PROTOKÓŁ z VI posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 17 maja 2019 roku, o godzinie 11:00 w siedzibie Ministerstwa Cyfryzacji.

Spotkanie z Panem Karolem Okońskim, Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa i Sekretarzem Stanu w Ministerstwie Cyfryzacji, dotyczące cyberbezpieczeństwa w kontekście wdrożenia 5G.

Pan Minister Karol Okoński spotkał się z Członkami Rady do Spraw Cyfryzacji, by porozmawiać na temat cyberbezpieczeństwa, które jest fundamentalną kwestią w kontekście wdrożenia 5G.

Minister Okoński wskazał, że Komisja Europejska zaleciła szereg działań, których celem jest zapewnienie wysokiego poziomu cyberbezpieczeństwa sieci 5G w całej Unii Europejskiej. Na szczeblu krajowym każde z państw członkowskich ma do końca czerwca 2019 r. przeprowadzić ocenę ryzyka związanego z krajową infrastrukturą sieci 5G. Na tej podstawie państwa członkowskie powinny zaktualizować dotychczasowe wymogi w zakresie cyberbezpieczeństwa.

Polska jest aktualnie w trakcie procesu szacowania ryzyka. Następstwem tego działania będzie zaproponowanie rozwiązań, by tym ryzykom zapobiec – może się okazać, że właściwym środkiem zaradczym będzie np. wprowadzenie zmian prawnych. Proces szacowania ryzyka i przygotowania polskiego podejścia jest dość dynamiczny, ze względu na zmieniającą się sytuację i decyzje innych państw – przytoczony został przykład choćby decyzji Prezydenta USA Donalda Trumpa, który wprowadził prawo umożliwiające Stanom Zjednoczonym zakazanie korzystania ze sprzętu i usług podmiotów uznanych za zagrożenie dla bezpieczeństwa narodowego w amerykańskich sieciach telekomunikacyjnych. USA ma więc możliwość wykluczenia pewnych dostawców z rynku – do listy tych podmiotów, co do których nałożone są pewne ograniczenia, dopisany został m.in. Huawei.

Podkreślone zostało, że Stany Zjednoczone, ale też Wielka Brytania czy Francja, mają o tyle inną sytuację, że tam w dotychczasowym sposobie budowy sieci telekomunikacyjnych regulatorzy wdrożyli takie rozwiązania, które spowodowały, że w administracji publicznej i w warstwie szkieletowej sieci po prostu nie ma firmy Huawei, a w Polsce jest ona obecna.

Wszystko to wpływa na dynamikę przygotowania polskiego podejścia. Wszelkie decyzje podejmowane przez stronę polską nie mogą z jednej strony abstrahować od wydarzeń na arenie międzynarodowej, ale z drugiej strony muszą również uwzględniać aktualny stan rzeczy na rynku telekomunikacyjnym w Polsce. Podkreślone zostało, że działania poszczególnych państw Unii Europejskiej będą różne, bo każdy ma inny punkt wyjściowy - inny stan prawny, stan infrastruktury i poziom konkurencyjności na rynku telekomunikacyjnym. Polska dąży do tego, żeby – biorąc pod uwagę perspektywę znaczenia sieci 5G w przyszłości – nie być uzależnionym od jednego dostawcy. Z tego powodu bardzo poważnie rozważane są takie rozwiąza-

nia, które pozwolą uniknąć sytuacji, że na danym odcinku sieci wykorzystywane są urządzenia tylko jednego dostawcy. Być może również w pewnych strefach specjalnych (np. w administracji rządowej) stworzone będą bardziej rygorystyczne warunki dotyczące tego, jakie urządzenia czy jakie oprogramowanie może być wykorzystywane. Działania te nie mają być wymierzone w konkretnego dostawcę – docelowo zakładane jest opieranie się na modelu certyfikacji/autoryzacji danych urządzeń, tak jak to jest np. we Francji. Zanim jednak taki system certyfikacji powstanie, będą musiały być podejmowane pewne działania doraźne (np. ostrzeżenia czy informacje o pewnych wykluczeniach), oparte oprócz aspektów technicznych na analizie ryzyka, dotyczącej również firm chińskich.

