PROTOKÓŁ z XXVII posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 25 lutego 2022 roku, o godzinie 12:00 w formie wideokonferencji.

Dyskusja Rady o zagadnieniach z zakresu tematyki wojskowej, telekomunikacyjnej oraz cyberbezpieczeństwa.

Pan Przewodniczący przekazał prośbę Pana Ministra Janusza Cieszyńskiego, aby Rada zajęła się tematami niezbędnymi ze względu na wojnę Rosji z Ukrainą i sytuację Polski, tj. tematami wojskowymi, telekomunikacyjnymi oraz cyberbezpieczeństwa. Prośba dotyczyła także sporządzenia spisu rekomendacji dla rządu, łącznie z postulatem znalezienia źródeł finansowania i powiększenia finansowania na projekty/programy.

Zaproponowano, aby jako pierwszy omówić temat powstania Wojskowego Systemu Telekomunikacyjnego. Pan Dyrektor płk Mariusz Chmielewski z Narodowego Centrum Badań Cyberprzestrzeni wspomniał o dwóch inicjatywach podjętych przez Ministerstwo Obrony Narodowej. Opracowano koncepcję przygotowania systemu łączności dla systemu kontroli bezpieczeństwa narodowego. Wyodrębnione zostały tam dwa obszary – obronny i ochronny. W obszarze obronnym odpowiedzialność spoczywa na siłach zbrojnych RP, w obszarze ochronnym na MSWiA. Rozgraniczenie musi zostać zaznaczone ze względu na m.in. ustawę o działach administracji rządowej[1]. Minister Obrony Narodowej ma także ograniczenia w zakresie dostarczania systemów dla pozostałych resortów. W sytuacjach wyższej konieczności dostarczono już pewne rozwiązanie, które jest w stanie integrować w rozległym systemie teleinformatycznym zwanym „MILNET-Z" (na poziomie zastrzeżone i niejawne) pewną informację przekazywaną do ministerstw oraz do poszczególnych pomiotów, m.in. kluczowych instytucji funkcjonujących w systemie bezpieczeństwa narodowego. Wskazano, że jest to poziom informacji zastrzeżonej. W koncepcji systemu łączności dla systemu kontroli bezpieczeństwa narodowego zostały wyodrębnione dwie enklawy informacyjne: tajna - działająca na poziomie ministerstw oraz zastrzeżona, która funkcjonuje od szczebla ministerstw do administracji państwowej na najniższych poziomach. Ta koncepcja została w prawie komunikacji elektronicznej tylko zasygnalizowana. Odrębne decyzje będą podlegały rekomendacji ministra ds. cyberbezpieczeństwa.

Wspomniano także, że GovTech KPRM, bazując na ww. inicjatywie, zbudował nowszą koncepcję - organizację komunikacji rządowej, dziedziczącą pewne rozwiązania z mechanizmów łączności dla systemu kontroli bezpieczeństwa narodowego, definiujące nie tylko poziom komunikacyjny, ale także pokazujące poszczególne usługi, które w tym systemie powinny działać (tj. komunikator szyfrowany, poczta elektroniczna, elektroniczny obieg dokumentów). Wymienione elementy wchodzą w skład systemu komunikacji rządowej wraz z tymi, które ten system dziedziczy – enklawa tajna oraz zastrzeżona.

Obecnie należy zbudować koncepcję systemu teleinformatycznego, który podlega akredytacji, mogącego spełniać określone role - jednak należałoby zwrócić się do Pana

[1] Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. 2021, poz. 1893)

Premiera, aby legislacyjnie pozwolił wdrażać pewne rozwiązania dotyczące tego systemu na poziomie krajowym i ministerstw. Takie rozwiązanie jest zbudowane - rozwiązanie techniczne o nazwie „MILNET-T"; wieloklauzulowe, wdrażane na poziomie strategicznym sił zbrojnych. Nie wiadomo jednak, czy to rozwiązanie będzie implementacją koncepcji, która w tej chwili powstała w ramach systemu komunikacji rządowej. To podsumowanie kilkuletniego procesu dojścia do rozwiązań koncepcyjnie doskonałych.

