Rekomendacja Rady ds. Cyfryzacji w przedmiocie utworzenia systemów łączności strategicznej związanych z zapewnieniem bezpieczeństwa w Cyberprzestrzeni RP z 14 kwietnia 2022 r.

W celu zabezpieczenia i ochrony interesu Rzeczypospolitej Polskiej w obszarze działalności telekomunikacyjnej związanej z obronnością, bezpieczeństwem i porządkiem publicznym, niezbędne staje się utworzenie odpowiednich systemów telekomunikacyjnych.

Technologie informatyczne (IT) wykorzystywane przez operatorów usług kluczowych, dostawców usług cyfrowych, operatorów infrastruktury krytycznej (w tym operatorów telekomunikacyjnych), stanowią element krytyczny dla ciągłości działania Państwa oraz zapewnienia bezpieczeństwa obywatelom. Co więcej, bezpieczeństwo najważniejszych sektorów gospodarki, ze szczególnym uwzględnieniem sektora energii, zależy od zapewnienia niezakłóconego działania przemysłowych systemów sterowania (OT), także w kontekście obronnym. Równocześnie, zadania związane z zestawianiem najistotniejszych z punktu widzenia bezpieczeństwa Państwa sieci teleinformatycznych były realizowane przez wiele resortów, organów i instytucji, w różny sposób zarówno pod względem prawnym, organizacyjnym, jak i technicznym.

Rekomendacja ma na celu zapewnienie wysokiej jakości mechanizmów w zakresie obronności, podniesienie poziomu bezpieczeństwa i usprawnienie procedur realizacji zadań publicznych w obszarze telekomunikacji i łączności strategicznej w cyberprzestrzeni w kontekście tak militarnym, jak i cywilnym.

Wojskowy System Telekomunikacyjny

Działania w cyberprzestrzeni stanowią integralną część operacji prowadzonych przez Siły Zbrojne RP samodzielnie, jak i w układzie sojuszniczym oraz koalicyjnym. Jednym z projektowanych rozwiązań prawnych jest uregulowanie funkcjonowania Wojskowego Systemu Telekomunikacyjnego, którego zadania są ściśle związane z sieciami telekomunikacyjnymi wraz z infrastrukturą telekomunikacyjną o istotnym znaczeniu dla obronności, bezpieczeństwa lub porządku publicznego. Siły Zbrojne RP, jako podstawowy element systemu obronnego państwa, mają obowiązek angażować się w działania w cyberprzestrzeni na tym samym poziomie, co w powietrzu, na lądzie i na morzu. Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni muszą więc obejmować: rozpoznawanie zagrożeń, ochronę i obronę systemów teleinformatycznych oraz zwalczanie źródeł zagrożeń.

Uregulowanie funkcjonowania Wojskowego Systemu Telekomunikacyjnego na poziomie ustawowym pozwala na udoskonalenie struktur wojskowych, które zapewnią skuteczniejsze planowanie, dowodzenie i zarządzanie zasobami, umiejętnościami i zdolnościami. Wojskowy System Telekomunikacyjny będzie pozwalał na bieżące rozpoznanie zagrożeń oraz ocenę sytuacji w celu podjęcia właściwych środków ochrony lub aktywnego przeciwdziałania źródłom zagrożeń. Mając na uwadze dynamikę rozwoju technologii tworzących środowisko, jakim jest cyberprzestrzeń, resort obrony narodowej dąży do wytworzenia bądź pozyskania

nowatorskiego zestawu narzędzi, który podniesie ich skuteczność działania w tej domenie. Tym samym rekomenduje się, aby zadania właścicielskie i organizatorskie funkcjonowania Wojskowego Systemu Telekomunikacyjnego dalej realizował Minister Obrony Narodowej.

Operator strategicznej sieci bezpieczeństwa (OSSB)

Zapewnienie zdolności w zakresie łączności służbom bezpieczeństwa i porządku publicznego, a także wysokiego poziomu bezpieczeństwa sieci teleinformatycznych stanowiących komunikacyjny kręgosłup Państwa to wyzwanie, dla realizacji którego planuje się powołanie instytucji Operatora strategicznej sieci bezpieczeństwa (OSSB). W założeniach ustawowych strategiczna sieć bezpieczeństwa będzie uruchamiana i zarządzana przez OSSB wskazywanego w zarządzeniu Prezesa Rady Ministrów.

Regulacje prawne

Ze względu na zagrożenia o charakterze konfliktów hybrydowych, zakres kompetencji dotyczących telekomunikacji obejmie sprawy z obszaru *stricte* związanego z bezpieczeństwem także wewnętrznym w cyberprzestrzeni, w warunkach pokoju, co oznacza konieczność współpracy międzyresortowej. Jednocześnie nowy model koordynacji zadań i nowa architektura powiązań i zależności obu systemów na poziomie centralnym, tworzenie uwarunkowań związanych ze współdziałaniem obu systemów, pozwoli na rozdział zadań publicznych w zakresie obsługi sieci strategicznych od innych aktywności związanych z zapewnieniem cyberbezpieczeństwa, w warunkach normalnego funkcjonowania Państwa, jak i w warunkach zagrożeń czy stanów nadzwyczajnych.

