PROTOKÓŁ z III posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 29 września 2023 roku, o godzinie 13:00 w formie wideokonferencji.

Dyskusja nad stanowiskiem w sprawie DWR.

Pan Przewodniczący rozpoczął dyskusję na temat uchwały Rady w sprawie Dostawców Wysokiego Ryzyka od omówienia propozycji poprawek do projektu uchwały przesłanych mailowo przez członków Rady.

Jeden z członków Rady zaapelował, by w dyskusji nad poprawkami i nad całą treścią uchwały mieć świadomość, że stanowisko nie odnosi się do interesu pojedynczego dostawcy, klienta, operatora czy firmy, która korzysta z jakiejkolwiek technologii, lecz do interesu bezpieczeństwa państwa. Nie należy patrzeć na korzyści jakiegokolwiek podmiotu przy podejmowaniu decyzji o DWR. Obecnie mamy w kraju ogromne ryzyko masowego zaopatrywania się wielu instytucji publicznych w sprzęt dostawców, którzy podczas obowiązywania ustawy o krajowym systemie cyberbezpieczeństwa KSC, znajdowaliby się na liście DWR.

Odniesiono się do pytania przesłanego mailowo przez jednego z członków Rady, czy istnieją szacunki dotyczące kosztów i możliwości wymiany sprzętu w obiektach infrastruktury krytycznej. Jeden z członków Rady odpowiedział, że problem może polegać na dwóch kwestiach. Należy najpierw określić kryteria DWR i czy dotyczą one określonej konkretnej kategorii urządzeń np. telekomunikacyjnych, ale także 4G lub 5G, czy też mówimy wyłącznie o urządzeniach aktywnych piątej generacji, np. budowanych w systemie non stand alone, takim który wymaga stosowania LTE - 4G. Trudność polega nie tylko na braku ustawowych kryteriów, ale na tym, że obiekty infrastruktury krytycznej dotyczą 11 różnych sfer, jak np. zaopatrzenia w wodę czy żywność, a ich wykaz jest niejawny. Być może takie szacunki zostały uczynione, jednak nie ma do nich dostępu, albo posiadamy ograniczony obraz sytuacji.

W toku dyskusji zauważono, że uchwała Rady to bardzo potrzebny akt, tym bardziej powinien być starannie przygotowany, aby polski biznes czuł, że akt nie jest wprowadzany nad jego głową, ale w interesach całego kraju. Dbanie o polskich przedsiębiorców oraz uwzględnianie ich interesów to bezpieczeństwo państwa. Wprowadzając ten akt Rada powinna być świadoma, jaki wpływ będzie miał na biznes i konkurencyjność rynku. Istnieje bardzo duża różnica pomiędzy operatorami w ilości posiadania chińskiego sprzętu. Ustawa i jej zapisy zostaną zrealizowane przez operatorów, jednak należy uwzględnić, że dla każdego z nich będzie to inne wyzwanie. Ponadto operatorzy posiadają różne łańcuchy dostaw i sposoby funkcjonowania – należy się zastanowić, czy Rada nie wysforuje jednych firm przed drugimi, czy nie naruszy cennej równowagi w Polsce. Istotnym elementem jest szeroki wpływ przedmiotowej zmiany na cały rynek.

Zauważono, że dyskusja toczy się na temat skutków, a nie przyczyny - wybrzmiewa brak regulacji prawnych. Głównym celem uchwały powinno być zwrócenie uwagi ustawodawcy, aby w jak najszybszym stopniu uregulował kwestie prawne oraz wprowadził je w życie.

Podmioty, o których wspomina Rada, korzystają z luki prawnej. Istotą jest, iż mimo tego, że Rada jest organem doradczym Ministra Cyfryzacji, to informatyka w bardzo szerokim tego słowa znaczeniu nie obejmuje tylko zadań, jakie są przypisane do MC. Wyrażono zdanie, aby z treści uchwały Rady wypływał czytelny komunikat, że brak regulacji prawnych jest podstawą problemu. Można dyskutować, czy ograniczać się na tę chwilę do regulacji prawnych dotyczących sieci 5G, które są najpilniejsze lub podchodzić systemowo - ująć w sposób ogólny i syntetyczny to zjawisko. Uchwała mająca rangę istotnego aktu opiniotwórczego powinna jak najszerzej oddziaływać i zwracać uwagę na wszystkie obszary. Należy zastanowić się nad kwestią wymieniania w uchwale terminów, mając na uwadze zachowanie pewnych proporcji wyważenia przesłania, którym kieruje się uchwała. Rada szczegółów technicznych nie jest w stanie przewidzieć - czy będzie realne zachowanie zaproponowanych przez Radę terminów, biorąc pod uwagę łańcuchy dostaw i skalę, w jakiej niektóre podmioty gospodarcze posiadają wdrożony system czy urządzenia DWR. Być może dla niektórych podmiotów taki termin zakończy ich funkcjonowanie na rynku. Należy poddać refleksji proponowane daty, aby w treści uchwały w sposób realny ocenić czas potrzebny do wymiany tej technologii.

