VIII kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

# KANCELARIA SEJMU
# Biuro Komisji Sejmowych

## PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Administracji i Spraw Wewnętrznych**
**(nr 148)**
z dnia 11 kwietnia 2018 r.

# Pełny zapis przebiegu posiedzenia

# Komisji Administracji i Spraw Wewnętrznych (nr 148)

11 kwietnia 2018 r.

Komisja Administracji i Spraw Wewnętrznych, obradująca pod przewodnictwem posła **Arkadiusza Czartoryskiego (PiS)**, przewodniczącego Komisji, rozpatrzyła:

**– informację Ministra Cyfryzacji i Ministra Spraw Wewnętrznych i Administracji na temat działalności państwa i podmiotów państwowych w zakresie ochrony, zapobiegania i koordynacji bezpieczeństwa komputerowego i bezpieczeństwa w cyberprzestrzeni, w tym system monitorowania incydentów i zdarzeń oraz reagowania na zagrożenia;**

**– propozycje tematów kontroli do planu pracy Najwyższej Izby Kontroli na 2019 r.**

W posiedzeniu udział wzięli: **Karol Okoński** podsekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami, **Dariusz Bogucki** dyrektor Departamentu Teleinformatyki Ministerstwa Spraw Wewnętrznych i Administracji wraz ze współpracownikami, **Marek Kubiak** dyrektor Rządowego Centrum Bezpieczeństwa, **Marek Bieńkowski** dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli wraz ze współpracownikami, **Piotr Pietrzak** zastępca dyrektora Biura Łączności i Informatyki Komendy Głównej Straży Granicznej, **Marcin Kuskowski** pełnomocnik Komendanta Głównego Policji do spraw bezpieczeństwa cyberprzestrzeni, **Joanna Maj-Marjańska** przedstawicielka Biura Bezpieczeństwa Narodowego.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Magda Jedynak, Izabella Kulesza-Rozesłaniec, Anna Pilarska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dzień dobry państwu. Otwieram posiedzenie Komisji Administracji i Spraw Wewnętrznych.

W porządku obrad mamy rozpatrzenie informacji ministra cyfryzacji i ministra spraw wewnętrznych na temat działalności państwa i podmiotów państwowych w zakresie ochrony, zapobiegania i koordynacji bezpieczeństwa komputerowego i bezpieczeństwa w cyberprzestrzeni, w tym system monitorowania incydentów i zdarzeń oraz reagowania na zagrożenia. W pkt 2 będzie rozpatrzenie propozycji tematów kontroli do planu pracy Najwyższej Izby Kontroli na 2019 r.

Szanowni państwo, witam na naszym posiedzeniu pana ministra Karola Okońskiego – podsekretarza stanu w Ministerstwie Cyfryzacji. To będzie to wiodące wystąpienie. Chciałbym tylko przypomnieć, że do naszych materiałów zostało załączone pismo ministra cyfryzacji – pana Marka Zagórskiego, ze stycznia 2018 r. Witam również przedstawicieli Ministerstwa Spraw Wewnętrznych i Administracji. Na posiedzeniu jest obecny pan dyrektor Dariusz Bogucki, który został upoważniony. Witam serdecznie również państwa współpracowników z Ministerstwa Spraw Wewnętrznych i Administracji. Reprezentowane są departamenty: bezpieczeństwa i teleinformatyki. Witam przedstawicieli Najwyższej Izby Kontroli. Witam również pana Marka Kubiaka – dyrektora Rządowego Centrum Bezpieczeństwa. Witam serdecznie. Witam wszystkich państwa z Komendy Głównej Policji, Komendy Głównej Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego i pozostałych instytucji, których nie wymieniłem. Witam wszystkich bardzo serdecznie. Zabierając głos, proszę o przedstawianie instytucji, którą państwo reprezentujecie.

Szanowni państwo, jak widzimy, minister cyfryzacji przygotował prezentację, którą wyświetli podczas swojego wystąpienia. Bardzo więc bym prosił o zgaszenie światła tutaj

przynajmniej w tej części prezydialnej. O, dziękuję bardzo. Bardzo proszę, panie ministrze. Przepraszam, czy są uwagi do porządku obrad? Nie słyszę. Dziękuję.

Bardzo proszę, panie ministrze.

**Podsekretarz stanu w Ministerstwie Cyfryzacji Karol Okoński:**

Panie przewodniczący, Wysoka Komisjo, ten materiał, który będziemy państwu wyświetlać w charakterze takiej pomocy ułatwiającej przekazanie informacji prezentujących stan prac, jak również zawartość ustawy o krajowym systemie cyberbezpieczeństwa, to jest tylko taka pomoc wizualna. Jeśli chodzi o zawartość, to najważniejszy jest ten materiał, który państwo otrzymali wcześniej, dołączony do pisma pana ministra Zagórskiego. Siłą rzeczy na tym etapie prac w tej informacji nie wchodzimy we wszystkie szczegóły tej ustawy, natomiast chcemy głównie jeszcze raz omówić założenia, zależności i wszystkie podmioty, które są objęte tą ustawą. Stąd też będzie taki moment, w którym wyświetlimy taki schemat, który na pierwszy rzut oka wygląda bardzo groźnie *nomen omen*, ale na tym schemacie będzie również państwu łatwiej rozpoznać wszystkie zależności, które występują pomiędzy podmiotami.

Proszę państwa, patrząc na nasze obecne krajowe przepisy, nie ma w tym momencie żadnej ustawy, która opisywałaby w sposób szczegółowy i zbiorczy zagadnienia cyberbezpieczeństwa w poszczególnych sektorach. Stąd istnieje potrzeba uwzględnienia tych elementów, które są opisane w dyrektywie unijnej w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej, czyli w skrócie NIS, i zaimplementowania do polskiego prawa. Jednocześnie jest to również pewien sposób uporządkowania tych przepisów w jednym akcie normatywnym, gdyż do tej pory te obowiązki nałożone na ministra cyfryzacji wynikają z paru różnych ustaw – z ustawy o informatyzacji, z Krajowych Ram Interoperacyjności, z Prawa telekomunikacyjnego i z ustawy o usługach zaufania i identyfikacji elektronicznej. Te obowiązki, które są zawarte w dyrektywie NIS, a które ujmujemy w naszych polskich przepisach prawa, to przede wszystkim wyznaczenie organów właściwych dla operatorów usług kluczowych i dostawców usług cyfrowych. Mówimy więc de facto o wskazaniu konkretnych organów administracji opiekujących się danym sektorem. Jakie to są sektory, jakie to są relacje, jak powiedziałem, omówimy na schemacie, bo to będzie – myślę – bardziej czytelne dla państwa.

Wprowadzone również zostało pojęcie pojedynczego punktu kontaktowego. Chodzi z kolei o współpracę w ramach całej Unii Europejskiej pomiędzy poszczególnymi krajami członkowskimi i o wyznaczenie, o jasne wskazanie odpowiedzialnego za ten kontakt z poszczególnymi odpowiednikami w innych państwach. To jest coś, co również reguluje ta ustawa. Wprowadza ona również pojęcie operatorów usług kluczowych oraz pewien system wymagań, który jest nałożony w momencie stwierdzenia, w momencie zaklasyfikowania danego podmiotu do tej grupy. Określa ona, jakie obowiązki są nałożone z perspektywy zapewnienia bezpieczeństwa teleinformatycznego na te podmioty. Porządkuje oraz ujednolica i systematyzuje sposób wymiany informacji i raportowania o incydentach, wprowadzając kategorię poważnego incydentu u operatorów usług kluczowych oraz kategorię istotnego incydentu u dostawców usług cyfrowych. O tych zależnościach również więcej opowiemy na tym schemacie, na tym diagramie przedstawiającym relacje. Mocuje również formalnie strategię bezpieczeństwa sieci informacji, czyli daje podstawę do tworzenia takiego dokumentu strategicznego. Wyznacza również tak zwane CSIRT, czyli Computer Security Incident Response Teams, czyli centra, które mają reagować na incydenty bezpieczeństwa w systemach komputerowych. Wskazuje jednoznacznie, który CSIRT odpowiada za które usługi kluczowe i których dostawców kluczowych.

Tak jak mówiłem, sama ustawa jest siłą rzeczy implementacją dyrektywy NIS. Stąd też wynikają pewne terminy, o których zaraz będziemy mówić, ale generalnie jest również okazją do tworzenia i opisania tego efektywnego sposobu zarządzania bezpieczeństwem teleinformatycznym w państwie. Siłą rzeczy po wdrożeniu tych przepisów zakładamy, że dzięki temu będziemy w stanie zapewnić niezakłócone świadczenie usług kluczowych i usług cyfrowych oraz zostanie osiągnięty odpowiedni poziom bezpieczeństwa tych sys-

temów informatycznych, które są przewidziane do świadczenia tych usług. Mówimy więc jednocześnie o poziomie zabezpieczeń jak i o zapewnieniu ciągłości działania.