Podejmowane obecnie przez polski rząd działania zmierzają do publicznego zaprezentowania proponowanych rozwiązań. Obecnie w Ministerstwie Cyfryzacji trwają prace, w które zaangażowane są departamenty MC (przede wszystkim Departament Cyberbezpieczeństwa oraz Departament Telekomunikacji), NASK, Instytut Łączności i Agencja Bezpieczeństwa Wewnętrznego. Docelowo do grupy zaangażowanych podmiotów dołączą jeszcze MSZ, MSWiA, MON, Agencja Wywiadu i prawdopodobnie MPiT. Pozwoli to wspólnie ocenić potencjalne konsekwencje proponowanych działań – ich wpływ na politykę międzynarodową i na rynek wewnętrzny. Działania rządu mogą mieć wpływ na plany inwestycyjne i plany rozwoju operatorów telekomunikacyjnych, więc również z nimi należy w pewien sposób przedyskutować te propozycje.

Intencją MC jest, by pierwsze aukcje na sieci 5G przeprowadzić w przyszłym roku – z tego względu planowane działania dotyczące kwestii cyberbezpieczeństwa powinny pojawić się szybko, żeby operatorzy byli w stanie przygotować się do nowych okoliczności.

Minister podkreślił również, że przy okazji tematu wdrożenia 5G i przeprowadzanego procesu szacowania ryzyka dla Komisji Europejskiej, na wewnętrzne potrzeby Polski, proces ten został rozszerzony o dyskusję na temat infrastruktury krytycznej, operatorów usług kluczowych (w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa), operatorów usług zaufania (z ustawy o usługach zaufania oraz identyfikacji elektronicznej) oraz przedsiębiorców telekomunikacyjnych i administracji publicznej. Analiza ryzyka, która ma powstać do końca czerwca, skupiona będzie więc głównie na sieci 5G, ale może dotknąć także wymienionych obszarów.

Członkowie Rady wyrazili zaniepokojenie kwestiami związanymi z intensywną obecnością w Polsce firmy Huawei, która w świetle aktualnych wydarzeń międzynarodowych jest podmiotem szczególnym. Minister podkreślił, że MC uważnie śledzi rozwój sytuacji, a także spotyka się z przedstawicielami chińskiej firmy, ale spotyka się także z przedstawicielami innych firm, żeby zachęcić do inwestowania w Polsce i wejścia na polski rynek, aby zwiększyć jego konkurencyjność.

Jeden z Członków Rady zauważył, że Huawei jest obecny w infrastrukturze krytycznej państwa, o czym trzeba pamiętać. Należy się więc zastanowić, czy jest to problemem czy nie.

Podkreślone zostało również, że obecnie w Polsce nie ma instytucji, która miałaby kompetencje i upoważnienie do tego, by określić – na podstawie badań technicznych oprogramowania/urządzeń - co możemy dopuszczać do użytkowania, czego nie, co konkretnie powinniśmy traktować jako zagrożenie itp. Minister wskazał, że w ustawie o krajowym systemie cyberbezpieczeństwa jest przewidziane ciało kolegialne – Kolegium ds. cyberbezpieczeństwa – które w swoich kompetencjach ma m.in. doradzanie Premierowi w podejmowaniu strategicznych decyzji i wspieranie Pełnomocnika Rządu ds. cyberbezpieczeństwa w wydawaniu rekomendacji. Minister zauważył, że wydaje się, że tego typu działania powinny być wypadkową różnych interesów poszczególnych działów państwa, dlatego też Kolegium i Rada Ministrów to właściwe instytucje do podejmowania kierunkowych decyzji. Kwestię kompetencji technicznych natomiast ma uzupełnić projekt KSO3C, realizowany przez IŁ, NASK i EMAG, który docelowo doprowadzi do powstania w Polsce jednostki certyfikującej za zgodność z *Common Criteria*. Co istotne, jest to model otwarty, do którego mogą być dodawane inne laboratoria (bądź mogą być rozszerzane kompetencje już istniejących), co pozwoli w przyszłości dokonywać certyfikacji nie tylko za zgodność z *Common Criteria*, ale również za zgodność z innymi profilami/wytycznymi, powstającymi na mocy *Cybersecurity Act*. Należy jednak pamiętać, że aby móc mówić o jakościowej zmianie musi upłynąć kilka lat.

