezpieczeństwa.

Jeśli chodzi jeszcze o jeden mechanizm, który jest powiązany z infrastrukturą krytyczną, to minister jest tzw. organem kontroli, zgodnie z ustawą o kontroli niektórych inwestycji. Tutaj minister może zablokować poprzez zgłoszenie decyzji sprzeciwu o nabywanie dominacji w spółkach, które też prowadzą działalność szeroko rozumianych sektorach energii elektrycznej, ropy naftowej, paliw gazowych i też innych. Tutaj przy każdorazowym nabyciu w spółce, która jest wyszczególniona w rozporządzeniu, które się wydaje na podstawie ustawy o kontroli – bo mamy tzw. rozporządzenie w sprawie podmiotów podlegających szczególnej ochronie – każdy kto chciałby nabyć to czy to z krajowych podmiotów dominację, to jest tzw. przekroczenie albo 25%, 30% bądź 33% akcji w spółce, bądź też sprzedać zorganizowaną część przedsiębiorstwa, musi przyjść do ministra aktywów państwowych, żeby uzyskać zgodę na tego typu transakcję. Tego typu transakcje są rozpatrywane. Teraz ostatnia jest rozpatrywana kwestia nabywania dominacji w spółce Oil Petrol, która też niedawno znalazła się na wykazie infrastruktury krytycznej. To jest też taki mechanizm, który pozwala nam czuwać i mieć w pieczę nad tym, co się dzieje z tym mieniem.

Ponadto, jako organ kontroli, dostajemy też informacje z całej Unii Europejskiej od wszystkich państw członkowskich na temat tego, jakie podobne nabycia dominacji dzieją się na obszarze ich kraju i też dostajemy do opiniowania pod kątem, w jakiś sposób wpływa to na bezpieczeństwo i porządek publiczny w Polsce.

Odnosząc się już tak bardziej stricte do tematu naszego posiedzenia, mówiąc o zagrożeniach, kaskadowości i pozostałych kwestii, to tak naprawdę tutaj głównie zadania są realizowane poprzez zarządy spółek, które wdrażają różnego rodzaju zabezpieczenia fizyczne czy też inne. Teraz na przykład w planie inwestycyjnym PERN jest przeliczana inwestycja w zakresie stworzenia zabezpieczenia antydronowego docelowo w ciągu 3 lat na wszystkich jedenastu bazach paliw. Tak naprawdę spółki podejmują szereg działań w zakresie zabezpieczenia tych obiektów i minister poprzez te swoje uprawnienia współpracy z pełnomocnikami, ze służbami specjalnymi...

Podsekretarz stanu w Ministerstwie Klimatu i Środowiska, pełnomocnik rządu do spraw strategicznej infrastruktury energetycznej Maciej Bando:

Przepraszam bardzo, panie dyrektorze. Maciej Bando, pełnomocnik rządu do spraw strategicznej infrastruktury energetycznej. Chciałem wszystkim uczestnikom przypomnieć, że sam wykaz infrastruktury krytycznej nie jest dokumentem jawnym, jak również udostępnianie informacji na temat prac prowadzonych przez poszczególne spółki nie powinno być omawiane w takim trybie. Proszę mi wybaczyć panie dyrektorze, ale ponieważ mówi pan akurat o spółkach, które nadzoruję, więc pozwoliłem sobie wkroczyć. Mówmy o prawie, które jest publicznie znane i dostępne, nie wnikając w szczegóły. Dziękuję.

Zastępca dyrektora departamentu MAP Bartosz Pelk:

Ten materiał, który przywoływałem, jest materiałem jawnym, bo jest to uchwała walnego zgromadzenia...Wiem, wiem, ale to jest informacja. Chciałem tylko powiedzieć, że taki projekt jest. Te działania są tutaj realizowane poprzez zarządy i ministerstwo we współpracy z agencjami, ministerstwami. Myślę, że to tyle, jeśli chodzi o kwestie, jak ta infrastruktura krytyczna jest zorganizowana w zakresie Ministerstwa Aktywów Państwowych. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję panie dyrektorze i oczywiście dziękuję panu ministrowi za tę uwagę. Oczywiście mamy świadomość tego, że niektóre informacje, które mogłyby być przekazywane są opatrzone klauzulą i takich informacji w tym trybie posiedzenia podkomisji nie oczekujemy od państwa. Gdyby takie informacje ktoś z państwa chciał przekazywać, to zwracam uwagę na fakt, że posiedzenie podkomisji jest również transmitowane za pośrednictwem internetu i jest ogólnodostępne. Gdy będziemy potrzebowali informacji, które są opatrzone klauzulą, będziemy zwracać się o zwołanie posiedzenia w trybie niejawnym, ale to nie dzisiaj. Dzisiaj porozmawiamy o tym, czy jesteśmy co do zasady przygotowani, czy są wyznaczone, czy gdzieś ewentualnie są potrzeby doprecyzowania legislacyjnego ze strony Sejmu, doszczegółowienia procedur. Bardzo dziękuję, panie dyrektorze.

Kto z państwa zabierze kolejny głos? Skoro już mamy Ministerstwo Aktywów Państwowych, to może wywołamy kolejne ministerstwo? Bardzo proszę.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji Marcin Wysocki:

Panie przewodniczący, Wysoka Komisjo, szanowni państwo, Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji. Ja może krótko w takim samym duchu, jak mój przedmówca, na temat zadań ministra cyfryzacji. Minister cyfryzacji odpowiada z kolei za trzy systemy infrastruktury krytycznej: za łączność (wspólnie z ministrem aktywów państwowych), za sieci teleinformatyczne i za systemy zapewniające ciągłość działania administracji publicznej. Zgodnie z Narodowym Programem Ochrony Infrastruktury Krytycznej oczywiście wszyscy ministrowie mają udział między innymi w procesie oceny ryzyka występującego w sytuacji kryzysowej w państwie wywołanej zakłóceniem funkcjonowania systemu infrastruktury krytycznej oraz wykonywaniu zadań określonych w ustawie o zarządzaniu kryzysowym. Wśród głównych zadań ministra cyfryzacji jest oczywiście utrzymywanie kontaktu z operatorami infrastruktury krytycznej tychże systemów, analiza i uzgadnianie planów ochrony infrastruktury krytycznej, analiza wniosków o wpisanie lub wykreślenie z wykazu infrastruktury krytycznej we współpracy z operatorem i Rządowym Centrum Bezpieczeństwa. Mamy tu również taką naszą inicjatywę – coroczne Forum Ochrony Infrastruktury Krytycznej. Ostatnie takie forum odbyło się 29 września zeszłego roku. Oczywiście tematem przewodnim były zagadnienia aktualne dla systemów, które są w opiece ministra cyfryzacji. Byli ważni przedstawiciele administracji publicznej, prelegenci, przedstawiciele świata nauki, administracji, Komendy Głównej Policji, Rządowego Centrum Bezpieczeństwa, polityki poznańskiej. Ostatnie forum było poświęcone zagrożeniu stworzonym przez systemy bezzałogowe oraz zagadnieniom związanym z zabezpieczeniem fizycznym obiektów infrastruktury krytycznej.