Następnie przytoczono przykłady zakazu używania technologii chińskich w innych krajach, w których nie doszło do zaburzenia konkurencyjności ich rynków. Wskazano na pozytywny wpływ - pojawi się przestrzeń dla polskich dostawców (m.in. Open Ran), aby zastąpić DWR.

Zwrócono uwagę na użytkowników produktów DWR, ponieważ nie są to tylko operatorzy telekomunikacyjni, w dużej części jest to administracja publiczna. Jeżeli mowa jest o bezpieczeństwie budowanych systemów teleinformatycznych, to obowiązują w tym zakresie wymagania normy mówiącej o systemie zarządzania bezpieczeństwem informacji. Jest ona oparta na tym, że przedsiębiorca we wszystkim, co wykonuje budując czy eksploatując systemy teleinformatyczne, opiera się na analizie ryzyka. Niewyobrażalne jest, aby nieświadomie ktokolwiek oparł się na jednym dostawcy budując systemy usługowe. Przedsiębiorca, ryzyko związane z tymi zakupami powinien rozpatrywać w kontekście swojej wiedzy na temat sytuacji na rynku. Na końcu jest regulacja państwowa, co nie znaczy, że we wcześniejszych etapach eksploatujący czy budujący takie systemy byli zwolnieni z myślenia o ryzyku związanym z zastosowaniem określonych produktów. Uchwała Rady dotyczy wszystkich komponentów systemów teleinformatycznych, zaczynając od elementów telekomunikacyjnych przez komputery, macierze, wszystko to, co ma dostęp do sieci. Ryzyko, o którym mówi Rada, jest ryzykiem powszechnie znanym od kilku lat, w związku z czym powinno być brane pod uwagę przy jakichkolwiek decyzjach inwestycyjnych i udostępnianiu usług obywatelom przez podmioty świadczące usługi, nie tylko telekomunikacyjne, ale także chmurowe.

Rada powinna wskazywać kierunki co do potrzebnych regulacji, obszary oraz aspekty danego problemu, który powinien być uregulowany. Od dawna wiadomo, że brakuje ustawy o KSC, co niesie negatywne konsekwencje, np. w temacie 5G. Rada powinna spojrzeć szerzej, niż tylko odnosić się do sektora telekomunikacyjnego, ponieważ problem DWR jest znacznie

obszerniejszy. Zaproponowano ogólne, kierunkowe przygotowanie uchwały i wskazanie Panu Ministrowi, że regulacja jest niezbędna. Trzeba też wziąć pod uwagę fakt, że jeśli Rada będzie bardziej szczegółowo wkraczać w uchwale w konkretne propozycje np. co do terminów, to należy także uwzględnić wpływ na rynek. W przypadku woli politycznej czy uchwały rządowej stanowiącej, że dany dostawca jest uznawany za DWR należy mieć plan, jak rozsądnie wycofać się z urządzeń czy zakupu chroniąc łańcuchy dostaw.

Pan Przewodniczący zaznaczył, że można spełnić oczekiwania części z członków Rady, aby nie wskazywać konkretnego czasu na wymianę urządzeń od DWR, a podkreślić, że powinien być to termin maksymalnie krótki. Omawiamy problem nie jest nieistotnym aspektem, ponieważ idąc śladem pewnych propozycji rządowych, które ostatnio zaczęły wydłużać ten termin, może okazać się, że czas usunięcia takiego sprzętu równa się czasowi jego funkcjonowania. Następnie Pan Przewodniczący zdecydował, że głosowanie w sprawie uchwały nie zostanie przeprowadzone podczas posiedzenia, ponieważ należy wysłuchać wszystkich głosów, i odnieść się do nich w propozycjach zmian w projekcie.