Jeden z Członków Rady zapytał czy są plany stworzenia na poziomie europejskim wspólnej strategii i podejścia do chińskich firm technologicznych. Minister wskazał, że dokonując analizy ryzyka państwa unijne konsultują się ze sobą, są grupy państw o zbliżonych podejściach (*like-minded*), odbywają się również spotkania bilateralne. Polska jest np. w stałym kontakcie z Czechami, Estonią, Wielką Brytanią, Niemcami, Francją. Wydaje się jednak, że wspólnej europejskiej strategii nie będzie – Komisja Europejska chce raczej zmobilizować kraje, żeby używały podobnej/tej samej metodologii oceny ryzyka. Komisja podkreśla też, że należy w maksymalny sposób wykorzystać prawodawstwo unijne, które już istnieje, jak choćby *Cybersecurity Act*, dyrektywy telekomunikacyjne, dyrektywę ePrivacy czy dyrektywę o monitorowaniu inwestycji zagranicznych. Jeszcze raz zostało również podkreślone, że każde z państw ma inny punkt startu, przez co każdy będzie raczej bronił swojej niezależności.

Poruszona została również kwestia wsparcia dla polskich firm. Minister wskazał, że krokiem w stronę zwiększenia szans firm z sektora małych i średnich przedsiębiorstw jest nowelizowane Prawo Zamówień Publicznych, które umożliwi zwiększenie procentowego udziału małych i średnich przedsiębiorstw w zamówieniach publicznych, dzięki czemu wzrośnie innowacyjność sektora MŚP. Nie dotyczy to wprost rynku cyberbezpieczeństwa, jednak na pewno i w tym zakresie znajdzie to swoje przełożenie. Wskazane zostało, że są również programy start-upowe i programy związane z badaniem i rozwojem w ramach NCBiR, do których mogą być - i są - zapraszane polskie firmy. Planowane jest również utworzenie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych, a także ustanowienie sieci krajowych ośrodków koordynacji, które będą kumulować wiedzę i pomagać lokalnym firmom w ich rozwoju. Kwestią otwartą jest w tym kontekście nadal to, gdzie powstanie to Europejskie Centrum – Polska będzie starać się o to,

by zlokalizowane było ono w naszym regionie, być może nawet w Polsce. Co również istotne należy pamiętać też o programie *Digital Europe*, w ramach którego w kolejnej perspektywie finansowej przeznaczone jest 2 mld euro na cyberbezpieczeństwo, a wydawanie tych środków ma być właśnie przez te regionalne ośrodki. Jest to szansa, by stymulować rozwój polskich firm. Z tego względu MC stara się, by ten mechanizm wsparcia odpowiednio zafunkcjonował, żeby polskie firmy mogły maksymalnie szybko skorzystać z tych środków, jak tylko się one pojawią. Minister podkreślił również, że zintensyfikowane zainteresowanie obszarem cyberbezpieczeństwa będzie mogło przełożyć się na podwyższoną aktywność polskich firm i na zwiększenie ich roli na arenie międzynarodowej.

Przewodniczący zapewnił, że Rada ds. Cyfryzacji udzieli wszelkiego wsparcia Ministerstwu Cyfryzacji i Pełnomocnikowi Rządu ds. cyberbezpieczeństwa.

Wprowadzenie do Programu Zintegrowanej Informatyzacji Państwa - wystąpienie Pana Jacka Paziewskiego, Dyrektora Biura Analiz i Projektów Strategicznych MC.