Mam też swoje przemyślenia. Pytanie jest, czy również opowiedzieć o tym co się zmieni w zarządzaniu kryzysowym w kontekście cyberbezpieczeństwa, panie przewodniczący? Dobrze. Wczoraj rozpoczęły się konsultacje publiczne, uzgodnienia, opiniowanie ustawy wdrażającej dyrektywę NIS2 poświęconej zwiększeniu cyberbezpieczeństwa na poziomie unijnym. Wśród tych instytucji prawnych, które przewiduje dyrektywa, jest również obowiązek po stronie kraju członkowskiego przyjęcia planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym to planie powinno się określić cele, tryby zarządzania incydentami, zarządzania kryzysowego właśnie w przypadku wystąpienia takich incydentów. Dlatego zaproponowaliśmy – projekt jest obecnie w toku uzgodnień wprowadzenia krajowego planu jako dokumentu strategicznego, który określi rolę organu, środków, procedur – w przypadku wystąpienia sytuacji kryzysowej związanej z cyberbezpieczeństwem dokument. Wierzmy, że posłuży on koordynacji działań organów państwa w zakresie zapewnienia cyberbezpieczeństwa i zarządzania kryzysowego w celu zapewnienia maksymalnej efektywności. Zgodnie z projektem ustawy dokument będzie przyjmowany w drodze uchwały Rady Ministrów a zostanie przygotowany przez ministra właściwego do spraw informatyzacji. Oczywiście duża rola w jego przygotowaniu będzie spoczywać na Rządowym Centrum Bezpieczeństwa, jako gwaranta takiej spójności ze wszystkimi dokumentami z zakresu zarządzania strategicznego zarówno na poziomie strategicznym przede wszystkim, ale również action planów dokumentów wykonawczych.

Jeszcze kilka słów o krajowym planie. Będzie on określał:

- cele krajowych środków i działań służących w zakresie gotowości zadania organów zaangażowanych w zarządzanie kryzysowe w celach bezpieczeństwa i procedury zarządzania kryzysowego w cyberprzestrzeni, w tym włączenia do ogólnych krajowych ram zarządzania kryzysowego oraz kanału wymiany informacji;
- krajowe środki służące do zapewnienia gotowości na wypadek wystąpienia incydentu na dużą skalę, w tym ćwiczenia i szkolenia;
- zasady współpracy między sektorem publicznym i prywatnym w obszarze zarządzania kryzysowego;
- rodzaje krytycznej infrastruktury teleinformatycznej;
- krajowe procedury ustalania między odpowiednimi organami i instytucjami krajowymi, mające na celu zapewnienie efektywnego uczestnictwa nas jako Polski w skoordynowanym zarządzaniu incydentami i zarządzaniu kryzysowym w celu zapewnienia bezpieczeństwa na dużą skalę na poziomie Unii, oraz efektywnego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania.

Oczywiście minister cyfryzacji będzie miał uprawnienia, zgodnie z projektem, do odpytywania innych organów administracji co do realizacji strategii. W myśl tego projektu minister cyfryzacji będzie odpowiedzialny za wymiar cywilny. Natomiast w sprawach dotyczących obrony państwa oraz Sił Zbrojnych Rzeczypospolitej Polskiej wydaje nam się, że tym odpowiednim organem jest minister obrony narodowej.

Jak to rozwiązanie ma się z innymi projektowanymi rozwiązaniami prawnymi? Myślę, że wypowiedzą się koledzy z Rządowego Centrum Bezpieczeństwa. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Dziękuję. W takim razie proszę o zabranie głosu przedstawiciela ministra klimatu.

Podsekretarz stanu w MKiŚ Maciej Bando:

Dziękujemy bardzo. W Ministerstwie Klimatu i Środowiska funkcjonuje Departament Spraw Obronnych Zarządzania Kryzysowego i Bezpieczeństwa. Poproszę pana dyrektora Panka o przedstawienie informacji.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję, panie ministrze.

Zastępca dyrektora Departamentu Spraw Obronnych, Zarządzania Kryzysowego i Bezpieczeństwa Ministerstwa Klimatu i Środowiska Ireneusz Panek:

Panie przewodniczący, szanowni państwo, jeżeli chodzi o systemy, którymi zajmuje się Ministerstwo Klimatu i Środowiska, to mamy dwa systemy: system zaopatrzenia w ener-

gie, surowce energetyczne i paliwa oraz system produkcji składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. Tutaj nie chciałbym absolutnie powtarzać, ponieważ właściwie te zadania, które realizujemy jako departament w Ministerstwie Klimatu i Środowiska, są bardzo zbieżne do tych, które realizowane są przez departamenty, które panowie tutaj przedstawiali.

Jeżeli chodzi o system zaopatrywania w energię, surowce energetyczne i paliwa, obejmuje on w szczególności jednostki wytwórcze energii elektrycznej i ciepła, punkty wejścia surowców w kraju, czyli terminale Gazoport, Naftoport track, interkonektory, połączenia graniczne z państwami sąsiadującymi oraz systemy przesyłu. Dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Z ministerstw jeszcze mamy infrastrukturę. Poproszę o zabranie głosu.

Dyrektor Biura Zarządzania Kryzysowego w Ministerstwie Infrastruktury Zbigniew Kręcisz:

Panie przewodniczący, szanowni państwo, Ministerstwo Infrastruktury odpowiada za dwa systemy infrastruktury krytycznej. To jest system zaopatrzenia w wodę i system transportowy. System zaopatrzenia w wodę to około 70 obiektów. Jest również ponad 70 obiektów systemu transportowego.

