PROTOKÓŁ z VII posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 28 maja 2021 roku, o godzinie 13:00 w formie wideokonferencji.

Cyberprzestępczość – cyberbezpieczeństwo: Pani Agnieszka Gryszczyńska – struktura problemu; Pan Tadeusz Chomicki, Ambassador for Cyber & Tech Affairs oraz Pan Mirosław Broiło, Radca-Minister ds. Bezpieczeństwa Cybernetycznego i Technologicznego, Departament Polityki Bezpieczeństwa w Ministerstwie Spraw Zagranicznych.

Pan Ambasador T. Chomicki w swoim wystąpieniu podkreślił, że rozwój technologii cyfrowych stawia nas w obliczu przełomowego momentu. Cyberbezpieczeństwo jest warunkiem funkcjonowania we wszystkich sektorach i obszarach. Pan Ambasador wyjaśnił, że bardzo ważna jest współpraca międzynarodowa w identyfikacji źródeł zagrożeń. Wymiarów międzynarodowych jest kilka, można podzielić je na trzy kategorie, w których są podejmowane działania w wymiarze dwustronnym. Współpraca dwustronna dotyczy także działań politycznych, przykładem jest wspólne wspieranie się na poziomie politycznych deklaracji w przypadku ataku na jedno z państw.

Pan Ambasador podkreślił, że ważna jest współpraca w ramach podmiotów międzynarodowych, które mają twardą agendę, dotyczy ona Unii Europejskiej oraz NATO.

Wyjaśnił, że NATO od kilku lat dostrzega potrzebę polepszenia poziomu cyberbezpieczeństwa na poziomie organizacji oraz wspomagania na poziomie państw członkowskich. W tym celu NATO podjęło działania reformujące. Podczas szczytu NATO w 2016 r. podjęto formalną decyzję o uznaniu cyberprzestrzeni za oddzielną dziedzinę działań. Z punktu widzenia NATO ważne jest to, że obrona cybernetyczna jest częścią obrony zbiorowej. Do działań w cyberprzestrzeni stosuje się prawo międzynarodowe. Polityka obrony cybernetycznej NATO mówi o potrzebie wzmocnienia działań w zakresie zdolności do wykrywania zagrożeń i obrony przed zagrożeniami cybernetycznymi. Pan Ambasador wspomniał, że jednym z celów NATO, jak również UE, jest poprawa wymiany informacji o zagrożeniach. Polityka cyberbezpieczeństwa mówi o zwiększeniu współpracy, edukacji, wspólnych ćwiczeń oraz ilości szkoleń.

W ramach Unii Europejskiej w 2013 r. przyjęto pierwszą Strategię Cyberbezpieczeństwa. Pan Ambasador wymienił szereg innych ważnych dokumentów, które przyjęto po tym czasie, m.in.: w 2014 r. Rada przyjęła dokument dotyczący sposobu zarządzania Internetem. W 2015 r. przyjęto wnioski, które dały podstawy działań dyplomatycznych Unii i państw członkowskich w zakresie cyberprzestrzeni. W 2017 r. Rada przyjęła konkluzje, które dały możliwość stworzenia zestawu narzędzi do działań w zakresie cyberbezpieczeństwa oraz dokumenty wspólnych oświadczeń dotyczące wzmacniania odporności i obrony UE. W 2018 r. przyjęto dokumenty dotyczące współpracy przy budowie unijnych zdolności w zakresie cyberbezpieczeństwa. W 2020 r. przedstawiono projekt nowej Strategii Cyberbezpieczeństwa obejmujący cały szereg obszarów m.in. wzmocnienie odporności, suwerenności i przewodniej roli UE w cyberbezpieczeństwie.

Drugi obszar to zwiększenie zdolności unijnych do zapobiegania odpowiedzi na ataki cybernetyczne i niewłaściwe działania w cyberprzestrzeni. Pan Ambasador wspomniał, że ważnym wymiarem jest to, że strategia unijna kładzie duży nacisk, aby w procesach tworzenia odporności i zdolności cyberbezpieczeństwa było miejsce dla podmiotów pochodzących spoza administracji rządowych.

Zostało podkreślone, że bardzo ważnym wątkiem w obszarze współpracy unijnej jest kwestia podnoszenia suwerenności Unii w zakresie cyberprzestrzeni. Unia powinna budować swoją suwerenność, ale to nie powinno odbywać się kosztem sojuszy gwarantujących bezpieczeństwo.

Pan Ambasador podkreślił, że jednym z podejmowanych działań przez Unię jest utworzenie Europejskiego Centrum zajmującego się rozwojem zdolności w zakresie cyberbezpieczeństwa. Instytucja ta ma na celu działanie na rzecz wszystkich państw członkowskich oraz wspieranie współpracy różnych podmiotów w wymiarze horyzontalnym i wertykalnym.