Kolejny wypowiadający się uznał, że stanowisko Rady jest wyważone. Rada mówi ogólnie, że dostawcy z krajów wysokiego ryzyka to nie tylko kwestia administracji publicznej, nie tylko jest to kwestia infrastruktury krytycznej albo rozwiązań telekomunikacyjnych w szczególności 5G. Rada wskazuje, że temat jest kompleksowy, złożony i wymaga uniwersalnego zaadresowania, a z drugiej strony pokazuje dlaczego wprowadzenie definicji DWR jest pilne. Ponadto każda firma funkcjonując na rynku, a zwłaszcza informatycznym jest odpowiedzialna za przeprowadzanie analizy ryzyka swojego modelu biznesowego, rozwiązań technologicznych itd. Każda dojrzała organizacja kierując się analizą ryzyka powinna zastosować mityganty – dodatkowy monitoring i audyty. Sektor bankowy przygląda się z niepokojem temu, co dzieje się z ustawą o KSC. Dla banków idealne byłyby wzorce, które funkcjonują, nawet jeśli nie są wprost przypisane, czy to do administracji publicznej, czy dla konkretnych spółek i rozwiązań.

W dalszej części dyskusji wskazane zostało, że operatorzy mieli świadomość ryzyka. Od czasów Toolbox mówi się wprost o DWR. Wcześniej ten wątek był poruszany w rezolucjach Parlamentu Europejskiego, a ostatnio wyraźnie adresowany w wypowiedziach Komisji Europejskiej co do konkretnych dostawców. Zwrócono także uwagę na NATO i wyraźny komunikat o postrzeganiu Chin jako głównego rywala zagrażającego systemowi bezpieczeństwa, który stosuje rozwiązania oparte o siłę. Poszczególne państwa członkowskie wprowadziły ograniczenia dotyczące działalności DWR. Stany Zjednoczone zakazały stosowania urządzeń, nie tylko telekomunikacyjnych. Zwrócono uwagę, że systemy nadzoru wizyjnego, które w Polsce są i były używane, zostały oparte na masywnej transmisji do Chin, a przecież zgodnie z obowiązującym prawem telekomunikacyjnym operatorzy mają obowiązek prawny unikania uzależnienia od jednego dostawcy.

Rada może indywidualnie przedyskutować każdą koncepcję. Istotne jest, aby wypowiedzieli się operatorzy, czyli podmioty których ta zmiana dotyczy. Nie chodzi o to, by operatorzy stali się ofiarami tej zmiany, a o próbę zbudowania zrozumienia po ich stronie, po stronie biznesu.

Odnośnie dyskusji i wątpliwości dotyczących sytuacji, w której pojawi się w treści uchwały termin wycofania DWR – być może dobrym rozwiązaniem będzie zawarcie takiego sformułowania, które nie wskazuje wprost konkretnego terminu, ale bierze pod uwagę termin wynikający z analiz ryzyka. Te działania wskażą, jaki termin będzie najbezpieczniejszy również z punktu widzenia interesu państwa (bo tym interesem są także interesy gospodarki narodowej utrzymywanej przez biznes). Z drugiej strony Rada nie powinna się w dużym stopniu skupiać na skutkach, ponieważ uchwała Rady nie jest aktem prawotwórczym, jednak może wpłynąć na sytuację poszczególnych sektorów gospodarki. Ustawodawca może się ze zdaniem Rady nie zgodzić, albo zaproponować inne rozwiązania, także bardziej restrykcyjne niż zaprojektowane przez Radę.

Jeden z członków Rady nawiązał do konkurencyjności i wolnego rynku – jeśli konsument nie ma wyboru dokonania innego zakupu produktu niż wyprodukowanego w Chinach, to nie można mówić o całkowicie wolnym rynku. Chińczycy zadziałali takimi cenami, że zdominowali konkurencję.

Rada jako organ doradczy powinna także zaproponować potrzebę analizy – mapy wpływów w Polsce, obszarów w jakich funkcjonuje chińska infrastruktura, skali inwestycji oraz wpływu decyzji o DWR na gospodarkę kraju. Sieci telekomunikacyjne są fundamentalne dla funkcjonowania kraju i obywateli. W przypadku wykluczenia konkretnych dostawców, generują się wielkie koszty, które nie zostaną przeznaczone na inne potrzebne inwestycje w Polsce. Jesteśmy jednym z najbardziej konkurencyjnych rynków w Europie - to powoduje bardzo niskie ceny i operatorzy nie mogą swobodnie kształtować cen detalicznych. Chcąc rozwijać bardzo potrzebne inwestycje, branża telekomunikacyjna nie ma możliwości zwiększania przychodów.

Podsumowując dyskusję Pan Przewodniczący zaznaczył, że Rada doradza Ministrowi Cyfryzacji, a Minister jako członek Rady Ministrów powinien zajmować stanowisko we wszystkich sprawach dot. cyfryzacji. Są więc one także polem działania Rady. Zwrócono uwagę na kwestię łańcuchów dostaw, a także na równowagę w sektorze, Rada musi mieć na uwadze relacje między producentami, a konsumentami. Powodem ponownego podjęcia uchwały Rady w sprawie DWR jest to, że legislator nie wprowadził tej definicji do prawa. Rada chce zasygnalizować, że jest to konieczne, aby w izbach i organizacjach biznesowych można było mówić o konsekwencjach zdefiniowania DWR.