To jest lista podmiotów, które są objęte ustawą, które są wprowadzane do krajowego systemu. Jak mówiłem, są to operatorzy usług kluczowych i dostawcy usług cyfrowych. Te poszczególne centra zarządzania incydentami. Są trzy takie centra. Jedno jest dla obszaru militarnego – CERT MON czy CERT MIL, CERT.GOV.PL, które znajduje się pod nadzorem Agencji Bezpieczeństwa Wewnętrznego oraz NC CYBER, czyli CERT NASK-owy, dla obszaru cywilnego. Są przewidziane sektorowe zespoły reagowania na incydenty, pojedynczy punkt kontaktu oraz poniżej wymienione instytucje, które również są objęte tymi przepisami. O nich więcej też powiemy na schemacie. Oprócz tego wprowadzone są pewne nowe ciała, mianowicie projektowaną ustawą wprowadzony jest pełnomocnik rządu do spraw cyberbezpieczeństwa wyznaczony przez prezesa Rady Ministrów oraz Kolegium do Spraw Cyberbezpieczeństwa, które pełni rolę doradczą dla pełnomocnika. Trochę więcej o różnicach między tymi ciałami też za chwilę.

Mówiłem o harmonogramie pracy. Jak państwo spojrzą na ten plan działań, to w tym momencie jesteśmy, jeśli chodzi o projekt samej ustawy, na etapie komisji prawniczej, czyli jesteśmy po Komitecie Stałym Rady Ministrów, który przyjął projekt ustawy. Komisja prawnicza jest zaplanowana na przyszły tydzień. Jeśli zakończy się uzgodnieniami, to w ostatnim tygodniu kwietnia, mielibyśmy Radę Ministrów, i w drugiej połowie maja albo w połowie maja, jak zakładam trwałyby prace w parlamencie. Podpis prezydenta w takim wariancie również optymistycznym to jest druga połowa czerwca. Tak trzeba by było na to patrzyć. Patrząc na ten kalendarz działań, będzie to oznaczać, że na moment wejścia w życie dyrektywy, czyli na dzień 9 maja, nie będziemy mieli uchwalonych przepisów krajowych, natomiast ten przedział prawny, kiedy wciąż będzie obowiązywało polskie prawo, jak przewidujemy, będzie trwał jakiś miesiąc – półtora miesiąca czasu. Jeśli chodzi o informacje na ten temat, to myślę również, że warto by było powiedzieć, jak Polska pozycjonuje się na tle innych państw, jeśli chodzi o implementację dyrektywy.

Jakkolwiek nie jesteśmy zadowoleni z tego, że wszystko wskazuje na to, że tego terminu 9 maja nie uda się dotrzymać, to jednak z perspektywy porównania, jak to wygląda w poszczególnych krajach unijnych, i tak trzeba powiedzieć, że jesteśmy wciąż w czele procesu zaawansowania, jeżeli chodzi o legislację. W tym momencie, jeżeli chodzi o kraje unijne, przyjęte ustawy mają Niemcy, Francja i Czechy, w parlamencie ustawy są w Finlandii, Słowacji i Chorwacji. Kolejnych 8 państw, w tym Polska, jest mniej więcej na etapie rady ministrów. Natomiast kolejnych 5 państw to są jeszcze konsultacje międzyresortowe. 5 kolejnych państw to jest nawet jeszcze przed konsultacjami publicznymi, a najmniej zaawansowany proces, czyli *de facto* jakieś warianty robocze ustawy, to są jeszcze kolejne 5 państw – Węgry, Dania, Luksemburg, Rumunia i Słowenia. To nie jest do końca pocieszające, ale – jak mówię – z perspektywy porównywania otoczenia w państwach członkowskich jesteśmy mniej więcej w środku stawki tych państw, jeśli chodzi o stan zaawansowania prac nad ustawą.

Proszę państwa, teraz oddałbym głos panu dyrektorowi Szyszce, który opisze schemat, który w tym momencie wyświetliłem na ekranie, zatrzymując się nad tymi poszczególnymi elementami. Oczywiście to jest ostatni slajd i ostatnia część naszej prezentacji, więc zakładam, że jeśli coś jeszcze po niej będzie niejasne albo będzie wymagało dyskusji, to oczywiście jesteśmy do dyspozycji. Proszę, panie dyrektorze.

**Dyrektor Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji Andrzej Szyszko:**

Dziękuję. Panie przewodniczący, Wysoka Komisjo, tak, jak wspomniał pan minister, ten slajd został podzielony na pewne takie elementy. Zacznę opowiadać od lewej strony. Tak, jak pan minister był uprzejmy powiedzieć, kolorem magentowym mamy zaznaczony CSIRT poziomu krajowego, na który będą się składały de facto CSIRT-y, czyli te zespoły reagowania na incydenty komputerowe właśnie w sferze wojskowej, czyli MIL-CERT, w sferze administracji publicznej CERT.GOV.PL umieszczony w Agencji Bezpieczeństwa Wewnętrznego i oczywiście CERT Polska zlokalizowany w Państwowym Insty-

tucie Badawczym Naukowej Akademickiej Sieci Komputerowej. Z CSIRT-em poziomu krajowego, czyli *de facto* z tymi trzema CSIRT-ami, będzie współpracowała prokuratura oraz policja przy rozwiązywaniu incydentów. Trzy CSIRT-y są ze sobą połączone celem pokazania, że po prostu będą miały jeden system informatyczny opisany w projekcie ustawy. Dzięki temu systemowi te CSIRT-y będą wymieniały informacje między sobą oraz interesariuszami ustawy. W razie, kiedy incydent zgodnie z projektem ustawy będzie tak zwanym incydentem krytycznym, zostanie powołany zespół do spraw incydentów krytycznych, nad którym – że tak powiem – pieczę będzie sprawowało Rządowe Centrum Bezpieczeństwa, a w razie dalszej eskalacji takiego incydentu na przykład na poziom transgraniczny, będzie uruchamiany Rządowy Zespół Zarządzania Kryzysowego. Sieć... Może inaczej. CSIRT-y będą współpracowały w ramach sieci CSIRT-ów z innymi swoimi odpowiednikami w państwach członkowskich Unii Europejskiej celem właśnie zarządzania incydentami teleinformatycznymi, które są właśnie poważne, krytyczne i które są przede wszystkim transgraniczne, czyli obejmują przynajmniej 2 państwa członkowskie. Ze współpracą międzynarodową jest związany także pojedynczy punkt kontaktowy, który będzie przekazywał do sieci CSIRT-ów zebrane informacje, ale takie bardziej sumaryczne. Pojedynczy punkt kontaktowy, który według projektu ustawy będzie umieszczony w Ministerstwie Cyfryzacji, będzie współpracował w ramach grupy współpracy oraz z innymi podmiotami tego typu, jak pojedyncze punkty kontaktowe w państwach członkowskich tak, aby zapewnić spójny przepływ informacji pomiędzy wszystkimi państwami członkowskimi.

Po środku slajdu są umieszczone sektorowe zespoły reagowania oraz podmioty świadczące usługi cyberbezpieczeństwa. Według projektu ustawy takie sektorowe zespoły reagowania mogą być powoływane w sektorach, które są *de facto* tożsame z działami administracji rządowej, w takim celu, aby ułatwić zarządzaniem incydentem pomiędzy podmiotem, gdzie taki incydent miał miejsce, a CSIRT-em, który będzie *de facto* na samej górze, czyli tym CSIRT-em umieszczonym po lewej stronie slajdu. Jeżeli chodzi o podmioty świadczące usługi cyberbezpieczeństwa, to są inne podmioty typowo komercyjne, które po prostu mogą świadczyć dla tak zwanych operatorów usługi kluczowej swoje usługi z zakresu cyberbezpieczeństwa, czyli na przykład chociażby doradzanie. Po prawej stronie slajdu mamy w szarych prostokątach wymienione działy administracji, ale z punktu widzenia dyrektywy, o której pan minister był uprzejmy powiedzieć – dyrektywy NIS. Następnie są organy właściwe, które będą dokonywały szeregu czynności opisanych w projekcie ustawy wobec tych podmiotów, które są tutaj wymienione. Dla przykładu więc minister energii będzie organem właściwym dla całego sektora energii, a minister cyfryzacji wraz z ministrem obrony narodowej w zależności od podmiotu będzie organem właściwym dla infrastruktury cyfrowej.

Oddzielnym blokiem tutaj na samym dole po prawej stronie są przedsiębiorcy telekomunikacyjni. Dla nich takim właściwym organem będzie Urząd Komunikacji Elektronicznej. I mamy tutaj oczywiście zawartych obywateli i administrację publiczną. Administracja publiczna w tym przypadku jest bardzo szeroko rozumiana, zarówno jako administracja samorządowa, jak i cała administracja publiczna, która nie jest ujęta po prawej stronie w tych sektorach związanych z dyrektywą NIS. Z kolei na samej górze tak po środku mamy pełnomocnika rządu oraz Kolegium do Spraw Cyberbezpieczeństwa. Za chwilę również opowiem dokładnie, czym się będą te dwa podmioty charakteryzowały. Jeżeli natomiast chodzi o tę samą administrację publiczną jako taką, to przede wszystkim w projekcie ustawy zawarliśmy informację, że każdy podmiot publiczny, który wcześniej był wyszczególniony na slajdach, będzie zobowiązany do wyznaczenia osoby, która będzie odpowiedzialna przede wszystkim za kontakty z podmiotami całego Krajowego Systemu Cyberbezpieczeństwa, czyli *de facto* w każdej jednostce administracji będzie wyznaczony taki jeden człowiek, żeby było wiadomo, z kim trzeba się kontaktować, jeżeli zaistnieje incydent. Z kolei wszystkie jednostki samorządu terytorialnego mogą wyznaczyć osobę odpowiedzialną za utrzymywanie takich kontaktów, ale według projektu ustawy może to być również osoba wyznaczona na przykład chociażby dla kilku gmin.