Jeżeli chodzi o system transportowy, bo tutaj było to wskazane w agendzie, są to nowo wrzucone do wykazu infrastruktury krytycznej przejścia graniczne, kolejowe tunele, mosty i dworce pod stacje trakcyjne, drogowe mosty.

Jeżeli chodzi o system transportowy, to takie obiekty jak nowo wprowadzone do wykazu przejścia graniczne, kolejowe tunele i mosty, dworce pod stacje trakcyjne, drogowe mosty, porty lotnicze wskazane i morskie, tory wodne wraz z falochronami.

W chwili obecnej zostały przekazane dodatkowe wnioski o rozszerzenie wykazu infrastruktury krytycznej w zakresie systemu transportowego o obiekty lotnicze oraz obiekty będące w zarządzie PGW Wody Polskie. Trwa również analiza dotycząca włączenia obiektów i urządzeń kolejowych do wykazu infrastruktury krytycznej. Ponadto to, co mówili też moi przedmówcy, w oparciu o wszelkie zadania i uprawnienia wynikające z Narodowego Programu Ochrony Infrastruktury Krytycznej dokonujemy w ministerstwie okresowych analiz i ocen skuteczności. Wyjeżdżamy tak naprawdę na obiekty infrastruktury krytycznej, badamy ich możliwości i ochronę.

To, co było też wspomniane, trafiają do nas oczywiście plany ochrony infrastruktury krytycznej do uzgodnienia. Współpracujemy z Rządowym Centrum Bezpieczeństwa, z Centrum Antyterrorystycznym ABW w zakresie wymiany informacji o zagrożeniach dotyczących infrastruktury krytycznej. Dziękuję uprzejmie.

Przewodniczący poseł Konrad Fryszak (KO):

Po tym wystąpieniu mamy chyba wszystkie kluczowe ministerstwa, które zabrały głos. Chyba, że jeszcze Ministerstwo Spraw Wewnętrznych i Administracji. Panie dyrektorze?

Dyrektor Departamentu Ochrony Ludności i Zarządzania Kryzysowego Ministerstwa Spraw Wewnętrznych i Administracji Dariusz Marczyński:

Dzień dobry państwu. Panie przewodniczący, jeśli pan pozwoli, to chętnie uzupełniając zabiorę głos po wystąpieniu dyrektora Rządowego Centrum Bezpieczeństwa.

Przewodniczący poseł Konrad Fryszak (KO):

Tak, oczywiście. To był mój kolejny plan, poprosić pana dyrektora o zabranie głosu.

Dyrektor Rządowego Centrum Bezpieczeństwa Zbigniew Muszyński:

Panie przewodniczący, panie posłanki i panowie posłowie, analizując temat dzisiejszego spotkania, stwierdziłem że nie ma sensu, żebyśmy przywoływali przepisy dotyczące ustawy zarządzania kryzysowego. Nie ma sensu mówić co to jest Narodowy Program Infrastruktury Krytycznej, bo te materiały są ogólnie dostępne i można się z nimi zapoznać. Szkoda państwa czasu, żeby o tych rzeczach mówić. Wydawało nam się, że w dniu dzisiejszym bardziej interesujący będzie dla państwa element wzmacniania odporności kluczowych elementów infrastruktury krytycznej.

Po drugie, nie chcemy też z punktu widzenia nas, jako prowadzących wykaz podmiotów krytycznych, który jest niejawnym, cokolwiek dzisiaj przedstawiać na temat konkretnych podmiotów.

Jeżeli chodzi o temat związany z odpornością kluczowych elementów infrastruktury krytycznej, to w zeszłym roku we współpracy z Ministerstwem Klimatu i Środowiska, bardzo dziękujemy ministerstwu bo to była niebywale dobra współpraca, jeśli chodzi o przeprowadzenie dwuetapowych stress testów infrastruktury, ponieważ nic lepiej nie odpowie nam na pytanie na jakim jesteśmy etapie, jeżeli chodzi o odporność jak zrealizowanie realnych stress testów, a nie żadnych pokazów czegoś, co by było uwidocznione tylko włącznie, jak jesteśmy zdolni, zdrowi i skuteczni.

Stress testy były dwuetapowe. Miały na celu sprawdzenie polityki procedur funkcjonujących u operatorów infrastruktury przewidzianych na wypadek nagłych zdarzeń oraz określenie możliwości administracji publicznej w zakresie udzielania wsparcia operatorowi infrastruktury krytycznej. Było przygotowanych 16 scenariuszy zawierających incydenty skutkujące ograniczeniem lub całkowitym wstrzymaniem świadczonego przez operatorów usług. Stress testy przeprowadzono w dwóch etapach. Pierwszy był 15–18 czerwca 2023 r. i obejmował 10 zdarzeń. Drugi był w okresie 13–16 września 2023 r. i obejmował 6 zdarzeń. Stress testy odbyły się na rzeczywistych stanowiskach pracy w siedzibach operatorów infrastruktury krytycznej. Podmioty biorące udział odpowiedzialne były za przygotowanie własnych miejsc ćwiczeń oraz określenie własnego składu zespołu ćwiczącego z właściwych komórek organizacyjnych w służbie jednostek organizacyjnych podległych lub przez nie nadzorowanych.

W siedzibie RCB na czas ćwiczeń stworzono sztab koordynujący, w skład którego weszli przedstawiciele zaproszonych urzędów, instytucji. W siedzibach urzędów i instytucji na czas ćwiczeń utworzono struktury właściwe do podejmowania działań, wydawania poleceń i decyzji. W siedzibie Rządowego Centrum Bezpieczeństwa na czas ćwiczeń utworzono zespół komunikacji strategicznej.

Celami szczegółowymi osiągniętymi podczas realizacji stress testu było zmniejszenie ryzyka wystąpienia zagrożenia, podniesienie odporności i ustanowienie barier ograniczających rozprzestrzenianie się zagrożenia, sprawdzenie mechanizmów zarządzania skutkami zagrożenia, sprawdzenie rozwiązań organizacyjnych i proceduralnych zawartych w planach ochrony infrastruktury krytycznej, sprawdzenie obiegu informacji i przetestowanie mechanizmów koordynacji polityki informacyjnej w sprawie ewentualnych słabych punktów, dobrych praktyk i szacowanie oczywiście strat finansowych i wizerunkowych.