Pan Jacek Paziewski przedstawił Członkom Rady ds. Cyfryzacji prośbę Ministerstwa Cyfryzacji o zaopiniowanie dokumentu programowego – Programu Zintegrowanej Informatyzacji Państwa. Wskazał, że po wielu miesiącach prac nad dokumentem obecna jego postać może podlegać już całościowej ocenie i opiniowaniu. Zaznaczył, że wstępne konsultacje były przeprowadzone w ciągu ostatnich miesięcy, a pierwszym merytorycznym punktem odniesienia dla aktualnej treści PZIP są wyniki ewaluacji programu przyjętego w 2016r. Wnioski z tej ewaluacji są syntetycznie przedstawione w treści obecnego dokumentu w części „Diagnoza".

Dyrektor Paziewski wskazał, że w przygotowaniu diagnozy uczestniczyła również poprzednia Rada ds. Cyfryzacji – był to etap formułowania zakresu problemów, którymi PZIP ma się zająć. Przeprowadzone zostały również wstępne konsultacje zakresu dokumentu – szczególnie treści diagnozy – z przedstawicielami resortów i z dwoma zespołami o charakterze think-tanku: z Klubem Jagiellońskim i Zespołem Cyfrowa Polska.

PZIP jest aktualnie w trakcie procesu konsultacji. Wsparcie Rady ds. Cyfryzacji w tym procesie potrzebne jest na dwóch płaszczyznach – z jednej strony chodzi o ocenę całości pod względem spójności logicznej i zakresu treściowego, a z drugiej strony o uwagi merytoryczne w odniesieniu do konkretnych treści.

Trudność ze sformułowaniem treści PZIP wynika z faktu, że jest on historycznie programem rozwoju dość nisko umiejscowionym w strukturze rządowych dokumentów strategicznych. Również sama nazwa dokumentu pozostała historyczna (żeby ją zmienić należałoby aktualizować dokumenty wyższego rzędu), przyjmuje się jednak, że Program Zintegrowanej Informatyzacji Państwa jest programem cyfryzacji - w dzisiejszych czasach informatyzacja właściwie sprowadza się do cyfryzacji, a sformułowanie „zintegrowana informatyzacja" wskazuje na podejmowanie działań w obszarze cyfrowym.

Podkreślone zostało, że Program Zintegrowanej Informatyzacji Państwa odpowiada na kierunki przedstawione w strategiach europejskich:

- Jednolity Rynek Cyfrowy,
- Plan działania UE na rzecz administracji elektronicznej na lata 2016–2020,
- Deklaracja tallińska.

Wpływ na PZIP mają również strategie krajowe – tj. Strategia na rzecz Odpowiedzialnego Rozwoju i Strategia Sprawne Państwo (jedna z dziewięciu strategii sektorowych SOR), do której PZIP się odnosi.

Należy również pamiętać, że PZIP nie jest jedynym dokumentem strategicznym Ministra Cyfryzacji – są jeszcze inne tematyczne, obszarowe dokumenty o charakterze planów strategicznych:

- Narodowy Plan Szerokopasmowy (którego częścią jest Plan wdrożenia 5G),
- Program otwierania danych publicznych

Rozpoczęto również prace nad Strategią rozwoju sztucznej inteligencji w Polsce i Programem rozwoju kompetencji cyfrowych. Wszystkie te cztery elementy są otoczeniem PZIP, ich treść jednak nie jest w PZIP powielana.

Dyrektor Paziewski zaznaczył, że wszystkie wymienione kwestie są bardzo istotne, bo pozwalają w pełni zrozumieć kontekst, w jakim PZIP funkcjonuje.

Przedstawione zostały problemy aktualnie zidentyfikowane w obszarze związanym z cyfryzacją państwa, które wymienione są w diagnozie w PZIP. Wskazano również główny cel programu, jakim jest *modernizacja administracji publicznej z wykorzystaniem technologii cyfrowych nakierowana na potrzebę podniesienia sprawności państwa i poprawienie jakości relacji administracji z obywatelami i innymi interesariuszami*. Cel główny PZIP zostanie osiągnięty poprzez realizację trzech celów szczegółowych:

I. Poprawę jakości oraz rozszerzenie zakresu komunikacji pomiędzy obywatelami i innymi interesariuszami a państwem;
II. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office);
III. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej.