Każdy podmiot publiczny już bardziej rozumiany jako administracja rządowa musi zapewnić zarządzanie incydentem w swojej własnej jednostce. Musi zgłaszać ten incy-

dent niezwłocznie. Według dyrektywy i tak samo według ustawy na zgłoszenie takiego incydentu są 24 godziny od momentu jego wykrycia. Taki incydent musi być zgłoszony do jednego z tych CSIRT-ów, które są wymienione po lewej stronie slajdu, ewentualnie do sektorowego zespołu reagowania. W każdym razie trzeba w ciągu 24 godzin taki incydent zgłosić. Jeżeli taki incydent będzie na przykład zgłoszony później niż po 24 godzinach, to według dyrektywy i ustawy na takiego operatora usługi kluczowej będzie można nałożyć karę finansową. Następnie tak, jak wspomniałem, ten incydent musi być zgłoszony i nie może być takiej sytuacji, że podmiot po prostu zgłasza incydent i o nim zapomina – on cały czas zarządza w swojej własnej jednostce takim incydentem. W związku z tym w projekcie ustawy również są opisane te obowiązki, żeby taki podmiot – powiem kolokwialnie – nie zapominał o tym, że jednak również ma pewne określone obowiązki wobec własnych pracowników i usług, które będzie świadczył na zewnątrz. To jeżeli chodzi o obowiązki tych podmiotów.

Natomiast w zakresie pełnomocnika rządu do spraw cyberbezpieczeństwa, to ten pełnomocnik według projektu ustawy ma co do zasady koordynować wszystkie działania dotyczące zapewnienia cyberbezpieczeństwa Rzeczypospolitej Polskiej. Pełnomocnikiem ma być sekretarz lub podsekretarz stanu. W projekcie ustawy nie wskazuje się, w którym *de facto* ministerstwie będzie ten sekretarz lub podsekretarz stanu wskazany. Ma on podlegać Radzie Ministrów. Projekt ustawy określa również bardzo szczegółowo, co konkretnie pełnomocnik ma wykonywać. Przede wszystkim ma dokonywać analizy i oceny funkcjonowania krajowego systemu cyberbezpieczeństwa, sprawować nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa i opiniować projekty aktów prawnych.

Ponadto, jak pan minister był uprzejmy jeszcze powiedzieć, zostanie powołane Kolegium do Spraw Cyberbezpieczeństwa jako organ opiniodawczo-doradczy Rady Ministrów. On jest tutaj pokazany na slajdzie w prawym górnym rogu. Co do zasady takie kolegium ma wyrażać opinie w takich sześciu najważniejszych sprawach. Wymienię tutaj takie, które są na pierwszym miejscu, czyli kierunki i plany na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa czy wykonywanie... w zasadzie kontrolowanie CSIRT-ów oraz sektorowych zespołów cyberbezpieczeństwa, czy właściwie wykonują powierzone im zadania zgodnie z szeroko pojętymi kierunkami i planami na rzecz przeciwdziałania szeroko rozumianym zagrożeniom cyberbezpieczeństwa. Na razie dziękuję.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję. Czy ze strony Ministerstwa Spraw Wewnętrznych jest wola uzupełnienia tych informacji?

**Dyrektor Departamentu Teleinformatyki Ministerstwa Spraw Wewnętrznych i Administracji Dariusz Bogucki:**

Szanowny panie przewodniczący, szanowni państwo, chcieliśmy nie tyle odnieść się do ustawy, ponieważ jest to ustawa prowadzona przez Ministerstwo Cyfryzacji, co tak naprawdę zreferować państwu informację na temat działalności państwa i podmiotów podległych ministrowi właściwemu do spraw wewnętrznych – zgodnie z upoważnieniem Komisji – na temat tego, co robimy. A więc nie warstwa prognostyczna, tylko tak naprawdę, co się dzieje w resorcie i z czym walczymy. Nie wiem więc, czy...

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Tak, bardzo proszę. Chodzi o to, żebyśmy w momencie rozpoczęcia dyskusji, zapoznali się już z tymi dwoma wystąpieniami. Bardzo proszę.

**Dyrektor Departamentu Teleinformatyki MSWiA Dariusz Bogucki:**

Dziękuję bardzo. Szanowni państwo, tak, jak powiedziałem trochę żartem, to jest tak, że resort właściwy do spraw wewnętrznych i administracji na bieżąco styka się z tymi zagrożeniami, które określa się cyberprzestępstwami. Z tymi zagrożeniami spotyka się ministerstwo jako urząd. Z tymi zagrożeniami spotykają się podległe ministrowi służby – Policja czy Straż Graniczna. To są zdarzenia, które nie są hipotetyczne, które dzieją się naprawdę. Cyberataki zdarzają się naprawdę – próby włamania się do systemów, pozyskania pewnej wiedzy tudzież załatwienia sobie, zrobienia czegoś. Mogę powiedzieć

żartem, że odnotowaliśmy jakiś czas temu próbę włamania się przez fire wall do ministerstwa w celu wyrobienia sobie dowodu osobistego. Ktoś chciał sobie wyrobić fałszywy dowód, natomiast robił to wyjątkowo nieudolnie.

Działania resortu można podzielić na takie cztery grupy. Pierwsza to są działania organizacyjno-prawne, druga to ściganie cyberprzestepczości, czym zajmuje się głównie Biuro do Spraw Zwalczania Cyberprzestępczości Policji, trzecia to są bardzo istotne działania o charakterze profilaktycznym, nie tylko informacyjno-promocyjnym, ale również profilaktycznym, i współpraca z innymi podmiotami. Jeśli chodzi o działania organizacyjne, to można powiedzieć, że zaczęliśmy działać od własnego podwórka. Pewne kwestie zostały uporządkowane. Wdrożono system zarządzania bezpieczeństwem informacji. Jest powołany pełnomocnik ministra do spraw cyberbezpieczeństwa. Co więcej, aktywnie działają zespoły reagowania na incydenty komputerowe – POL-CERT, który funkcjonuje w Policji, i KORUND, który funkcjonuje w Straży Granicznej. One działają od 2015 r. i funkcjonują aktywnie. To, nad czym pracujemy, a zasadniczo zaczęliśmy prace także w świetle projektu ustawy i projektu dyrektywy NIS, to jest to, żebyśmy utworzyli sektorowy SOC czy sektorowy CSIRT. Jest to zadanie o tyle trudne, że mamy dwa funkcjonujące – i to dobrze funkcjonujące – zespoły reagowania, więc nie chcemy budować jakiejś sztucznej czapki, natomiast chcemy zbudować coś, co da pewną wartość dodaną. Natomiast tak, jak mówiłem, jeśli chodzi o kwestię cyberbezpieczeństwa, to aktywnie się z tym zmagamy. To są zdarzenia, które się dzieją, z którymi mamy do czynienia.

Tutaj, nawiasem mówiąc, oczekując na wejście na posiedzenie Komisji, toczyliśmy dyskusję, bo w tej chwili w Stanach Zjednoczonych jest bardzo głośna sprawa data-mining który robił Facebook. Jest to taka rzecz, która totalnie ucieka naszej uwadze. Zasadniczo mówi się o niej na portalach specjalistycznych i być może prasa specjalistyczna o tym mówi. Otóż tak na dobrą sprawę pan Mark Zuckerberg przyznał się do dwóch rzeczy; jednej, że przetwarzał dane osobowe. Jest to pewnym wstrząsem dla Amerykanów, że można z danych osobowych…, bo tam jest inna kultura, jeśli chodzi o przetwarzanie danych, natomiast to, że okazało się, że w systemie Facebook istnieje od bardzo, bardzo dawna – pewnie od jakichś początkowych wersji – pewna podatność, która pozwalała uzyskać dużo więcej danych, niż teoretycznie można było wyciągnąć z tego Facebooka tak kaskadowo, czyli nie tylko o tych osobach, o które pytaliśmy, ale również o tych, którzy byli znajomymi, znajomymi i tak dalej. I teraz tak naprawdę jest pytanie, czy to jest podatność, o której wszyscy zapomnieli, bo ona dotyczy jakiejś bardzo starej początkowej wersji Facebooka, czy to jest tak, że było o tym wiadomo, ale wszystkim to pasowało, ponieważ za megabajty danych były płacone pieniądze? I to jest również tak naprawdę jądro tego, z czym – można powiedzieć – w cyberbezpieczeństwie stykamy się, że bardzo często musimy zacząć od własnego podwórka, żeby właśnie takich podatności, o których już nikt do końca nie pamięta, skąd się wzięły, nie było. My to robimy.