Proszę państwa, realizacja tych stress testów w znaczący sposób przyczynia się do uściślenia współdziałania i podejmowania doraźnych działań przez operatorów. Dodatkowym założeniem przeprowadzania tych testów było również uzyskanie od operatorów informacji o stanie gotowości. Powyższe zrealizowane zostało poprzez prowadzenie wśród operatorów badania samooceny – co było dla nas bardzo istotne – posiadanych sił, środków i analizy posiadanych procedur uruchamiania środków w warunkach skrajnych.

Na podstawie ankiety uzyskanej od operatorów był raport, który zanonimizowano, biorąc pod uwagę różne podmioty z listy infrastruktury krytycznej. Chciałbym państwu tylko zaprezentować pytania, które były. Nie chciałbym dzisiaj na tym forum mówić jak procentowo wychodziło, jeżeli chodzi o to, ile podmiotów uznało, że pewne elementy są już gotowe, a które nie. Na ten moment wołałbym w sposób jawny tego nie mówić.

Ustaliliśmy czy zagrożenia w obszarze antagonistycznym, czyli takie, dla których trudno ustalić motyw w jakim się wydarzyły, bo jeżeli mówimy o zagrożeniach hybrydowych często mówimy o motywach politycznych państwa niejasno przedstawionych, mówimy często o zagrożeniach terrorystycznych, ale wiadomo, że to organizacje terrorystyczne. Jednak jest szereg innych czynności, działań, które mogą wystąpić, a które mogą być spowodowane przez człowieka i nazwalibyśmy je antagonistyczne.

Pytaliśmy się, czy zagrożenia antagonistyczne zostały wcześniej zidentyfikowane. Wszyscy musieli powiedzieć czy te zagrożenia, które były w scenariuszu, były brane pod uwagę, czy nie. Czy zagrożenia, które wystąpiły, były brane pod uwagę w analizie ryzyka,

ponieważ proszę państwa przypominam, że unijny mechanizm ochrony ludności narzuca na nas (dokładnie art. 6 tego mechanizmu) bardzo poważne podejście do oszacowania ryzyka.

Jaka jest skala oddziaływania potencjalnych skutków na odbiorców usługi? Słowo „usługi” podkreślam i za chwilę wyjaśnię dlaczego. To się trochę teraz zmieni pod względem formalnoprawnym, biorąc pod uwagę dyrektywę CER. Jaki jest wpływ na inne podmioty i usługi? Też to jest związane z dyrektywą CER – to pytanie, które zadaliśmy podmiotom.

Czy istnieje proces zarządzania ryzykiem związanym z wystąpieniem wskazanych podczas ćwiczeń zagrożeń? Czy podmioty posiadają zabezpieczenia adekwatne do wskazanych zagrożeń? Czy podmioty posiadają wystarczającą ilość krytycznych komponentów, w tym zasobów ludzkich pozwalających przywrócić usługę do pożądanego poziomu funkcjonowania przed zdarzeniem? W ramach tych ćwiczeń ustalaliśmy, w przypadku jakiegoś zagrożenia krytycznego, które spowodowałoby unieruchomienie określonej usługi, jaki jest czas odtworzenia tej usługi przez dany podmiot krytyczny.

Jeśli chodzi o odpowiedzi procentowe, tak jak powiedziałem, nie chcę tego przytaczać. Jeżeli chodzi o poszczególne podmioty, to były różne odpowiedzi i informacje czy byli na to gotowi, czy nie.

Podsumowując chciałbym powiedzieć, że obecna ustawa o zarządzaniu kryzysowym skupia się przede wszystkim na ochronie pojedynczych obiektów. Do tej pory mieliśmy myślenie o charakterze ochrony infrastruktury krytycznej. Dyrektywa CER to zmienia bardzo mocno z racji tego, że dyrektywa CER mówi o usługach kluczowych i podmiotach krytycznych, które mają świadczyć usługi. Dlatego też w zeszłym miesiącu pan premier zlecił Rządowemu Centrum Bezpieczeństwa dokonanie nowelizacji ustawy o zarządzaniu kresowym w kontekście implementacji dyrektywy CER i również elementów unijnego mechanizmu ochrony ludności. W związku z tym, mówiąc szczerze, że to podejście, które na dzień dzisiejszy jest w związku z obecnie funkcjonującą ustawą, zmieni się dosyć mocno. Problem wytłumaczenia wszystkim użytkownikom, dlaczego przechodzimy od tylko wyłącznie ochrony obiektowej, czyli infrastruktury krytycznej, na ochronę usług będzie trudny do przedstawienia, wyjaśnienia. Niemniej jednak pamiętajmy, że podmiot infrastruktury krytycznej może być tylko elementem całej usługi, a każdy fragment danej usługi może rzutować na ten właśnie podmiot infrastruktury krytycznej.

Chciałem jeszcze w dwóch zdaniach powiedzieć, że w ramach tych planowanych zmian, jeśli chodzi o ustawę o zarządzaniu kryzysowym – nie chcę oczywiście w tej chwili mówić o szczegółach, bo jesteśmy już mocno zaawansowani – jeżeli chodzi o ustalenia musimy jeszcze pewne szczegóły poustalać, ale musimy też pamiętać o tym, że są pewne rodzaje obiektów, które wymagają zainteresowania się ich bezpieczeństwem zanim w ogóle powstaną. Stąd chcemy też mówić w tej nowej ustawie o obiektach w trakcie budowy. Jeżeli będziemy mieli elektrownię atomową czy farmy wiatrowe, to wcześniej musimy myśleć o kwestiach bezpieczeństwa, a nie po tym jak cała infrastruktura powstanie.