Do celów szczegółowych w dokumencie zostały przedstawione kierunki interwencji, którymi odpowiednio są:

I. Reorientacja administracji publicznej na usługi zorientowane wokół potrzeb obywatela;
II. Implementacja narzędzi horyzontalnych, wspierających działania administracji publicznej:
    - Architektura Informacyjna Państwa
    - Zarządzanie infrastrukturą IT
    - Elektronizacja zarządzania dokumentacją
    - Jednolity system identyfikacji elektronicznej

- Jednolity system doręczeń elektronicznych
- Elektronizacja świadczeń zdrowotnych
- Centralna Platforma Analityczna

III. Rozwój kompetencji cyfrowych obywateli, pracowników administracji publicznej oraz specjalistów TIK

Dyrektor Paziewski wskazał również, że jednym z załączników do PZIP będzie Plan działań wszystkich resortów, służących realizacji założeń Programu – ma on obejmować projekty, planowane programy wszystkich resortów, a nie tylko Ministerstwa Cyfryzacji, jak było dotychczas.

Przewodniczący zaznaczył, że przyczyny niedojrzałości państwa polskiego nie leżą w braku informatyzacji. Jeżeli więc poprzez PZIP chce się osiągnąć większą dojrzałość administracji, powinna być najpierw wykonana analiza systemowa braków dojrzałości tej administracji w ogóle, nie tylko w kwestii informatyzacji. Dyrektor Paziewski zauważył, że takiej systemowej analizy procesów, a nie tylko tej części wspieranej systemami czy e-usługami, nie było. Wskazał natomiast, że w MSWiA taki projekt - System monitorowania usług publicznych (SMUP) – powstaje i w jakimś zakresie wychodzi naprzeciw potrzebie mierzenia efektywności świadczenia usług publicznych. W zakresie zainteresowania MC są procesy, które można wesprzeć elektronicznie. Wiceprzewodniczący zauważył, że to nie PZIP, a Strategia Sprawne Państwo reguluje tak naprawdę kwestie funkcjonowania państwa polskiego – w SSP podjęta jest analiza funkcjonowania państwa i omówione są kwestie takie, jak skuteczne zarządzanie i koordynacja działań rozwojowych, zwiększenie sprawności instytucjonalnej państwa, skuteczny wymiar sprawiedliwości i prokuratura, efektywne świadczenie usług publicznych itp. PZIP jest więc właściwie planem wykonawczym do celów/priorytetów zawartych w SSP.

Jeden z członków Rady zauważył, że informatyzacja na pewno zmieni sposób świadczenia usług i ułatwi ocenę ich jakości, bieżącą kontrolę tego co się dzieje, przede wszystkim na styku administracji i jej interesariuszy. Zauważył, że SMUP jest zaprojektowany na badanie tego, co się dzieje obecnie, a jeżeli będziemy mieli do czynienia z postępująca informatyzacją, to zmieni się zarówno jakość świadczenia usług, jak i pojawią się inne sposoby badania tego, jak ta jakość wygląda. Zapytał, czy w PZIP przewidziano jakieś procedury/instrumenty, które będą reagować na te zmiany. Dyrektor Paziewski wskazał, że monitorowanie efektywności działań administracji i satysfakcji klienta administracji będzie badana – już dziś są do tego pewne narzędzia.

Poruszona została również kwestia inwentaryzacji infrastruktury informacyjnej państwa. Jeden z członków Rady zapytał, czy policzona została liczba rejestrów publicznych i rejestrów urzędowych. Jest ich bowiem zdecydowanie za dużo, przy czym rejestry te nie współpracują ze sobą, a na osoby dostarczające danych nakładane są coraz to nowe obowiązki zasilania tymi samymi danymi kolejnych rejestrów. Dyrektor Paziewski wskazał, że inwentaryzacja taka została wykonana, jednak jej jakość nie jest jeszcze satysfakcjonująca. Zauważył, że istniejące metody pozyskiwania informacji o komponentach Architektury Informacyjnej Pań-