To, co mogę jeszcze dodać, ponieważ o tym jest szerzej tutaj w szczegółowym opracowaniu, natomiast to są bardzo aktywne działania w zakresie podnoszenia poziomu świadomości, dlatego że same działania, same zabezpieczenia nic nie dadzą, jeżeli po drugiej stronie mamy użytkowników, którzy są nieświadomi, dla których to jest kwestia wyimaginowana albo która dzieje się za oceanem. Te rzeczy dzieją się tutaj i dzieją się w sposób aktywny, dzieją się naprawdę. Dodam jeszcze tylko tyle, że we wszystkich tych działaniach współdziałamy aktywnie z zespołem CERT.GOV.PL, zarówno Straż Graniczna jak i Policja.

Ja tylko w skrócie streściłem to bardzo obszerne sprawozdanie, które państwo posłowie dostali, więc to na razie tyle. Dziękuję bardzo.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję bardzo. Proszę państwa, rozumiem, że ze strony rządowej to jest informacja, która na tym etapie jest pełna, tak?

Bardzo proszę, otwieram dyskusję. Bardzo złożona problematyka cyberbezpieczeństwa. W zasadzie jest to nowa problematyka. Jeżeli pomyślimy o takim systemowym ujęciu, kto po stronie rządowej byłby liderem, to widzimy wyraźnie, że wychodzi na to, że Ministerstwo Cyfryzacji jest tutaj liderem. Stąd ten referat ze strony pana dyrektora

z Ministerstwa Spraw Wewnętrznych i Administracji jest wystąpieniem uzupełniającym. Mamy również dokument. Bardzo proszę, czy są pytania ze strony państwa członków Komisji?

Ja chciałbym zapytać pana ministra o taką rzecz. Poczta Polska została wybrana jako narodowy operator cyfrowy i świadczy różnego rodzaju usługi cyfrowe na poziomie narodowym. Jak na przykład patrzę na tę tabelkę, to w którym z tych kwadratów należy dostarczyciela usług cyfrowych umiejscowić? Czy tam, gdzie są przedsiębiorcy telekomunikacyjni? Nie bardzo to widzę. A tutaj w tej pionowej, gdzie jest infrastruktura cyfrowa, dostawy usług cyfrowych? Czy na tym poziomie umieścilibyśmy Pocztę Polską?

**Dyrektor Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji Andrzej Szyszko:**

To znaczy, poczta jest wyznaczonym operatorem dla usług pocztowych. Jeśli miałaby pełnić rolę operatora usług cyfrowych, to wtedy faktycznie byłaby w obszarze infrastruktury cyfrowej. Jeśli chodzi o pocztę, to takiego segmentu wprost nie wyróżniamy, czyli jest tutaj jakby elementem administracji publicznej.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Wchodząc na pierwszą stronę Poczty Polskiej czytamy: „Narodowy operator cyfrowy", i jest tutaj informacja... Teraz pod pojęciem usług pocztowych zanika wszystko, co tradycyjne, co wyobrażamy sobie o poczcie, a za chwilę będziemy mieli praktycznie w 99% przeniesione do świata cyfrowego.

**Dyrektor Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji Andrzej Szyszko:**

Ja bym nie był takim optymistą, panie przewodniczący, ale poniekąd jako Ministerstwo Cyfryzacji też mamy taki cel, ale głównie z perspektywy ułatwień dla obywateli i efektywności kosztowej, żeby te usługi zamieniać z postaci fizycznej do postaci cyfrowej. Natomiast narodowy operator cyfrowy jest pewną – powiedziałbym – taką figurą stylistyczną, którą poczta używa, mówiąc o swoich aspiracjach. Nie jest wykluczone, że tak się stanie, ale wtedy faktycznie będzie w obszarze usług cyfrowych jako dostawca usługi zaufania związanej na przykład z dostarczeniem listu elektronicznego poleconego.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Rozumiem, że chodzi o uzupełnienie mojego pytania?

**Poseł Jerzy Polaczek (PiS):**

Tak, ja chciałbym to uszczegółowić, bo również zamieniliśmy na ten temat z panem przewodniczącym dwa zdania i ja tylko chciałbym przypomnieć, że Ministerstwo Cyfryzacji podpisało 31 sierpnia 2016 r. umowę czy porozumienie z Pocztą Polską i platformą pocztowych usług cyfrowych znaną pod nazwą Envelo, której istotą jest budowa oficjalnego kanału komunikacji obywatela z państwem. Jest to wpisane również w strategię poczty jako – powiedziałbym – naturalny element przede wszystkim z jednej strony rynkowy dla Poczty Polskiej, bo przecież tutaj za chwilę możemy mieć zupełnie inną sytuację za 2–3 lata, jeżeli chodzi o – mówiąc wprost – zwijanie wszelkiego rodzaju usług w cudzysłowie analogowych. To jest bardzo zasadne pytanie, jak ten aspekt kontaktu obywatela – jedynego oficjalnego kontaktu z państwem poprzez ten kanał jedynej platformy cyfrowej obsługującej różnego rodzaju – powiedziałbym – usługi publiczne, będzie funkcjonował w tym aspekcie, który referował pan minister, 4,5 tys. placówek pocztowych w Polsce. To jest takie – powiedziałbym – uzupełnienie pytania pana przewodniczącego. To jest otwarte pytanie do ministerstwa o ewentualną analizę tego problemu. Dziękuję.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję bardzo. Trzy pytania i może potem odpowiedzi, dobrze? Możecie państwo spokojnie sobie zanotować te problemy, które podnosimy. Pan przewodniczący Wójcik.

**Poseł Marek Wójcik (PO):**

Dziękuję bardzo. Ja mam akurat trzy pytania, ale trochę też zaintrygował mnie pan reprezentujący Ministerstwo Spraw Wewnętrznych i Administracji, mówiąc na przykład o próbie wyrobienia dowodu osobistego, bo rozumiem, że w tym obszarze cyberbezpie-

czeństwa państwa są różne sprawy. Na pewnych poziomach jest to problem obywatela – o to też za chwilę będę pytał – ale na pewnym poziomie to jest problem państwa, kiedy ktoś na przykład próbuje się włamać do jakiegoś systemu informatycznego. Pan akurat podał taki przypadek. Jakie państwo widzicie zagrożenia, jeżeli chodzi o bezpieczeństwo państwowych systemów informatycznych? Czy to jest to, że te systemy są niewydzielone na przykład, czy jest jakiś brak kultury użytkowania przejawiający się tym, że ktoś na przykład podłącza do tych systemów jakieś niesprawdzone urządzenia? Skąd tak naprawdę te próby ataku pochodzą? Jakie główne zagrożenia państwo rozpoznaliście i jakie są główne problemy tych państwowych systemów?

Drugie pytanie to pytanie z perspektywy szarego użytkownika. Ja rozumiem, że prezentacja bardzo dobrze wygląda, natomiast chciałbym wiedzieć, gdzie ma się zgłosić taki przeciętny Kowalski, który padnie ofiarą jakiegoś przestępstwa w internecie, na przykład takiego przestępstwa ransomware'owego, czyli blokady oprogramowania na komputerze, które może zostać odblokowane po wpłaceniu jakieś kwoty okupu. Czy jest sens, żeby taka osoba zgłaszała taką sprawę na jakimś najbliższym swoim dzielnicowym komisariacie Policji, czy też taka osoba powinna się kontaktować z kimś innym po to, żeby ktoś jej po prostu pomógł? Czy takie zgłoszenie się do komisariatu znajdującego się najbliżej miejsca zamieszkania w ogóle cokolwiek pomaga, czy lepiej wystąpić do jakiegoś centrum, które jest w stanie w takich sytuacjach pomóc?

I trzecia rzecz. To już dotyczy właściwie mojego osobistego doświadczenia, dlatego że sposób funkcjonowania w internecie również powoduje pewne kłopoty dla administracji publicznej, dla sądownictwa, dla wymiaru sprawiedliwości. Zresztą ja sam kilka lat temu padłem ofiarą jakiegoś nieuczciwego kontrahenta w internecie. Kupowałem jakiś przedmiot i bardzo szybko udało mi się skorzystać z jakiegoś programu ochrony kupujących. Uzyskałem zwrot pieniędzy, więc właściwie byłem zadowolony z tej sprawy, natomiast później widziałem, że jeszcze przez 3 czy 4 lata toczyła się sprawa przeciwko nieuczciwemu przedsiębiorcy, który miał siedzibę bodajże w Olsztynie, ale specyfika handlu w internecie jest taka, że poszkodowani byli po prostu na terenie całego kraju, więc to były niekończące się wezwania do różnego rodzaju stawienia się przed policją, sądem. Na szczęście były one wykonywane w ramach pomocy prawnej, więc jeździłem w obrębie własnego miasta, a nie po całym kraju, choć chyba takie wezwanie w tym przypadku do Olsztyna też miałem, a jestem ze Śląska, żeby to obrazowo przedstawić. Pytanie, czy tutaj nie są potrzebne jakieś zmiany prawa dotyczącego prowadzenia postępowań w takich sprawach? Czy rzeczywiście ta praktyka prokuratury przesłuchiwania właściwie każdego poszkodowanego w sytuacji, kiedy takich poszkodowanych, którzy zgłosili swoją szkodę, są prawdopodobnie setki, a często tysiące… To musi powodować ogromne koszty po stronie organów ścigania, po stronie policji, po stronie prokuratury i po stronie sądownictwa. To tyle. Dziękuję bardzo.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję bardzo. Jeszcze pan przewodniczący, bardzo proszę.