Na potrzeby aktualnych działań i przesyłania informacji, integracji MON oraz MSWiA, wykorzystywane są działające łącza teleinformatyczne i integrowane informacje ze Strażą Graniczną w systemie „MILNET-Z". System ten wojsko dostarcza w ograniczonym zakresie. Pewne instytucje są dołączane do dodatkowej rządowej enklawy, umożliwiającej korzystanie z usług na potrzeby komunikacji zastrzeżonej pomiędzy tymi instytucjami.

Wskazano, że obsługa systemu teleinformatycznego i cały system dołączania, zarządzania i administracji tym systemem spoczywa na organizatorze systemu. Należy brać pod uwagę ogrom wysiłku, który musi wprost przyjąć na siebie organizator systemu. Obecnie nie istnieją przepisy prawne umożliwiające wzięcie odpowiedzialności za tak rozległy system.

Pan Przewodniczący zauważył, że jest różnica między organizatorem, a właścicielem systemu – Rada powinna zająć stanowisko w tej sprawie. Trzeba połączyć te dwie funkcje, ale podmioty muszą być związane ze sobą m.in. administracyjnie, prawnie i hierarchicznie.

Jeden z członków Rady zauważył, że jest to wyspecjalizowany system o specyficznych zadaniach, które leżą w kompetencjach MON, natomiast nie można łączyć zadań Wojskowego Systemu Telekomunikacyjnego z systemami proponowanymi na gruncie ustawy o krajowym systemie cyberbezpieczeństwa.

Wskazano, że z koncepcji sygnalizowanych przez Pana Ministra Janusza Cieszyńskiego, ministerstwo właściwe do spraw cyfryzacji będzie nadzorowało bezpośrednio enklawę cywilną. Ze względu na wspomnianą już ustawę o działach administracji rządowej, Minister Obrony Narodowej nie może zabezpieczać systemu ochronnego państwa. W MON, w jednostkach wojskowych, wyodrębniono lokalnych administratorów - zorganizowano system najniższej obsługi technicznej, która przekłada się na szczelność systemu. Są to pewne procedury, które w wielu miejscach nie będą pasowały do domeny cywilnej.

Zauważono, że sprawą pilną jest budowanie strategicznej sieci bezpieczeństwa oraz powołanie operatora strategicznego. Pan Przewodniczący zauważył, że w rekomendacjach Rady powinien być zawarty postulat architektury komunikacji i bezpieczeństwa.

W dalszej części posiedzenia omówiono temat zagrożeń związanych z dezinformacją. Dezinformacja od jakiegoś czasu jest traktowana w doktrynie cyberbezpieczeństwa jako niezwykle istotny element. Przedstawiono listę priorytetów mogących być przedmiotem zainteresowania rządu oraz innych instytucji/organizacji. Najważniejszy jest brak systemowego podejścia i wskazania właściciela tematu, który zajmowałby się problemem dezinformacji. Takie działania prowadzi obecnie Narodowe Centrum Badań Cyberprzestrzeni, NASK, a także MSZ. Działania te są rozproszone i nie wykorzystują potencjału naukowego i

eksperckiego w Polsce. Pierwszą rekomendacją jest zmapowanie zasobów, którymi dysponuje nasz kraj oraz zbudowanie współpracy między poszczególnymi podmiotami sieci, mogącymi wspierać działania związane z analizą przestrzeni informacyjnej, narracji sentymentów i różnego rodzaju operacji wpływów psychologicznych, które są prowadzone. Ponadto zarekomendowano także:

- zainicjowanie „okrągłego stołu" przy którym mogą zasiąść przedstawiciele rządu, biznesu, trzeciego sektora, akademii i mediów - jego celem mogłoby być stworzenie programów ramowych walki z dezinformacją,
- opracowanie strategicznych programów finansowania badań nad dezinformacją i monitorowania sieci,
- pilne sfinansowanie nowoczesnych narzędzi analitycznych do monitorowania cyberprzestrzeni, które mogą być oparte o big data, wyposażone w analizę sentymentu, analizę audiowizualną umożliwiającą wieloplatformowe i wielojęzykowe badania,
- stworzenie profesjonalnych szkoleń z zakresu walki z zagrożeniami w obszarze komunikacji strategicznej, operacji informacyjnych i psychologicznych - są one w ograniczonym zakresie realizowane głównie dla urzędników i żołnierzy, jednak mogłyby być przeprowadzone w ramach szeroko rozumianej administracji,
- rozszerzenie programu edukacji publicznej w obszarze rozwoju kompetencji medialnych, krytycznego myślenia i niebezpieczeństw, które występują w sieci na inne grupy i podmioty,
- zainicjowanie kampanii społecznej w telewizji i prasie,
- wprowadzenie przepisów prawnych definiujących działania dezinformacyjne i ustalających sankcję w warunkach szczególnie istotnych dla zachowania suwerenności, bezpieczeństwa i demokracji, ponieważ te działania nasilają się i w coraz istotniejszy sposób dezintegrują oraz wpływają negatywnie na bezpieczeństwo kraju.