Dyskusja w sprawie Ewakuacji Danych.

Uznano, że temat jest bardzo istotny, jednak trudny do uchwycenia w zakresie jego granic, mając na uwadze strukturę państwa. Pojawia się pytanie jak nisko w jego hierarchii należałoby zejść z ewakuowaniem danych. Wszystko, co robią poszczególne instytucje państwowe i samorządowe, jest potrzebne do określonych celów. Będzie to gigantyczny zakres informacji, w dodatku tak różnie zinformatyzowanych instytucji poruszających się w obszarze różnych systemów oprogramowania, struktur baz danych itd., że można uznać takie maksymalne działanie za niewykonalne.

Pan Przewodniczący wskazał, że należy myśleć o minimalnym polu systemów, być może węższym niż infrastruktura krytyczna, ponieważ to jest odpowiedź na pytanie, co państwo musi posiadać w razie potrzeby restartu do uruchomienia ciągłości państwa w przypadku zniszczenia tej ciągłości przez jakiś czas.

Pomysł dyskusji w sprawie ewakuacji danych zaczął się od standardów służących ochronie infrastruktury krytycznej, które przygotowało Rządowe Centrum Bezpieczeństwa. Jesteśmy w procesie, który ma polegać na wdrożeniu przede wszystkim Dyrektywy NIS 2, ale również Dyrektywy CER. Występuje problem z różnymi terminologiami, jak obiekty infrastruktury krytycznej – ustawa o KSC używa jeszcze innych określeń. Być może ścisłej delimitacji nie da się uzyskać. Wskazany został Projekt e-Ambasada, który Rada zaproponowała, a rząd będzie realizował – zgromadzenie takiego zasobu danych, który pozwoli na zapewnienie ciągłości państwa. Być może pewną podpowiedzią jest to, co znalazło się w najnowszym projekcie Uchwały Rady Ministrów zmieniającej uchwałę w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa", z uwagi na obecność w projekcie wyłączeń w kontekście przetwarzania w chmurze publicznej. Czym innym jest opracowywanie planów związanych z zabezpieczaniem danych. Mowa o specjalnych rozwiązaniach, w tym również związanych z tym, jakie dane mogą i powinny znajdować się w chmurze publicznej czy być ewakuowane poza granice kraju, gdzie pojawia się skomplikowany problem dotyczący styku ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, wcześniej wspomnianej uchwały RM czy krajowych ram interoperacyjności.

Zauważono, że warto byłoby zwrócić uwagę w stanowisku Rady na sposób ewakuacji danych - jednorazowy czy na zasadzie replikacji – rozwiązania są całkowicie od siebie odrębne. Ma to fundamentalne znaczenie dla całościowego podejścia do tego problemu. Zbyt mocne wchodzenie w szczegóły w zakresie uchwały Rady nie jest wskazane, ponieważ odpowiedź wskażą poszczególne analizy i strategie obronności państwa. Będzie należało przygotować infrastrukturę w Polsce do ponownego korzystania nie wiadomo przez jaki czas z danych zgromadzonych w e-Ambasadzie. Przykładem, z którego warto skorzystać jest doświadczenie Estonii - w 2017 r. wprowadziła takie rozwiązania w swoim kraju. Pan Przewodniczący poprosił członków Rady o zgłaszanie się do zespołu redakcyjnego. Zespół został utworzony.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Andrzej Dulka
4. Agnieszka Gryszczyńska
5. Agnieszka Jankowska
6. Jolanta Jaworska
7. Michał Kanownik
8. Agnieszka Kister
9. Janusz Kosiński
10. Anna Beata Kwiatkowska
11. Dariusz Milka
12. Jarosław Mojsiejuk
13. Józef Orzeł - Przewodniczący
14. Tomasz Rychter
15. Patrycja Staniszewska
16. Robert Trętowski
17. Sławomir Wojciechowski
18. Małgorzata Zakrzewska

Zaproszeni goście:

19. Wiesław Paluszyński, ekspert Rady
20. Jacek Paziewski, ekspert Rady

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

21. Katarzyna Bis – Płaza, Dyrektor Departamentu Projektów i Strategii w MC
22. Monika Pieniek, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC
23. Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC
24. Sylwia Stefaniak, Ekspertka w Departamencie Innowacji i Technologii w MC
25. Katarzyna Stopińska, Biuro Ministra w MC
26. Joanna Laskowska, Biuro Ministra w MC