**Poseł Jerzy Polaczek (PiS):**

Jeszcze raz pozwolę sobie zabrać głos, bo czuję się trochę wywołany niejako przy okazji tej prezentacji ministerstwa. Chcę skorzystać z naturalnej okazji, żeby jeszcze raz doprecyzować istotę problemu. Mianowicie, w obszarze tego schematu, który tutaj wszyscy widzimy, brak takiego elementu, jakim jest – można powiedzieć – odpowiedź czy brak odpowiedzi na pytanie: Czy poprzez gwałtowny rozwój usług cyfrowych w relacjach: państwo – obywatel, poprzez operatora wyznaczonego, jakim jest Poczta Polska… To pytanie zasadnicze polega na tym, czy będzie to wykonywała platforma usług cyfrowych, która już jest czy miała być budowania, czy jest tutaj – powiedzmy – naturalna kontynuacja tego procesu, czy później ten scenariusz może rozwinąć się w taki sposób, że zostanie ten istotny z punktu widzenia obywatela segment powierzony podmiotom zewnętrznym. Przecież mamy w takich państwach, jak Francja czy Estonia, bardzo znaczący – powiedziałbym – udział e-skrzynki, e-doręczeń jako naturalny proces obiegu informacji. Nie wiem, mówiąc tak symbolicznie, można zawiadomienie z urzędu administracyjnego otrzymać na swój zaufany profil w ciągu jednego dnia. To są zupełnie – powiedziałbym

– zasadnicze zmiany. Chodzi o rozstrzygnięcie z punktu widzenia państwa i tego zagadnienia, które jest dzisiaj omawiane, czy skutkiem ewentualnych jakichś zaniedbań nie będzie pozbawienie się przez państwo wpływu, który wróci z drugiej strony ze zdwojoną siłą za kilka lat? Dziękuję.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Bardzo proszę, panie ministrze.

**Podsekretarz stanu w MC Karol Okoński:**

Dobrze, ja po kolei odniosę się do tych pytań. Może faktycznie najpierw zacznę od pytania pana przewodniczącego Polaczka dotyczącego poczty. To co mogę powiedzieć, to to, że jest tak, że faktycznie rozmawiamy. Potwierdzam to, że trwają rozmowy i uzgodnienia z Pocztą Polską i z Ministerstwem Infrastruktury, zmierzające do tego, żeby przygotować model działania, który będzie uwzględniał wszystkie aspekty wydanych już pieniędzy, jak na przykład na platformę Envelo, czy kwestie wydajności i bezpieczeństwa, ale również możliwości wynikające z otoczenia prawnego. I tu bardzo prawdopodobnym wariantem jest faktycznie to, że zostanie zdefiniowane – ale to są zmiany prawne, które muszą być jeszcze zaprojektowane szczegółowo – pojęcie narodowego operatora cyfrowego. Pozostanie jedynie kwestia, w jaki sposób on będzie wybrany – czy będzie go można wskazać wprost w ustawie, czy będzie musiał być wyłoniony w przetargu, tak jak jest wyłaniany na okres 10 lat operator wyznaczony dla usług pocztowych. Dyrektywa eIDAS, która w tym momencie obowiązuje, jeżeli chodzi o usługi zaufania – rejestrowany list polecony elektroniczny jest jedną z takich usług – nakłada obowiązek konkurencyjnego sposobu uregulowania tego rynku, więc jak to finalnie się zakończy, jest jeszcze – jak mówię – elementem analiz. Faktycznie jest tak, że w niektórych państwach, jak w Czechach czy we Francji, ci operatorzy byli po prostu wskazani przez państwo, to znaczy, tym operatorem usług cyfrowych takiego elektronicznego listu poleconego była poczta z danego kraju, natomiast było to jeszcze przed dyrektywą eIDAS. Są też takie kraje, jak Dania, która po prostu ogłosiła przetarg, który wygrała poczta duńska. Są też mieszane rozwiązania, jak na przykład funkcjonujące we Włoszech. To, co mogę więc potwierdzić, to jest to, że zdając sobie sprawę z powagi usługi i z poniesionych inwestycji, trwają prace, które w jakiś sposób pomogą wykorzystać potencjał Poczty Polskiej. Potwierdzam to, natomiast nie mogę w tym momencie przesądzić dokładnego scenariusza.

Jeżeli chodzi o bezpieczeństwo systemów informatycznych, to może pan dyrektor Bogucki będzie chciał jeszcze uzupełnić. Ja tylko powiem ze swojej strony, że jeżeli chodzi na przykład o wydanie dowodu, to włamanie z zewnątrz jest praktycznie niemożliwe, bo to jest po prostu sieć odseparowana, więc ktoś musiałby się jakoś włamać i – że tak powiem – połączyć galwanicznie z tamtą siecią. Natomiast generalnie ten poziom bezpieczeństwa systemów wynika też z przepisów nakładanych na podmioty, również ze względu na wymogi prowadzenia polityki bezpieczeństwa. System rejestrów państwowych posiada tę politykę. Jest ona zresztą teraz aktualizowana w wyniku również pewnych uwag, które były zgłoszone przez Najwyższą Izbę Kontroli.

Jeżeli chodzi o przestępstwa wobec obywatela, to pamiętajmy, że... To znaczy, trzeba zwrócić uwagę na to, że dyrektywa NIS generalnie przede wszystkim stawia na zapewnienie bezpieczeństwa państwa jako takiego z perspektywy jego ciągłości działania i bezpieczeństwa, a więc kładzie nacisk na te podmioty, które są krytyczne z punktu widzenia tego, żeby państwo działało w tym świecie wirtualnym. Ona więc wprost nie reguluje, nie nakłada ani obowiązków, ani dodatkowych praw na konkretnego obywatela z perspektywy tego, jak on korzysta z internetu. Z perspektywy przestępstw typu ransomware *de facto* wchodzą w grę obecne przepisy i będą nadal wchodziły dotyczące tego, że obywatel ma możliwość czy obowiązek zgłosić taką sprawę albo na Policję albo może również szukać pomocy w NASK poprzez pewien rodzaj... To znaczy NASK informuje i publikuje informacje o tych zagrożeniach, więc można też jakby śledzić w ten sposób i przygotować się do tych zagrożeń oraz szukać ewentualnie porady z perspektywy tych działań, które mogą być podjęte, natomiast on nie nakłada w tym momencie na dostawców usług jakichś obowiązków w stosunku do obywatela, chyba że to jest włamanie, które zagra-

żałoby po prostu całemu państwu, biorąc pod uwagę jego skalę. Wtedy ta koordynacja pomiędzy podmiotami wręcz czasami na poziomie europejskim jest po prostu niezbędna.

Jeśli chodzi o oszustwa w handlu elektronicznym, to jest to trochę analogiczna sytuacja, chyba że mielibyśmy do czynienia z jakimś włamaniem, z jakąś masową akcją, która naraża dużą liczbę użytkowników. Dyrektywa wprowadza pojęcie internetowej platformy handlowej, mając na myśli po prostu platformy typu – powiedzmy, że to będzie doprecyzowane w rozporządzeniu, ale możemy sobie wyobrazić –na przykład Allegro. Jakieś włamanie do Allegro, które mogłoby zagrozić masowej liczbie obywateli faktycznie byłoby objęte działaniem państwa. Natomiast to byłby po prostu ten kluczowy operator cyfrowy. On zostałby wskazany i na niego nałożone byłyby dodatkowe obowiązki.

To tyle z mojej strony, jeśli chodzi o odpowiedzi.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję bardzo.

**Dyrektor Departamentu Teleinformatyki MSWiA Dariusz Bogucki:**

Gwoli uzupełnienia, to jest rzeczywiście tak, jak powiedział pan minister Okoński, że akurat system do wydawania dowodów i paszportów jest galwanicznie odseparowany, ta część produkcyjna oczywiście, od ogólnodostępnej sieci internet. Wobec tego, próbując wejść przez link do platformy ePUAP, gdzie składa się te wnioski, próbując tam wpisać admin, admin, bo być może się trafi, to na pewno tą drogą do tego systemu nikt się nie dostanie.

Jeżeli natomiast chodzi o bezpieczeństwo, dokładnie tak, jak pan minister powiedział, nie pamiętam, który z tych nawróconych hakerów – to powiedział chyba Mytnik – że nie ma systemów bezpiecznych, są tylko lepiej lub gorzej zabezpieczone. Również w takich systemach, które są teoretycznie totalnie od wszystkiego odcięte – nie zapominajmy o tym – istnieje pewna metoda, która jest bardzo skuteczna wycieku informacji, czyli kret – człowiek, który jest w środku, który, jeżeli ma możliwość, bo ktoś zapomni o tym, żeby zablokować port USB czy nagrywarkę DVD, zgra takie dane i wyciągnie na zewnątrz. Ale to też jest kwestia, że jeżeli chodzi o zabezpieczenia, nie mówimy tylko o samej technice, ale też o kwestiach organizacyjnych i o kwestiach bezpieczeństwa. To jest cały system. Nie można jednego elementu rozpatrywać w oderwaniu od innych elementów.