Również ważna jest kwestia dotycząca pisania planów ochrony przez różne podmioty krytyczne. Chcemy przejść na element certyfikowania na stworzenie minimalnych standardów, które będzie trzeba spełnić. To, co koledzy z Ministerstwa Cyfryzacji powiedzieli, dla nas bardzo ważne jest, żeby nowa ustawa o krajowym systemie cyberbezpieczeństwa, w oparciu o NIS2 była kompatybilna z tą naszą nowelizowaną ustawą o zarządzaniu kryzysowym. Obecny ze mną szef wydziału ochrony infrastruktury krytycznej pan doktor inżynier Witold Skomra bierze udział, konsultuje się cały czas z kolegami z Ministerstwa Cyfryzacji w zakresie prac nad NIS2. Chcemy, żeby to było od początku do końca kompatybilne, ponieważ dzisiaj trudno sobie wyobrazić, żeby jakkolwiek sektor funkcjonował bez informatyki, bez sfery cyber. Oczywiście największym wyzwaniem będzie dla nas ustalenie, które to są podmioty kluczowe dyrektywy CER. Przypominam tylko, że dyrektywa CER mówi o jakiś minimalnym zastosowaniu uwarunkowań wynikających dyrektywy, a każdy kraj członkowski może sobie dowolnie elementy poszerzyć,

jeżeli chodzi o swoje kwestie związane z bezpieczeństwem świadczenia usług kluczowych w ochronie infrastruktury krytycznej. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Panie dyrektorze, czy teraz zabierze pan głos?

Dyrektor departamentu MSWiA Dariusz Marczyński:

Bardzo dziękuję, panie przewodniczący. Myślę, że w tej chwili bardziej zrozumiała jest istota, dlaczego prosiłem, żeby moje wystąpienie poprzedziło wystąpienie dyrektora RCB. Mianowicie przy każdej formule identyfikacji zagrożeń w infrastrukturze krytycznej, ale też i w ocenie ryzyk, w tym obszarze zadań uczestniczy Ministerstwo Spraw Wewnętrznych, zwłaszcza jeśli chodzi o ocenę zadaniową i ewentualnie uruchamianie systemu bezpieczeństwa publicznego i bezpieczeństwa powszechnego, jak i zarówno w ocenie przeciwdziałania zagrożeniom, jak i w procesie reagowania.

Stąd to, o czym powiedział pan dyrektor RCB odnośnie przygotowania implementacji dyrektywy CER. Tak że we współdziałaniu przy implementacji dyrektywy NIS2, chcemy w tym procesie nie tylko uczestniczyć, a minister spraw wewnętrznych popiera bardzo mocno to oczekiwane od dawna działanie, zwłaszcza jeśli chodzi o filozofię przejścia z podejścia ochrony infrastruktury krytycznej, z podejścia obiektowego na usługowe. Praktycznie przy wszystkich matrycach ryzyk, gdy patrzymy na obszar sektora energetycznego czy transportowego, mamy zawsze przy tym zadaniu realizację uruchomienia systemu bezpieczeństwa publicznego i powszechnego. Stąd też patrzymy nie tylko na sektor, który dzisiaj nadzoruje minister spraw wewnętrznych, np. ratownictwo, ale w przestrzeni tutaj wspomnianych sektorów mamy rozpisane bardzo szczegółowe zadania dla Straży Granicznej, Policji, Państwowej Straży Pożarnej, jako że czujemy się współodpowiedzialni za te sektory w każdym procesie i w każdej fazie zarządzania ochroną infrastruktury krytycznej.

Na dziś wydaje się, że kluczową kwestią jest zmiana przepisów i tak jak Parlament Europejski, Komisja podjęła decyzję, żeby implementacja dyrektywy nastąpiła możliwie najszybciej. To jest kierunek strategiczny, który nie tylko popieramy, ale chcemy w nim uczestniczyć. Bardzo dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Dziękuję. Czy ktoś z państwa chciałby jeszcze zrobić głos? Nie widzę. Pan komendant? Bardzo proszę.

Zastępca komendanta głównego Państwowej Straży Pożarnej Józef Galica:

Szanowny panie przewodniczący, szanowni państwo. Co prawda zostałem jako pierwszy wywołany do głosu, ale myślę, że to się dobrze tutaj poukładało.

Przewodniczący poseł Konrad Fryszak (KO):

Panie komendancie, tylko dlatego, że jak nie ma chętnych, to wiadomo, że Straż jest zawsze pierwsza.

Zastępca komendanta głównego PSP Józef Galica:

Dziękuję bardzo. Państwowa Straż Pożarna jest pewnego rodzaju jednym z elementów struktury państwa, która chroni infrastrukturę krytyczną. Tutaj parę słów o naszej infrastrukturze, bo tu taką też w zasadzie posiadamy. Przy Komendancie Głównym jest zespół reagowania kryzysowego. Mamy szesnaście planów ochrony infrastruktury krytycznej w ramach wszystkich komend wojewódzkich i jeden plan ochrony infrastruktury krytycznej Komendy Głównej. Bardzo aktywnie uczestniczymy w procesie reagowania i do tego służy w zasadzie cały potencjał Straży Pożarnej. Może tutaj tak ekspresowo powiem, że jest to 504 jednostek ratowniczo-gaśniczych, około 30 tys. strażaków, 5030 jedenastek ochotniczych straży pożarnych, w ramach Krajowego Systemu Ratowniczo-Gaśniczego. Nie chcę tutaj zanudzać, ale to 1600 samochodów ratowniczo-gaśniczych, 4200 samochodów specjalnych. Posiadamy też w swoich zasobach i potencjale ratowniczym 194 specjalistyczne grupy poszukiwawcze. To wszystko jest w każdej chwili dostępne do ochrony infrastruktury krytycznej. Oczywiście stałym elementem

jest też przeciwdziałanie zagrożeniom, więc uczestniczymy w uzgadnianiu wszelkiego rodzaju planów ochrony struktury krytycznej. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Bardzo proszę.

Prezes Krajowego Sztabu Ratownictwa Społecznego Sieci Ratunkowej Jerzy Płókarz:

Dziękuję, panie przewodniczący. Jerzy Płókarz, Krajowy Sztab Ratownictwa Społecznej Sieci Ratunkowej. Nasza organizacja chciałaby zwrócić uwagę, a może nie tyle zwrócić uwagę ile zapytać się przedstawicieli rządu, czy państwo bierzecie pod uwagę problem związany z tym, że firma Orange, która przejęła Telekomunikację Polską, systematycznie niszczy, likwiduje infrastrukturę łączności przewodowej. W naszej ocenie jest to problem dosyć poważny, ponieważ w sytuacji kryzysowej zagrożenia bezpieczeństwa państwa wyłączyć łączność bezprzewodową jest stosunkowo łatwo, ale o wiele trudniej jest wyłączyć łączność przewodową. Tutaj może warto zwrócić na to uwagę, bo w ocenie nas, łącznościowców, jest to jednak pewien problem.