Pan Minister M. Broiło wskazał, że Polska obejmuje przewodnictwo w Organizacji Bezpieczeństwa i Współpracy w Europie w 2022 r. Od czasu utworzenia OBWE po przyjęciu deklaracji końcowej Konferencji Bezpieczeństwa i Współpracy w Europie w 1975 r. w Helsinkach OBWE bardzo poszerzyło swój zakres. Zajmuje się wymiarem ekonomiczno-środowiskowym i tzw. wymiarem ludzkim rozumianym jako wymiar dotyczący praw człowieka. Najmłodszym podwymiarem jest wymiar cybernetyczny mieszczący się w wymiarze polityczno – wojskowym. W tym wymiarze, zadanie dla polskiego przewodnictwa to organizacja konferencji na temat bezpieczeństwa cybernetycznego. Planem do zrealizowania jest przyjęcie deklaracji na poziomie ministerialnym dotyczącej bezpieczeństwa cybernetycznego. Ogólny priorytet przewodnictwa Polski w obszarze bezpieczeństwa cybernetycznego to zwrócenie uwagi na wzmacnianie świadomości i budowania odporności społecznej w przestrzeni cybernetycznej.

Pan Ambasador przedstawił zależności pomiędzy procesami w obszarach ONZ. ONZ ma podział na komitety specjalizujące się w obszarach działań oraz organizacje, w uproszczeniu mówiąc, działające na obrzeżach ONZ. W ramach tzw. pierwszego Komitetu toczą się od wielu lat działania w zakresie odpowiedzialnego zachowania państw w cyberprzestrzeni. W celu wypracowania dokumentów powołano grupę ekspertów rządowych. Grupa ta wypracowała dokumenty obejmujące normy zachowania się państw w cyberprzestrzeni. 11 z tych norm zostało przyjętych przez Zgromadzenie Ogólne Narodów Zjednoczonych. Została także powołana otwarta grupa robocza, do której każde państwo mogło przystąpić. Trwały w niej spory o końcowy dokument. Przyjęto taki, który mówi o tym, że prawo międzynarodowe powinno się stosować do cyberprzestrzeni. Powołano kolejną otwartą grupę roboczą, której kadencja ma trwać 5 lat. W trzecim komitecie uruchomiono proces utworzenia międzynarodowej konwencji regulującej kwestię cyberprzestępczości. Pan Ambasador wspomniał, że zakończyła się praca grupy roboczej *international expert group* nie mająca statusu wypracowania konwencji. Miała porównywać zastosowania prawa do

cyberprzestrzeni oraz możliwości współpracy państw. Nie ma jednak decyzji o przedłużeniu prac tej grupy.

Następnie swoje wystąpienie rozpoczęła Pani Agnieszka Gryszczyńska, która omówiła m.in. rosnące statystyki w zakresie cyberprzestępczości. Problemem są oszustwa komputerowe w tym phishing. Większość badań, opracowań naukowych bądź popularnonaukowych, opiera się przede wszystkim na rozdziale 33 kodeksu karnego dodając ewentualnie oszustwo komputerowe z kwalifikacji art. 287 § 1-2 kodeksu karnego. Należy jednak zwrócić uwagę na oszustwa internetowe, czyli sposób działania sprawców przez Internet z kwalifikacji art. 286 § 1-3 kodeksu karnego, których jest bardzo dużo. Pandemia COVID-19 dla cyberprzestępców stała się okazją do zwiększenia skuteczności ataków opartych na socjotechnice. Problemy cyberbezpieczeństwa podczas pandemii były przedmiotem analiz ekspertów podczas XII Konferencji Naukowej Bezpieczeństwo w Internecie – Cyberpandemia. Wspomniano także o skutkach ataków cyberprzestępców, fałszywych sklepach internetowych, fałszywych smsach, przejmowaniu przez cyberprzestępców danych logowania do portali społecznościowych, kaskadowych alarmach bombowych. Można z cyberprzestępczością walczyć poprzez m.in. zwiększenie poziomu współpracy i wymianę danych pomiędzy państwami. W sprawach z zakresu cyberprzestępczości najważniejszy jest szybki dostęp do danych. Celowe jest wprowadzenie obowiązków związanych z przechowywaniem logów dostępowych oraz danych abonentów usług świadczonych drogą elektroniczną przez okres 12 miesięcy (retencja danych).