Natomiast pan przewodniczący powiedział o tym naciągaczu i że później był pan ciągany. Ja nie, ale w rodzinie też ktoś doświadczył takiej sytuacji. Być może to ta sama osoba, ale też musiał się stawiać w kilku miejscach na przesłuchanie. To dotyczyło zakupu jakiejś rzeczy dla dziecka. To jest kwestia raczej wymiaru sprawiedliwości, a nie organów ścigania, chyba że on rzeczywiście w kilku miejscach funkcjonował.

**Poseł Marek Wójcik (PO):**

Zależy mi na odpowiedzi na pytanie, co może zrobić – bo ja rozumiem, dyrektywa dyrektywą, ale temat jest jakby troszeczkę szerszy niż sama dyrektywa – przeciętny Kowalski, któremu zablokowano po prostu komputer, który chciałby to zgłosić na policję i oczekuje, że to nie będzie tylko tak, że on zawiadomi policję, ale tak, że ta policja mu pomoże. Czy w takiej sytuacji jest sens, żeby on zgłaszał to w ogóle, żeby szedł na przykład na swój komisariat na osiedlu, czy też powinien próbować w jakiś sposób jakąś inną jednostkę czy jakąś inną strukturę policji poinformować o swoim problemie i tam poszukać pomocy?

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Pan poseł Mirosław Suchoń, proszę.

**Poseł Mirosław Suchoń (N):**

Bardzo dziękuję. Panie przewodniczący, panie ministrze, Wysoka Komisjo, mam pytania – powiedziałbym – wynikające również z informacji, które państwo przekazali, bo rzeczywiście, jeżeli chodzi o dokumentowanie procedur, muszę powiedzieć, że Polacy są mistrzami. To znaczy, my mamy naprawdę doskonałe procedury i wszystko bardzo dobrze przemyślane. Gorzej jest później z ich przestrzeganiem i weryfikacją przestrzegania tych procedur przez osoby zobowiązane, co jest oczywiście jedną – tak uważam – z najważniejszych podatności systemów w Polsce na różnego rodzaju incydenty. Myślę,

że to dotyczy również innych systemów na całym świecie. Generalnie jednak, jeżeli chodzi o dokumentację i biurokrację, to powiedziałbym, że przodujemy w tym względzie, co nie znaczy, że przestrzegamy. I teraz ważna jest weryfikacja w związku z tym przestrzegania tych wszystkich procedur, stosowania tych wszystkich procedur. Moje pytanie zasadniczo zmierza do uzyskania takiej informacji, czy istnieje coś takiego, jak standardy weryfikacji stosowania procedur? Czy jest coś takiego, co państwo rekomendują, być może w formie jakichś obowiązujących wytycznych, co w pewien sposób tym kierownikom jednostek nakazywałoby podejmowanie systematycznych, kompleksowych weryfikacji takich procedur? Interesują mnie również budżety związane z takimi pełnomocnikami, akurat w ministerstwie, do spraw bezpieczeństwa w cyberprzestrzeni. Interesuje mnie kwestia systemowa, czy jeżeli państwo tworzą tego rodzaju stanowiska, to jednocześnie ci pełnomocnicy mają wyznaczony swój budżet czy też muszą poruszać się w ramach budżetu jednostki, za każdym razem występując o zgodę przełożonego, kierownika jednostki? To jest dosyć istotna sprawa, bo zazwyczaj jest tak, że wyznacza się pełnomocników. Oni mają jakieś kompetencje, natomiast jeżeli chodzi o finansowanie działań, które w sferze bezpieczeństwa kosztuje i – to musimy sobie jasno powiedzieć – finansowanie szkoleń personelu, co kosztuje, to tutaj jest już gorzej. W związku z tym czy tego rodzaju osoby mają budżety, czy muszą się poruszać w ramach budżetu i zawsze za zgodą, bo nie mają jakiejś decyzyjności? Czy w tej materii również istnieją jakieś standardy postępowania?

Ważna rzecz, którą poruszono właśnie w stanowisku ministerstwa administracji. Otóż w cyberprzestrzeni te zagrożenia również stanowią kwestię wojen dezinformacyjnych. Ja uważam, że to jest generalnie bardzo poważny problem w Polsce i – myślę – mało doceniany, ale interesuje mnie sprawa, w jaki sposób zarówno Ministerstwo Cyfryzacji, ale również administracji podchodzi do tego tematu? Dziwię się, że nie ma przedstawiciela MON, bo jest to jeden – powiedziałbym – z takich obszarów, w którym MON również miałby coś do powiedzenia. Chciałbym jednak zapytać wprost, czy istnieje jakakolwiek forma analizy treści, które pojawiają się w mediach, na przykład pod artykułami, które dotyczą istotnych interesów naszego państwa? Pytam o to dlatego, że komentarze w internecie – zresztą myślę, że to jest wiedza, która coraz częściej jest powszechna dla coraz większej grupy osób, ale niestety niewystarczającej – mogą stanowić pewnego rodzaju formułę takiego miękkiego nacisku i wpływania na opinię publiczną niekoniecznie zgodnego z interesem naszego państwa. W związku z tym czy tego rodzaju działania są prowadzone, czy państwo mają to na względzie?

Kolejna rzecz dotyczy infrastruktury. Odniosę się akurat do policji. Z moich doświadczeń w całej Polsce wynika, że niestety ta infrastruktura jest niewystarczająca i bardzo często policjanci korzystają w swojej działalności również z prywatnych zasobów. Do tej pory był z tym problem, wieczny problem, policja wiecznie niedofinansowana, a w zakresie sprzętu informatycznego – powiedziałbym – naprawdę wiekowe zaległości. I pytanie: Czy państwo te aspekty analizują, czy one są przedmiotem szczególnej troski, bo to rzeczywiście jest taki aspekt, który – myślę – nie tylko w policji, ale w każdej instytucji, wpływa na bezpieczeństwo.

Ja się cieszę, że jest coś takiego jak program ograniczania przestępczości i antyspołecznych zachowań „Razem bezpieczniej" im. Władysława Stasiaka. To naprawdę jest rzecz, którą należy promować, tylko znowu pytanie: Dlaczego wojewodowie decydują o tych programach? Dlaczego to nie jest szerszy program skierowany do samorządów, tak żeby on mógł być powszechny. Kiedy przeczytałem listę gmin, mam takie wrażenie, że jednak – powiem na okrętkę – ta formuła jest taka – powiedziałbym – mało przejrzysta. Czy nie lepiej by było, żeby zorganizować otwarty konkurs, w którym mogłyby startować... który byłby recenzowany przez osoby niezwiązane z rządem, tak jak są związani wojewodowie? Czy nie można by było tego zrobić dla społeczeństwa, ale tak – wiecie państwo – z użyciem trzeciego sektora? Myślę, że byłoby to o wiele bardziej efektywne, bo problem tego rodzaju w internecie istnieje, on jest poważny, myślę, że dotyka większości z nas, którzy tu jesteśmy na tej sali, i trzeba z nim oczywiście walczyć. Ja niestety muszę udać się na salę, ponieważ nieszczęśliwie w tym samym momencie jest obradowany punkt, ale bardzo bym prosił o udzielenie ewentualnie odpowiedzi na piśmie, jeżeli

byłaby taka możliwość, a z pewnością wrócę tu po zakończeniu rozpatrywania tego punktu. Dziękuję bardzo.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję bardzo. Czy są jeszcze pytania z państwa strony? Bardzo proszę, pani poseł Hrynkiewicz. Chociaż, pani poseł, może sekundkę. To pytanie i dopytanie pana posła Marka Wójcika, jeżeli można by było prosić w tej chwili o krótką odpowiedź.

**Poseł Józefa Hrynkiewicz (PiS):**

Dobrze, bo ja mam inną sprawę.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Bardzo proszę, panie dyrektorze.

**Dyrektor Departamentu Teleinformatyki MSWiA Dariusz Bogucki:**

Chodzi o to pytanie, gdzie można zgłosić przestępstwo, tak?

**Poseł Marek Wójcik (PO):**

Tak.

**Dyrektor Departamentu Teleinformatyki MSWiA Dariusz Bogucki:**

W takim razie proszę bardzo.

**Pełnomocnik Komendanta Głównego Policji do spraw bezpieczeństwa cyberprzestrzeni Marcin Kuskowski:**

Panie przewodniczący, szanowni państwo, policja zgodnie z ustawą działa w tym zakresie, który ta ustawa jej daje, więc każdy obywatel, czując się zagrożony, ma prawo zgłosić informację o takim zagrożeniu do każdej jednostki policji tej najbliższej jego miejscu zamieszkania. W komendach wojewódzkich policji powstały wyspecjalizowane wydziały do walki z cyberprzestępczością, które są koordynowane przez Biuro do Walki z Cyberprzestępczością Komendy Głównej Policji, więc po dokonaniu takiego zgłoszenia na komisariat taka sprawa, takie zgłoszenie powinno zostać przekazane do tej wyspecjalizowanej jednostki, która tym incydentem, tym potencjalnym przestępstwem będzie się zajmować. My więc tak to widzimy.