Jeżeli chodzi o naszą organizację, to chciałbym pochwalić się naszymi możliwościami, bowiem w razie czego tworzymy taką łączność rezerwową. Jest to łączność oparta o około 2 mln punktów łączności – uwaga – niezależnych od infrastruktury energetycznej, bo są to z radiotelefony na akumulatory zasilane 12V i w sytuacjach kryzysowych, jak np. w 1997 r. powódź, stanowiliśmy jedyną łączność pomiędzy służbami państwowymi a obywatelem z uwagi na to, że było tyle tych punktów łączności niezależnych. Jest to nasycenie około 2 mln punktów w społeczeństwie. Tu wypada przypomnieć, że idea łączności obywatelskiej (CB Radio) powstała w czasie II wojny światowej, kiedy to konstruktor radiowy Al Gross ze Stanów Zjednoczonych w oparciu o tę łączność utrzymywał łączność aliantów z ludnością na okupowanych terenach. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję, panie prezesie. Czy na to pytanie ktoś z państwa zechce odpowiedzieć? Nie widzę chętnych. Może uproszczę pytanie. Jakie jest nasze podejście do komunikacji przewodowej na czas zagrożenia? Bardzo proszę, panie ministrze.

Podsekretarz stanu w MKiŚ Maciej Bando:

Panie przewodniczący, szanowni państwo, myślę że w dzisiejszych czasach należałoby rozróżnić dwa systemy komunikacyjne. Istotnie w dawnych czasach jedynym przedstawicielem analogowej łączności były sieci przewodowe. Dzisiaj możemy mówić o dwóch rodzajach łączności, czyli sieci cyfrowej (komórki współczesne) i analogowej, w skład której wchodzi zarówno połączenia przewodowe (stare telefony), jak i innego rodzaju łączność analogowa, np. CB Radio. To takie doprecyzowanie. Oba te systemy wciąż działają w różnych gałęziach gospodarki i niekoniecznie muszą się ograniczać tylko do przewodowej.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Czy ktoś z państwa ma pytania? Bardzo proszę, pan dyrektor z Ministerstwa Cyfryzacji.

Zastępca dyrektora departamentu MC Marcin Wysocki:

Dziękuję, panie przewodniczący. Przede wszystkim środki komunikacji powinny być rezydentne. Przed nami wiele wyzwań, między innymi zapewnienie większej powszechności dostępu również do komunikacji niejawnej, chociażby na poziomie zastrzeżonym. Organy państwa dążą do tego, żeby te zdolności w tym obszarze jak najbardziej rozwijać.

Co do kwestii prowokacyjnego postawienia pytania mogę powiedzieć, że na pewno zachodzą w telekomunikacji procesy migracji z sieci starych miedzianych na alternatywne rozwiązania. Natomiast, co do ogromnej skali inwestycji walczenia z „białymi plamami”, uzupełniania pokrycia zarówno sieciami stacjonarnymi jak i niestacjonarnymi, rozwojem łączności ruchomej, to szczegółowe dane moglibyśmy przekazać na piśmie. Natomiast z tego miejsca chciałem zadeklarować, że ta teza w mojej ocenie jest nieprawdziwa. Dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

To bardzo dobra informacja. Dziękuję. Czy są jakieś pytania? Bardzo proszę, pan dyrektor.

Zastępca dyrektora departamentu MAP Bartosz Pelk:

Ja bym tylko jeszcze dodał à propos Orange SA, że to jest też podmiot, który znajduje się na liście podmiotów podlegających ochronie, który podlega tej ochronie ustawy...

Przewodniczący poseł Konrad Fryszak (KO):

Chyba tego, to pan nie powinien mówić.

Zastępca dyrektora departamentu MAP Bartosz Pelk:

Panie przewodniczący, to są naprawdę jawne informacje. To jest ustawa jawna, rozporządzenie jest jawne, więc naprawdę nie mówię o niczym zastrzeżonym. Byłem pełnomocnikiem do spraw informacji niejawnych przez 3 lata i czuwam nad tym. Naprawdę mówię, jeszcze raz powtarzam, o jawnych rzeczach, które można przeczytać w internecie i ten wykaz też jest jawny. Spółka Orange podlega tej szczególnej ochronie i à propos tego pytania pana, które tutaj kolega dyrektor określił „prowokacyjne”, to jeżeli faktycznie miałyby miejsce sprzedawanie czy zaniechanie sprzedawania, czy eksploatacji tych sieci światłowodowych, które tworzyłyby zorganizowaną część przedsiębiorstwa, to tutaj też przepisy pozwalają na to, żeby takie procesy w odpowiedni sposób kontrolować i nad nimi czuwać.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Pani posłanka Urszula Nowogórska, bardzo proszę.

Posel Urszula Nowogórska (PSL-TD):

Panie przewodniczący, szanowni państwo, wedle pełnionych funkcji, godności reprezentowanych instytucji. Mam taki wniosek formalny, panie przewodniczący, żeby zastanowić się nad zwołaniem podkomisji w trybie niejawnym w najbliższym czasie i porozmawiać między innymi na tematy dotyczące łączności i tego, co tutaj pan zaczął nam przedstawiać.

Wydaje mi się, zresztą pan przewodniczący też ma chyba podobną sugestię, że jest niezbyt jasno wyznaczona granica pomiędzy informacjami jawnymi a niejawnymi, które można poruszać w tym trybie, w którym dzisiaj się spotykamy. W związku z czym w zeszłym roku na posiedzeniu podkomisji też sygnalizowałam, że warto by było przyrzeć się systemom łączności, budowie światłowodów i jednostkom, które nad tym czuwają, nadzorują i czyją są potem one własnością. Dlatego myślę, że taki wniosek, panie przewodniczący, dzisiaj złożę i bardzo proszę, aby takie posiedzenie w temacie poruszonym przeze mnie w trybie niejawnym zostało zorganizowane, oczywiście w ramach możliwości i czasu. Bardzo dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Pomyślimy nad tym, żebyśmy w ramach Komisji zrobili takie posiedzenie i może trochę w sposób bardziej otwarty rozmawiali o pewnych rzeczach i płynących stąd zagrożeniach. Bardzo proszę, pan przewodniczący.