Poinformowano, że ze strony Ministerstwa Obrony Narodowej podjęta została kampania „Fejkoodporni" zorganizowana przez Centrum Operacyjne MON. Ponadto Laboratorium Bezpieczeństwa Informacji przeprowadza badania analizujące korelacje sytuacji mających znaczenie z punktu widzenia bezpieczeństwa. Ponadto w siłach zbrojnych istnieje kilka ośrodków, które zajmują się kwestiami szkoleń dla żołnierzy. Zaangażowanych podmiotów jest bardzo dużo, co stwarza problem dotyczący nieskonsolidowania tych działań. Uznano, że należy stworzyć centrum/ośrodek międzyresortowy, który zajmie się tym tematem.

Wspomniano, że Instytut Kościuszki wydał podręcznik dla szkół ponadpodstawowych stworzony pod patronatem pana Ministra Janusza Cieszyńskiego pt. „Z tarczą! Jak chronić się przed dezinformacją?", który mógłby zostać dystrybuowany do szkół.

W dalszej części dyskusji Pan Przewodniczący ocenił pomysł zainicjowania „okrągłego stołu" jako dobry, biorąc pod uwagę brak właściciela tematu oraz mnóstwo inicjatyw. Wiele już w tym zakresie zostało zrobione. Potrzeba także porozumienia z Krajową Radą Radiofonii i Telewizji. Rekomendacja Rady powinna pokazać architekturę dowodzenia walką z dezinformacją. Jeśli jest to broń, to wojsko powinno mieć ją na czele. Część cywilna nie jest w stanie objąć militarnej części zagrożenia.

W toku dyskusji członkowie Rady zgłaszali propozycje innych rekomendacji, m.in. doprowadzenia do powołania tymczasowych lub docelowych CSIRT-ów sektorowych.

Jeden z członków Rady zaproponował, zwrócenie się do KRRiT w kontekście zakresu dezinformacji i edukacji medialnej.

Wyrażono zdanie, że jednym z kluczowych elementów dotyczących walki z dezinformacją jest ustalenie definicji, wskazanie czy takie działanie ma charakter nielegalny oraz ustalenie podmiotu ścigającego za takie działanie. Na świecie istnieją różne rozwiązania. KRRiT ma jedno z najważniejszych narzędzi – zmienioną ustawę o radiofonii i telewizji, która wprowadza możliwości blokowania i usuwania treści w sytuacji rozpowszechniania przez platformę internetową określonego rodzaju informacji dotyczących (obecnie bardzo wąskich) kwestii związanych z działaniem mowy nienawiści czy treściami pornograficznymi. W związku z tym pojawiło się pytanie czy rozszerzyć to narzędzie o inne aspekty związane z działaniem nielegalnym w sieci, np. dezinformacją, czy kierunkowo Rada uważa, że powinien zostać powołany odrębny zespół międzyresortowy tworzący strategię, politykę działania w ramach dezinformacji, współpracujący z KRRiT na poziomie jej kompetencji. KRRiT w zakresie działania odnośnie dezinformacji kompetencji do końca nie posiada z powodu braku definicji określonej w przepisach prawa, stąd postulat o zmiany regulacyjne.

Pan Przewodniczący wskazał, że najpierw należy zdefiniować pojęcie w odniesieniu do polskiego prawa, określić narzędzia walki, wskazać podmioty i ich kompetencje prawne w tych kwestiach i oceniać czy nie wymagają one zmian. Nie warto wchodzić w szczegóły, jeśli obecnie jest problem ze zdefiniowaniem „czapki" instytucjonalnej.