Natomiast jeżeli chodzi o druga kwestię związaną ze sprzętem teleinformatycznym policji, to myślę, że ta sprawa jakby idzie ku lepszemu. Posiadamy środki budżetowe, które systemowo, sukcesywnie są przeznaczane na sprzęt dla policjantów, tak żeby nie musieli stukać w takie klasyczne maszyny do pisanie, tylko mogli posługiwać się już komputerami. Myślę, że w tym kierunku to wszystko idzie. To nie jest tak, jak to tutaj zostało przedstawione. Myślę, że Policja ma już sprzęt do tego, ażeby być w stanie normalnie pracować, jeżeli chodzi chociażby o przyjmowanie zgłoszeń i zawiadomień o popełnieniu przestępstw czy tym podobnych historii. Dziękuję bardzo.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Proszę bardzo, pani profesor.

**Poseł Józefa Hrynkiewicz (PiS):**

Ja przeczytałam bardzo dokładnie materiał dotyczący programów profilaktycznych prowadzonych w MSWiA. W związku z tym mam swoje zdanie na temat tych programów. Jest to zdanie negatywne dlatego, że jak zrobimy gdzieś w Gostyniu czy gdzieś w Przeworsku konkurs na najlepszy spot czy na coś takiego, to naprawdę to nie powiększy tam – przypuszczam – bezpieczeństwa. Natomiast moje pytanie jest szersze. Pytanie generalne jest takie, czy Ministerstwo Spraw Wewnętrznych i Administracji jest instytucją publiczną, która ma się zajmować organizacją jakichś konkursów? Bardzo w to wątpię. Ja sądzę, że jeśli już państwo chcecie wydawać pieniądze, to nie piszecie, ile kosztują te wszystkie konkursy, te projekty, które organizujecie, a raz jest ich siedemnaście innym razem dwadzieścia parę, nie ma kosztu tych konkursów, potem jest program na lata 2018–2020 na każdy rok po 6,5 mln – to oczywiście można to robić, ale może robiłaby to jakąś organizacja społeczna, która jest do tego przygotowana? Jeśli już państwo to robicie, to ja poproszę o podsumowanie, ale nie czy wydali pieniądze czy nie wydali, czy zrobili spot czy zrobili konkurs, tylko po prostu analizę skuteczności tych

programów, bo jak rozumiem, te programy organizujecie – i policja i państwo – po to, żeby stworzyć pewne rozwiązania systemowe. Ja tak bym rozumiała funkcję ministerstwa czy policji, prawda?

Chodzi o to, żeby wypracowali, ale nie sami urzędnicy ze sobą, tylko żeby wypracowali po prostu ze środowiskami, które rzeczywiście zajmują się bardzo pogłębionymi badaniami związanymi z różnego rodzaju formami przestępczości, zagrożeń, niebezpieczeństw, które są wśród młodzieży. Takich badań jest sporo w Polsce realizowanych. Są wyspecjalizowane środowiska socjologiczne i pedagogiczne, które takie badania prowadzą i rozumiałabym, że państwo po prostu analizujecie to po to, żeby dojść do sformułowania jakiegoś programu systemowego, a nie po to, że zrobicie 286 projektów czy 98 albo ileś, bo to naprawdę nie od tego jest ministerstwo i nie od tego jest Komenda Główna. Ja rozumiem, że państwo spotkalibyście się ze specjalistami i opracowalibyście jakieś rozwiązania systemowe. Naprawdę jeżeli to jest 20 mln, to za 20 mln – zapewniam państwa – można opracować znakomite programy, można je wdrożyć, można przeszkolić nauczycieli na przykład w szkołach czy wychowawców czy jakichś pracowników, którzy będą się tym zajmować, a nie po prostu organizować jakieś konkursy. Jaki jest w ogóle sens – wytłumaczcie mi – dla Ministerstwa Spraw Wewnętrznych i Administracji organizowania takich różnych projektów? Przecież nie od tego moim zdaniem jest ministerstwo. Nigdy nie słyszałam, żeby administracja centralna, administracja rządowa zajmowała się takimi działaniami. To nie jest ani w kompetencji ministerstwa, ani w jakimś takim sensie, który pokazywałby szersze tło. Jeżeli jest jednak to szersze tło, bo ja wierzę, że nie jest to jakieś organizowanie konkursów, to proszę pokazać. Może państwo pokażecie analizę, może pokażecie przydatność tych rozwiązań, które zastosowaliście, ale nie na zasadzie konkursów. Ja rozumiem, że państwo wybieralibyście jakieś środowiska, które ze względu na swoje cechy społeczne, demograficzne, ekonomiczne, etnograficzne i jakieś inne jest właściwe do przeprowadzenia takich badań, przeprowadzali badania przy okazji, z tych badań wyciągali wnioski i na podstawie wyników tych badań formułowali projekty. Tego oczekuję od was, a nie tego, że będziecie pisali...

Nie wiem, za ile milionów te projekty były w roku 2016 i 2017 realizowane. Dlaczego o tym nie piszecie? Tak, pod tymi projektami nie ma. Myślałam, że pod każdym z tych projektów to będzie, bo przecież jest tam jeszcze jakiś koszt obsługi. Ile kosztuje sam taki projekt? Bardzo proszę, jeżeli nie jesteście państwo przygotowani do udzielenia odpowiedzi na to pytanie, o odpowiedź na piśmie.

Jeśli jeszcze ktoś potrafi mi odpowiedzieć na jedno pytanie, które mnie bardzo dręczy, to jest pytanie o bezpieczeństwo wytwarzania kart do głosowania w wyborach. Teraz będą wybory samorządowe, potem będą wybory parlamentarne, wybory do europarlamentu, wybory prezydenckie. Czy ten problem w państwa pracach związanych z bezpieczeństwem, bo to także należy do kategorii bezpieczeństwa – zabezpieczenie wytwarzana i dystrybucji kart do głosowania, czy ten program, czy ten projekt, czy prace nad tym zagadnieniem są prowadzone w Ministerstwie Spraw Wewnętrznych i Administracji?

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję. Bardzo proszę, panie dyrektorze.

**Dyrektor Departamentu Teleinformatyki MSWiA Dariusz Bogucki:**

Myślę, że wsłuchaliśmy się starannie w uwagi pani profesor i wypowiemy się szczegółowo na piśmie, natomiast ja powiem tak, że jeśli chodzi o program, to on został przyjęty 9 stycznia tego roku. 15 marca weszło w życie zarządzenie i pierwsze posiedzenie zespołu, który opracowuje ten program, odbędzie się dokładnie 16 kwietnia. Na to posiedzenie, jeśli można, przekażemy szczegółowe uwagi, które przedstawiła pani profesor.

**Poseł Józefa Hrynkiewicz (PiS):**

A co z działaniami, które zrealizowaliście w roku 2016 i 2017? Czy są jakieś analizy i wnioski z tych projektów, które państwo zrealizowaliście w roku 2016 i 2017? Czy one stanowiły podstawę do wypracowania jakichś rozwiązań systemowych, bo to, że organizujecie różnego rodzaju konkursy i eventy, naprawdę nie jest działaniem ministerstwa. Proszę wybaczyć, rozumiem gdyby to robiła jakaś organizacja społeczna czy fundacja, ktoś, komu byście to zlecili, ale też pod tym warunkiem, że chcecie z tego mieć jakiś

materiał potrzebny do stworzenia rozwiązań systemowych, bo inaczej takie działanie jest bez sensu na poziomie Ministerstwa Spraw Wewnętrznych i Administracji.

**Naczelnik Wydziału do Spraw Terroryzmu i Przestępczości Zorganizowanej w Departamencie Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji Ilona Idzikowska:**

Panie przewodniczący, Wysoka Komisjo, pani poseł, Ilona Idzikowska, Departament Porządku Publicznego MSWiA, do którego od niedawna wróciła rola koordynatora tego programu. Chciałabym poinformować, że szczegółowe informacje dotyczące kosztów poszczególnych realizowanych projektów są oczywiście u nas magazynowane i zbierane. Wszystkie projekty, które otrzymają dofinansowanie, oczywiście później są poddawane ewaluacji i takie informacje zostaną przedstawione na piśmie. Niestety nie dysponuję tutaj szczegółowym wyliczeniem poza tym, które jest w tym materiale, który do państwa posłów trafił, poza tymi kwotami, które w nim są już podane. Szczegółowe dodatkowe wyjaśnienia zostaną przekazane na piśmie. Tak, jak pan dyrektor już wspomniał, podczas najbliższego posiedzenia zespołu dedykowanego koordynacji programu „Razem bezpieczniej" w tej najnowszej edycji na najbliższe trzy lata poruszymy wszystkie postulaty podniesione przez panią poseł.

**Poseł Józefa Hrynkiewicz (PiS):**

Przepraszam, panie przewodniczący, czy mogę?

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Proszę.