Posel Piotr Lachowicz (KO):

Panie ministrze, panie generale, szanowni państwo, może dookreślę jako osoba, która prowadziła kiedyś postępowania sprawdzające w imieniu stosownych służb, jak nie byłem posłem.

Proszę państwa, określa to ustawa o ochronie informacji niejawnych – art. 34, na który zwrócił uwagę pan minister. Ona co prawda w ust.10 pkt 14 zwalnia posłów i senatorów z uzyskania poświadczenia bezpieczeństwa do dokumentów...mówimy: zastrzeżone, poufne, tajne. Natomiast już przy ściśle tajnych, jeżeli są takie informacje, to poseł lub senator musi przejść stosowne postępowanie sprawdzające.

Co mogę jeszcze dodać? Wszystko zależy, ponieważ my nie znamy, jaką klauzulę mają dokumenty lub to, co powiedział pan dyrektor, lub jej nie mają. Jeśli dokument nie ma klauzuli, to jest jawny. Natomiast jeśli ma klauzulę, to jeszcze musimy rozstrzygnąć jaka jest ta klauzula. Mówię do tego, o czym mówiła pani przewodnicząca, ponieważ

jeśli byłyby to dokumenty...oczywiście po odpowiednim przygotowaniu sali i pomieszczenia, w którym takie informacje są udostępniane, to jeśli byłaby to klauzula „tajne”, to my jako posłowie możemy uczestniczyć bez poświadczenia, ale gdyby to już były dokumenty mające charakter – o czym mówił pan minister – „ściśle tajne”, to wtedy już musielibyśmy uzyskać stosowne poświadczenie bezpieczeństwa. Dziękuję uprzejmie.

Pani przewodnicząca jest członkiem Komisji Obrony Narodowej i być może ma takie poświadczenie bezpieczeństwa.

Zastępca dyrektora departamentu MAP Bartosz Pelk:

Jeszcze raz powtórzę, że ustawa o kontroli niektórych inwestycji jest normalnym dokumentem prawnym. Rozporządzenie w sprawie wykazów podmiotów podlegających ochronie każdy może sobie w internecie ściągnąć, przeczytać. Ono jest wydawane co roku. Dziennikarze zawsze piszą na początku każdego roku o tych podmiotach. Naprawdę przysięgam, nie ujawniłem tutaj żadnej informacji chronionej państwowej, broń Boże.

Temat PERN-u. Rozumiem pana ministra, ale tak jak mówię, to też nie jest dokumentacja niejawna. Może mieć ona oznaczenie „tajemnica przedsiębiorstwa”, „tajemnica spółki”, ale akurat przed przyjściem też sobie zerknąłem na ten temat, bo chciałem to przejrzeć i te dokumenty nie miały takich odznaczeń. Informuję, że to nie jest informacja niejawna, ale przepraszam pana ministra za to, bo niepotrzebnie wywołaliśmy taką dyskusję. Powtarzam – mówię o jawnych sprawach.

Przewodniczący poseł Konrad Frysztak (KO):

Bardzo dziękuję. Są pytania. Bardzo proszę, panie pośle.

Poseł Arkadiusz Sikora (Lewica) – spoza składu Komisji:

Dziękuję. Panie przewodniczący, panie ministrze, panowie komendanci, pytanie o przesłanki, którymi kierujemy się wyznaczając tę infrastrukturę. Przepraszam, że pytam, ale jestem posłem pierwszą kadencję, być może posłowie tu bardziej doświadczeni już to przerabiali. Czy to są przesłanki dotyczące lokalizacji, patrz wojna za naszą wschodnią granicą, czy przesłanki wyłącznie wynikające z przeznaczenia tej infrastruktury? Jeżeli oczywiście to nie jest tajna odpowiedź. To jedno pytanie.

Drugie. Pan komendant mówił o zasobach Państwowej Straży Pożarnej. Czy one służą państwu do wszystkich akcji, czy są też takie, które są tylko dedykowane stricte do ochrony tej infrastruktury krytycznej z tych wszystkich, które pan wymieniał? Dziękuję.

Zastępca komendanta głównego PSP Józef Galica:

Króciutko. Nie ma oczywiście takich wydzielonych sił i środków, które w zasadzie posiadamy w ramach tych planów ratowniczych i ochrony infrastruktury krytycznej. Są tam dedykowane siły i środki, ale to siły i środki można powiedzieć ogólnie uniwersalne, krótko mówiąc – do wszystkiego.

Przewodniczący poseł Konrad Frysztak (KO):

Dziękuję. Kto odpowie na pierwsze pytanie? Bardzo proszę.

Doradca w Rządowym Centrum Bezpieczeństwa Witold Skomra:

Dzień dobry. Witold Skomra, Rządowe Centrum Bezpieczeństwa. Według obecnego stanu prawnego wyłanianie infrastruktury krytycznej odbywa się na takich trzech poziomach. Na początku trzeba wyraźnie powiedzieć, że nie jest to procedura decyzji administracyjnej. Efekt jest taki, że podmiot objęty tymi regulacjami nie może się odwołać do sądu co do meritum. Może się odwołać tylko i wyłącznie co do procedury. Dlaczego tak? Dlatego, że procedura zmierza do stwierdzenia stanu istniejącego, a nie do uznaniowości przyznania czegoś albo odebrania. Po prostu mamy stwierdzić, czy dane fakty mają miejsce i tylko tyle.