Dla podniesienia poziomu bezpieczeństwa i przeciwdziałania zjawisku kradzieży tożsamości celowe jest wprowadzenie obowiązków dotyczących lepszej weryfikacji tożsamości podmiotów korzystających z usług świadczonych drogą elektroniczną. Należy dokonać zmian w procesie pośrednictwa w rejestracji domen i nałożyć na rejestratorów obowiązki związane z weryfikacją tożsamości podmiotów rejestrujących domeny (abonentów). Jawny rejestr domeny .pl powinien zawierać dane kontaktowe do abonenta domeny (co najmniej adres e-mail). Aktualnie w bazie WHOIS nie są publikowane dane abonentów będących osobami fizycznymi. Dla porównania należy wskazać, że dla domeny *.eu baza WHOIS zawiera dane w postaci adresu mailowego abonenta. Celowe jest dalsze prowadzenie Listy Ostrzeżeń, należy jednak jej dalsze prowadzenie oprzeć o przepisy prawa powszechnie obowiązującego i wprowadzić procedurę odwoławczą.

Następnie Pan Ambasador T. Chomicki odpowiadał na pytania członków Rady. Wspomniał, że Polska jest pomysłodawcą inicjatyw w wymiarze międzynarodowym na poziomie dwustronnym i na poziomie organizacji np. UE, NATO czy też otwartych organizacji globalnych ONZ, OBWE. Polska jest inicjatorem szeregu *cyber dialog*, które obecnie są rozpoczęte. W zeszłym roku zostały uzgodnione z Londynem, Berlinem, Paryżem, Seulem dwustronne dialogi międzyresortowe w gronie administracji państwowej. Czasami rezultatem takich dialogów jest zgłoszenie wspólnej inicjatywy. W wymiarze unijnym czy NATO, Polska też zgłasza pomysły. Jest np. współinicjatorem kilku dokumentów unijnych w ostatnim czasie, jednak nie rangi regulacyjnej, lecz dotyczących podejmowanych kroków w zakresie budowy odporności. Są prace strategiczne w UE wychodzące poza obszar

cyberbezpiczeństwa dotyczące kompasu strategicznego i dla przykładu przygotowywany był wspólnie z Litwą dokument o *cyber resilience.* W zeszłym roku z Niemcami został przygotowany dokument dotyczący wzmocnienia *cyber diplomacy* oraz instrumentów dyplomacji unijnej. W ramach UE są podejmowane także działania wykraczające poza cyberbezpieczeństwo - w ramach działań dotyczących *single market* i *digital market* prowadzonych głównie przez KPRM w związku z przejęciem pionu UE z Ministerstwa Spraw Zagranicznych. To działania mające na celu zarówno ochronę rynku europejskiego jak i ochronę danych obywateli unijnych, narzucające wielkim partnerom (często amerykańskim firmom) standardy działania zgodne z przepisami unijnymi.

Pan Ambasador T. Chomicki zaznaczył, że należy tworzyć nawyki współpracy międzyresortowej w zakresie cyberbezpieczeństwa. Szkolenia są jednym z elementów przełamywania silosowego podejścia czy budowania poczucia pewnej wspólnoty osób, które zajmują się cyberbezpieczeństwem, niezależnie w jakim dziale rządu czy administracji pracują.

Pan Przewodniczący zaproponował, aby na jednym z posiedzeń Rady omówić kwestię *Digital Services Act* oraz *Digital Markets Act*, czyli kwestie usług cyfrowych i rynku internetowego, którymi zajmuje się Unia Europejska, a także odnieść się do projektu rozporządzenia w sprawie sztucznej inteligencji Komisji Europejskiej i rozpocząć prace Rady w tej materii.

Pan Przewodniczący zaproponował wsparcie i współpracę ze strony Rady z Panem Ambasadorem.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Konrad Ciesiołkiewicz
4. Janusz Cieszyński – Wiceprzewodniczący
5. Andrzej Dulka
6. Agnieszka Gryszczyńska
7. Michał Kanownik
8. Janusz Kosiński
9. Karol Krawczyk
10. Anna Beata Kwiatkowska
11. Mirosław Maj
12. Dariusz Milka
13. Aleksandra Musielak
14. Józef Orzeł - Przewodniczący
15. Bolesław Piasecki
16. Paweł Śniatała
17. Robert Trętowski
18. Mateusz Tykierko
19. Małgorzata Zakrzewska
20. Marcin Zarzecki

Zaproszeni goście:

21. Tadeusz Chomicki, Ambassador for Cyber & Tech Affairs
22. Mirosław Broiło, Radca-Minister ds. Bezpieczeństwa Cybernetycznego i Technologicznego, Departament Polityki Bezpieczeństwa w Ministerstwie Spraw Zagranicznych
23. Wiesław Paluszyński, ekspert Rady

Sekretariat Rady i pracownicy Kancelarii Prezesa Rady Ministrów:

24. Krzysztof Głomb, Pełnomocnik Ministra Cyfryzacji do spraw współpracy z administracją samorządową Rzeczpospolitej Polskiej

25. Monika Skrzyńska, Zastępca Dyrektora Departamentu Architektury Informacyjnej Państwa w KPRM
26. Katarzyna Staromłyńska-Gójska, KPRM
27. Anna Supeł, KPRM
28. Joanna Laskowska, KPRM