stwa, które zostały wykorzystane, koncentrują się bardziej na systemach niż na danych. Ponadto doraźna potrzeba KRMC związana z oceną projektowanych systemów informatycznych, ich zasadności, również wpływała na to, że nacisk położony był bardziej na architekturę warstwy systemowej, aplikacyjnej. Inwentaryzacja w warstwie semantycznej nie jest więc na tyle uporządkowana, by przedstawić kompleksowe wyniki – jest natomiast uruchomiony proces zmapowania głównych danych państwa w taki sposób, żeby można było wiarygodnie przedstawić całą informację. Dalsze działania związane z Architekturą Informacyjną Państwa zaplanowane są więc na kolejne kwartały, by informacja w tym zakresie rzeczywiście była pełna.

Podniesiony został też temat elektronizacji doręczeń. Wskazano, że jest to projekt kluczowy dla usprawnienia i rzeczywistego przeformatowania funkcjonowania urzędów publicznych. Podkreślone zostało, że wykorzystanie usługi hybrydowej umożliwiłoby obywatelom i innym interesariuszom administracji nadanie i odbiór korespondencji w postaci przesyłek pocztowych przy zachowaniu cyfryzacji korespondencji w podmiotach publicznych, dzięki czemu mógłby zniknąć obowiązek prowadzenia przez urzędy spraw w wersji papierowej i wszystko prowadzone byłoby w sposób elektroniczny. Pozwoliłoby to uporządkować pracę urzędów - skończyłoby problemy z dokumentacją, która raz prowadzona jest elektronicznie, a raz papierowo.

Jeden z członków Rady odniósł się również do kwestii podnoszenia kompetencji cyfrowych pracowników administracji publicznej. Pojawiło się pytanie, czy działanie to odnosić się będzie do osób już pracujących w administracji, czy raczej nakierowane jest na kształcenie na poziomie studiów wyższych z myślą o przyszłych pracownikach. Dyrektor Paziewski wskazał, że te działania dotyczą przeorganizowania znanych inicjatyw, jak Centrum Kompetencji Administracji.

Dyrektor Paziewski zaznaczył, że jeśli Rada ds. Cyfryzacji uważa, że MC zaniedbuje jakieś fundamentalne działania, czy jakiś kierunek jest niewłaściwie dobrany, to prosi Członków Rady o uwagi – w tym właśnie celu PZIP został Radzie przekazany.

Przewodniczący poprosił Członków Rady o analizę przekazanych przez Dyrektora Paziewskiego dokumentów. Poprosił również Zespół roboczy ds. infrastruktury o przewodzenie pracom nad przygotowaniem stanowiska Rady do Programu Zintegrowanej Informatyzacji Państwa i przygotowanie na kolejne posiedzenie draftu stanowiska RdC w tej sprawie.

Przewodniczący poprosił również Dyrektora Paziewskiego, by na kolejnym posiedzeniu Rady przedstawił bardziej szczegółowo temat Architektury Informacyjnej Państwa.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Joanna Adamczyk
2. Izabela Albrycht
3. Jacek Czarnecki
4. Krzysztof Dyki
5. Krzysztof Głomb - Wiceprzewodniczący
6. Paweł Gora
7. Agnieszka Gryszczyńska
8. Michał Kanownik
9. Anna Beata Kwiatkowska
10. Tomasz Łukawski
11. Dariusz Milka
12. Józef Orzeł – Przewodniczący
13. Piotr Patroński
14. Sebastian Szymański
15. Jacek Zadrożny

Zaproszeni goście:

16. Karol Okoński, Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Sekretarz Stanu w Ministerstwie Cyfryzacji
17. Andrzej Zybertowicz, Doradca Prezydenta RP
18. Jarosław Mosiejuk, ekspert
19. Wiesław Paluszyński, ekspert

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

20. Jacek Paziewski, Dyrektor Biura Analiz i Projektów Strategicznych w MC
21. Joanna Marczak-Redecka, Zastępca Dyrektora Biura Ministra w MC
22. Monika Skrzyńska, Doradca Ministra Cyfryzacji
23. Katarzyna Stopińska (MC)