W toku dyskusji zgłoszono temat rekomendacji w przedmiocie stworzenia „Ambasady Danych".

Ponownie nawiązano do tematu dezinformacji. Rozważano czy jest możliwość wprowadzenia mechanizmów utrudniających ataki oraz dezinformację, a jednym z nich byłoby wskazanie, jakie nazwy domenowe można rejestrować. Wydaje się, że na rejestr domeny.pl oraz sposób wykluczania z rejestracji określonych nazw domenowych rząd mógłby mieć wpływ.

Jeden z członków Rady zaproponował, aby pod rozwagę Rady poddać także podkreślenie potrzeby współpracy transatlantyckiej i paneuropejskiej w zapewnieniu bezpieczeństwa Polaków, a także rekomendację Rady w zakresie wsparcia Ukrainy w obszarze cyberbezpieczeństwa (należy rozważyć wsparcie finansowe, technologiczne i eksperckie).

Pojawiła się także propozycja uzupełnienia rekomendacji o konieczność jak najszybszego wzmocnienia inwestycyjnego Centrum Bezpieczeństwa w Rumunii, aby UE przyspieszyła prace nad uruchomieniem tego Centrum. Ponadto powinny znaleźć się środki budżetowe na doinwestowanie przede wszystkim samorządów w kwestii ochrony cybernetycznej. Stwierdzono, że w tym zakresie potrzebny jest ośrodek wsparcia cyberbezpieczeństwa. Trzeba zbudować sieć zarządzaną centralnie, zgodnie ze standardami.

Zgłoszono także temat ochrony centrów danych komercyjnych i niekomercyjnych z punktu widzenia reglamentacji dostawy energii elektrycznej.

Zaproponowano, aby wrócić do uchwały nr 7 w sprawie działań mających na celu zapobieganie kradzieży tożsamości z uwagi na aktualność większości postulatów, nabierających w kontekście wojny hybrydowej nowego znaczenia. Należy zwiększać bezpieczeństwo domeny.pl w świetle prac nad dyrektywą NIS. Możliwe jest także zwiększenie bezpieczeństwa w zakresie weryfikacji tożsamości osób korzystających z kanałów komunikacyjnych z administracją publiczną. Zwrócono także uwagę na problem związany ze spoofingiem. Dyskutowano o kwestiach z obszaru kradzieży tożsamości oraz cyberataków, które mają zostać zawarte w rekomendacjach dla Pana Ministra.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Konrad Ciesiołkiewcz
4. Andrzej Dulka
5. Agnieszka Gryszczyńska
6. Michał Kanownik
7. Janusz Kosiński
8. Karol Krawczyk
9. Anna Beata Kwiatkowska
10. Mirosław Maj
11. Dariusz Milka
12. Aleksandra Musielak
13. Józef Orzeł – Przewodniczący
14. Paweł Śniatała
15. Mateusz Tykierko
16. Małgorzata Zakrzewska

Zaproszeni goście:

17. płk Mariusz Chmielewski, Zastępca Dyrektora, Zastępca Dowódcy ds. informatyki w NCBC-DKWOC
18. Wiesław Paluszyński, ekspert Rady
19. Jarosław Mojsiejuk, ekspert Rady

Sekretariat Rady i pracownicy Kancelarii Prezesa Rady Ministrów:

20. Katarzyna Nosalska, Dyrektor Centrum Rozwoju Kompetencji Cyfrowych w KPRM
21. Aleksander Dumański, Dyrektor Departamentu Rozwoju Usług w KPRM
22. Michał Pukaluk, Dyrektor Departamentu Polityki Cyfrowej w KPRM
23. Ewa Świętochowska, Ekspertka, Departament Tożsamości Cyfrowej w KPRM
24. Krzysztof Głomb, Pełnomocnik Ministra Cyfryzacji do spraw współpracy z administracją samorządową Rzeczpospolitej Polskiej; Pełnomocnik Ministra

Cyfryzacji do spraw relacji z podmiotami działającymi na rzecz rozwoju kompetencji cyfrowych

25. Katarzyna Stopińska, KPRM
26. Anna Supeł, KPRM
27. Joanna Laskowska, KPRM