**Poseł Józefa Hrynkiewicz (PiS):**

Przepraszam, może niestarannie to przedstawiłam i to jest moja wina, ale mam takie wrażenie, że pani nie zrozumiała. Ja nie oczekuję od Ministerstwa Spraw Wewnętrznych i Administracji, że będziecie się zajmowali konkursami. To nie jest wasze zadanie, pani dyrektor. To nie jest zadanie ministerstwa. Możemy przejrzeć wszystkie dokumenty powołujące ministerstwo i tam go nie znajdziemy. Mnie interesuje to, abyście państwo w porozumieniu ze środowiskami, które mają znacznie szerszą, głębszą i bardziej zweryfikowaną wiedzę na temat niebezpieczeństw, pracowali nad rozwiązaniami systemowymi, takimi rozwiązaniami, które systemowo będą zapobiegały rozszerzaniu się pewnych niebezpiecznych zachowań, niebezpiecznych zjawisk, które przecież są. Nie musimy się przekonywać, że one takie są. To samo dotyczy ministerstwa, to samo dotyczy policji. Oczekuję po prostu rozwiązań systemowych opartych na sprawdzonej i naukowo udokumentowanej wiedzy. Inaczej to po prostu jest bez sensu. Pani dyrektor, taki departament nie ma sensu, żeby robił konkursy. Zrobi konkurs w Przeworsku, w Wieruszowie, gdzieś jeszcze, i co z tego wynika, jakie pani ma wnioski z tego konkursu, co z tego konkursu da się zastosować do rozwiązań systemowych? Ma pani to spisane?

**Naczelnik wydziału w MSWiA Ilona Idzikowska:**

To znaczy, konkursy na projekty, które uzyskują dofinansowanie, odbywają się na poziomie centralnym. To w MSWiA spotyka się komisja konkursowa, która rozpatruje projekty zgłaszane przez podmioty lokalne. To nie jest tak, że my jedziemy do Przeworska i tam organizujemy jakiś konkurs, tylko tutaj decydujemy, który projekt otrzyma dofinansowanie. Natomiast, jak mówię, szczegółowe informacje przedstawimy na piśmie na temat dotychczasowych projektów realizowanych w ramach poprzednich edycji programu „Razem bezpieczniej" jak również ustosunkujemy się do postulatów pani poseł.

**Poseł Józefa Hrynkiewicz (PiS):**

Nie przyjmuję tej odpowiedzi, przykro mi.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Przepraszam bardzo, ale uratuje nas jedynie rzeczywiście posługiwanie się tą formą pisemną, bo zostało niewiele minut do momentu, w którym następna komisja zajmie naszą salę, a jeszcze są kolejne pytania. W kolejności, w jakiej były zgłoszenia – pan poseł Suchoń, a potem pan poseł Wójcik.

**Poseł Mirosław Suchoń (N):**

Bardzo dziękuję. Ja tylko powtórzę, że uważam, iż to jest absolutnie zasadne i fajne, tylko myślę, że częściej należy korzystać z doświadczeń trzeciego sektora. Natomiast panie przewodniczący, ja mam prośbę do pana przewodniczącego. Myślę, że ta prezentacja jest dla nas istotna z punktu widzenia dalszego funkcjonowania i ewentualnego proponowania rozwiązań, dlatego też mam taką prośbę, żeby prezentacja trafiła na nasze skrzynki mailowe.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dobrze. Proszę bardzo, panie pośle.

**Poseł Marek Wójcik (PO):**

Dziękuję bardzo. Szanowni państwo, nie chcę państwa dręczyć pytaniami – nie taka jest moja intencja – tylko nie do końca mogę przyjąć taką odpowiedź. Ja oczywiście znam przepisy – że jeżeli ktoś pada ofiarą przestępstwa, to niech sobie idzie na najbliższy komisariat – to jest jego prawo – i niech tam zawiadomi, że popełniono przestępstwo. Specyfika przestępstw w internecie pewnie jest taka, że ich ofiarą pada bardzo wiele osób. Czasem są osoby, które mogą liczyć w domu, wśród znajomych na jakąś pomoc informatyczną, a czasem są to osoby, które mają tylko komputer i nie mają kogo poprosić. I takie osoby w takiej sytuacji, kiedy nagle na ekranie wyświetli się im komunikat „Masz zablokowany dostęp do komputera – zapłać 100 dolarów, to ci odblokujemy. Tu jest numer konta", czują, że padły ofiarą przestępstwa i faktycznie padają ofiarą przestępstwa. Taka osoba bierze laptopa i co teraz ma zrobić? Jeżeli pójdzie na ten najbliższy komisariat na osiedlu, to tam rzeczywiście pewnie ktoś zrobi zdjęcie tego komputera, pewnie zostanie przyjęte jakieś zawiadomienie o popełnieniu przestępstwa, ta osoba zostanie przesłuchana w charakterze pokrzywdzonego. OK, te wszystkie działania zostaną wykonane. Prawdopodobnie policjanci poopowiadają o różnych rzeczach, że za chwilę Bóg wie jacy fachowcy się tym zajmą i w ogóle to nie jest pierwszy raz, ale niestety idę o zakład, że za trzy miesiące większość z tych ludzi otrzyma po prostu informację o tym, że postępowanie zostało umorzone w związku z niewykryciem sprawców. Ten człowiek nie dostaje pomocy. W tym punkcie, do którego poszedł, czyli w komendzie dzielnicowej, to nie jest pomoc. Zarejestrowanie przestępstwa nie jest pomocą dla konkretnego obywatela. Chciałbym, żebyście państwo o tym myśleli również w ten sposób. To znaczy, jeżeli specjaliści są w komendzie wojewódzkiej, to może lepiej poinformować taką osobę, że ma iść do komendy wojewódzkiej, że tam uzyska pełne informacje na ten temat i bez złudzeń, bo być może będzie musiał zresetować system, być może będzie musiał zanieść go do jakiegoś informatyka, ale przynajmniej ta osoba nie będzie tkwiła w jakimś fałszywym wyobrażeniu dotyczącym swojej sytuacji i w jaki sposób policja takiej osobie jest w stanie pomóc. Nie oczekuję od państwa, że będziecie mieli specjalistów od przestępstw informatycznych na każdym poziomie – komisariatu, czy posterunku, bo to jest niemożliwe, tylko chcę wiedzieć, czy państwo też myślicie o tym, żeby takie osoby wysyłać rzeczywiście do fachowców. Fachowcy są rzadko spotkani, są cenni, jest ich w ogóle mało w populacji, w Policji też jest ich niewielu, muszą zajmować się poważnymi sprawami, natomiast nie każdy policjant jest w stanie takiemu obywatelowi pomóc. Chodzi o to, czy państwo o tym myślicie, bo poinformowanie obywatela, żeby poszedł do najbliższego komisariatu i tam zgłosił przestępstwo jest OK – z punktu widzenia procedury jest wszystko w porządku, ale z punktu widzenia takiego obywatela być może, kiedy będzie zgłaszał to przestępstwom, będzie jeszcze usatysfakcjonowany, ale wraz z upływem czasu jego zaufanie do państwa będzie niestety w moim przekonaniu malało. Dlatego proszę państwa o jakąś refleksję na ten temat. Dziękuję.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję bardzo. Proszę państwa, w drugim punkcie mamy propozycje tematów do planu pracy Najwyższej Izby Kontroli na 2019 r. Zostały zgłoszone tematy. One zostały załączone do przekazanych państwu dokumentów. Bardzo proszę, panie pośle.

**Poseł Marek Wójcik (PO):**

Dziękuję bardzo. Ja mam przed sobą te propozycje...

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Jest ich pięć.

**Poseł Marek Wójcik (PO):**

...tych pięciu tematów. Ja oczywiście nie mam do nich uwag, natomiast mam taką propozycję, aby do tych tematów dodać jeszcze jeden. To jest ocena stanu realizacji programu modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej, Biura Ochrony Rządu w latach 2017–2020. To jest plan na 2019 r. W związku z tym plan będzie wtedy w pełni rozpędzony i realizowany. Myślę, że byłoby dobrze, gdybyśmy mieli możliwość zapoznania się z taką informacją.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję. Czy są jeszcze inne propozycje? Proszę bardzo.

**Poseł Mirosław Suchoń (N):**

Panie przewodniczący, ja również zgadzam się z tymi tematami, które zostały przedstawione przez prezydium, natomiast bardzo proszę o ujęcie kolejnego tematu. Proponuję, aby przedmiotem tej kontroli było używanie środków przymusu bezpośredniego przez policję.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję. Czy są jeszcze jakieś propozycje tematów? Bardzo proszę, panie generale.

**Dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli Marek Bieńkowski:**

Panie przewodniczący, Wysoka Komisjo, ponieważ program modernizacji jest już mocno rozpędzony, panie pośle, bo on od stycznia ubiegłego roku funkcjonuje, od czerwca tego roku rozpoczynamy ogólnopolską kontrolę dotyczącą oceny tego etapu realizacji programu. Oczywiście procedura jest taka, że zgłoszone przez państwa tematy podlegają ocenie i zatwierdzeniu przez Kolegium Najwyższej Izby Kontroli. Dlatego na tym etapie przyjmujemy je do realizacji. Dziękuję bardzo.

**Przewodniczący poseł Arkadiusz Czartoryski (PiS):**

Dziękuję bardzo. Nie ma więcej propozycji tematów, więc rozumiem, że wszystkie przyjęliśmy w konsensusie.

Czy w sprawach różnych są pytania? Nie słyszę.

Zamykam posiedzenie Komisji.