Te trzy kroki po kolei, to jest sprawdzenie czy podmiot, obiekt podejrzewany, nazwijmy to, byciem infrastrukturą krytyczną, spełnia kryteria przekrojowe dla danego sektora. Te kryteria są charakterystyczne dla danego sektora. Co innego w sektorze energii, co innego w służbie zdrowia oczywiście. Później, czy spełnia przesłanki ustawowe związane z kluczową rolą dla funkcjonowania państwa w całości społeczeństwa,

gospodarki lub podmiotów gospodarczych. Wreszcie trzeci filtr, taki najciekawszy. To jest siedem obszarów związanych ze skutkami dysfunkcji danego obiektu. Tu już mamy takie twarde dane ilościowe w stylu: spodziewane straty wśród ludzi, spodziewana wielkość ewakuacji, straty finansowe liczone w procencie PKB, ale również zdolność czy zakłócenie zdolności do realizacji zobowiązań sojusznicznych międzynarodowych itd. Siłą rzeczy dane ilościowe z tych siedmiu obszarów są niejawne. Taki jest stan prawny na dzień dzisiejszy. Podkreślam, że mówimy cały czas o obiektach, chociaż po zmianie Narodowego Programu Ochrony Infrastruktury Krytycznej w zeszłym roku jest możliwość uznania za obiekt infrastruktury krytycznej również usługi. Tak, jak tu wspomniano, po raz pierwszy zastosowano to do przejść granicznych. Natomiast dyrektywa CER nakazuje rozszerzenie tego podejścia właśnie o podejście usługowe. Czyli od początku do końca bierzemy np. usługę dostawy paliw i wyszukujemy podmioty, które mogłyby tę usługę zakłócić. Czyli nie patrzymy powiedzmy na bazę paliw i bezpieczeństwo tejże bazy paliw, tylko jakie ono ma znaczenie dla funkcjonowania dostaw paliw w całym kraju. Będzie to żmudne, długotrwałe i w przeciwieństwie do dyrektywy NIS2, która nie daje żadnej możliwości dyskusji: czy podlegam, czy nie podlegam, tam jest tylko kryterium czy prowadzę daną działalność i jakim dużym podmiotem jestem, to niestety dyrektywa CER2 pozwala podmiotom na pewną uznaniowość.

Natomiast chciałem podkreślić, że i tak nie odchodzimy od ochrony obiektowej, wręcz ją wzmocnimy. Tak, że to przejście na podejście usługowe nie spowoduje żadnego osłabienia poziomu bezpieczeństwa, które zostało osiągnięte na dzień dzisiejszy.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Czy ktoś z państwa ma jeszcze jakieś pytania? Pozwolę sobie skonstruować pytanie, choć częściowo pan dyrektor z Rządowego Centrum Bezpieczeństwa, pan dyrektor Muszyński odpowiedział. Pytanie, czy to wy zostaliście wskazani jako ci, którzy będą implementować dyrektywę CER? Wiemy, że termin zawity jest chyba 17 października 2026 r. Obie?

Dyrektor RCB Zbigniew Muszyński:

Przepraszam, panie przewodniczący. Daty w 2026 r. to są daty wynikające z tego, co po wdrożeniu dyrektywy CER musimy osiągnąć w tych terminach.

Przewodniczący poseł Konrad Fryszak (KO):

Słuszna uwaga. I wy będziecie implementować?

Dyrektor RCB Zbigniew Muszyński:

Wystąpiłem do premiera o zgodę na to, żeby Rządowe Centrum Bezpieczeństwa procedowało nowelizację ustawy o zarządzaniu kryzysowym, ponieważ chcemy – co pan Wiktor Skomra powiedział wcześniej – żeby nie zgubić pewnych rozwiązań, które już funkcjonują i są u nas uznane przez podmioty krytyczne. Chcemy w związku z tym zrobić nowelizację. Głównym celem jest implementacja dyrektywy CER do ustawy o zarządzaniu kryzysowym. Dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Dziękuję. Mam jeszcze jedno pytanie. Czy zdefiniowaliście, to chyba pytanie do wszystkich państwa, elementy o tym charakterze kluczowym, których zaburzone działanie może mogłoby powodować sytuację kryzysową w dużej skali?

Doradca w RCB Witold Skomra:

Panie przewodniczący, szanowni państwo, taką wstępną listę około 120, o ile dobrze pamiętam, usług kluczowych, które powinniśmy brać pod uwagę pisząc swoje rozporządzenie, przygotowała Komisja Europejska i rozesłała do wszystkich krajów. Myśmy wstępnie przeprowadzili już takie dwie tury uzgodnień ze wszystkim ministerstwami, jak oni to widzą. Lista najpierw przekraczała liczbę około 300 usług kluczowych. Po komasacji zeszliśmy mniej więcej do 150, ale podejrzewam, że jak ukaże się sam projekt ustawy, a przede wszystkim jak się ukaże projekt ustawy o krajowym systemie cyberbezpieczeństwa, bo one są mocno powiązane, to pewnie tu jeszcze będą zmiany. Cały czas nad tym pracujemy, żeby ustalić, co tak naprawdę jest istotne dla funkcjonowania państwa.

Przewodniczący poseł Konrad Fryszak (KO):

Dziękuję bardzo. Proszę, panie dyrektorze.

Dyrektor RCB Zbigniew Muszyński:

Temat implementacji dyrektywy CER to nie jest problem tylko nasz Polski, tylko wszystkich państw Unii Europejskiej. Rozmawiamy z różnymi partnerami i wszyscy dyskutują, jak rozumieć dyrektywę CER i jak to tak naprawdę zaimplementować. Ten element usługowy jest na razie trudny do zrozumienia dla wielu osób i zakładamy, że na etapie obecnym rzeczywiście dyskutujemy na ten temat, jak to miałoby wyglądać. Zobaczmy jak to wyjdzie w skali w ogóle całej Unii Europejskiej. Zakładam, że w przyszłości po wdrożeniu tych przepisów nastąpi pewnego rodzaju rewizja wdrożonych narzędzi z tej racji, że jak zawsze życie zweryfikuje, jak to będzie wyglądało.

Przewodniczący poseł Konrad Fryszak (KO):

Dziękuję. Czy są jeszcze jakieś pytania? Czy ktoś z państwa chciałby zabrać jeszcze głos? Nie widzę, nie słyszę.

Zatem stwierdzam, że wyczerpaliśmy porządek dzisiejszych obrad. Bardzo państwu dziękuję.

Tak, jak powiedziałem, zwrócę się do pani przewodniczącej byśmy odbyli podobne posiedzenie w formule zamkniętej i porozmawiali sobie troszkę szerzej o pewnych rzeczach.

Bardzo państwu dziękuję za przybycie tak liczne na dzisiejszą podkomisję. Zamykam posiedzenie.