Należy zaznaczyć, iż odpowiedzialność za zapewnienie bezpieczeństwa usług leży przede wszystkim po stronie Państwa. Z tego powodu kluczowe stają się działania wspierające budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa, uwzględniając ich różnorodną specyfikę i różny stopień dojrzałości w dziedzinie telekomunikacji. Dlatego tak istotne staje się powierzenie zadań podmiotom posiadającym doświadczenie na rynku telekomunikacyjnym.

Ponadto, istotne staje się reagowanie na incydenty poważne, szczególnie w przypadku wystąpienia incydentów ponadsektorowych. W celu realizacji tego zadania, aktywność **OSSB** wydaje się kluczowa. W obecnych warunkach organizacji Państwa nie ma podmiotu, który realizowałby zadania uwzględniając całościowy i ponadsektorowy aspekt bezpieczeństwa w cyberprzestrzeni Rzeczpospolitej Polskiej.

Jedną z zasadniczych funkcji OSSB powinno stać się zapewnienie łączności mobilnej na potrzeby służb i organów zarzadzania kryzysowego w przypadkach związanych z wszelkimi katastrofami naturalnymi, awariami technicznymi i przeciwdziałaniem ich skutkom. Sieć OSSB powinna być więc także elementem infrastruktury przygotowanej do realizacji funkcji Crisis Managment - częścią cywilną w ramach NATO (zarówno Civil Emergency Planning i Consequence Management) oraz do współpracy ze ściśle zdefiniowaną częścią wojskową.

Budowanie strategicznej sieci bezpieczeństwa (SSB) zapewni skuteczniejsze planowanie, dowodzenie i zarządzanie zasobami, umiejętnościami i zdolnościami. Mając na uwadze

dynamikę rozwoju technologii tworzących środowisko, jakim jest cyberprzestrzeń, niezbędne staje się dążenie do wytworzenia bądź pozyskania nowatorskiego zestawu narzędzi, który podniesie ich skuteczność działania w tej domenie.

Zwiększenie skuteczności mechanizmów koordynacji kierowania bezpieczeństwem narodowym, w tym obroną Państwa, rozpoznawanie, monitorowanie i zapobieganie zagrożeniom, a także zapewnienie skutecznych mechanizmów reagowania oraz podnoszenie skuteczności służb państwowych to warunki konieczne do prawidłowego funkcjonowania Państwa oraz realizacji jego celów rozwojowych. Problematyka bezpieczeństwa narodowego obejmuje szereg zagadnień, tak z zakresu bezpieczeństwa zewnętrznego, jak i bezpieczeństwa wewnętrznego. Zmienia się międzynarodowe środowisko bezpieczeństwa Polski. Wnosimy także o możliwie szerokie wykorzystywanie tworzonych w Polsce technologii do budowy tej sieci.

Inwazja rosyjska na Ukrainę, konflikty w bezpośrednim lub bliskim sąsiedztwie Polski, niestabilność na wschodniej flance Sojuszu Północnoatlantyckiego i Unii Europejskiej oraz próby zmierzające do zmiany układu sił i odbudowy rosyjskiej strefy wpływów przy wykorzystaniu środków militarnych oraz ekonomicznych, to obecnie najważniejsze czynniki wpływające na bezpieczeństwo Polski i całego regionu.

Utworzenie WST oraz OSSB (przekazanie zadań OSSB do realizacji jednoosobowej Spółce Skarbu Państwa) stanowi początek realizacji działań na rzecz rozwoju strategicznej infrastruktury państwa również przy wykorzystaniu środków militarnych i obronnych w środowisku komunikacji elektronicznej i cyberprzestrzeni.

Należy zaznaczyć, iż w obliczu wzrostu znaczenia zagrożeń hybrydowych dla cyberbezpieczeństwa, które mogą utrudnić sprawne funkcjonowanie państwa, **NATO a także UE pozostają głównymi zewnętrznymi filarami polskiej polityki bezpieczeństwa i rozwoju**.

Polskim priorytetem są działania na rzecz osiągnięcia synergii wysiłków poszczególnych organów, instytucji i służb państwowych odpowiedzialnych za bezpieczeństwo Państwa, która pozwoli na bardziej efektywne rozpoznanie i przeciwdziałanie zagrożeniom oraz zwiększy odporność strategiczną.

Projektowane założenia dotyczące WST oraz OSSB stanowią element realizacji tego celu. Pożądanym efektem jest tworzenie zintegrowanego systemu bezpieczeństwa sieci. Jego wzmocnieniu służy, także modernizacja sieci strategicznych, przy znaczącym udziale krajowych spółek sektora publicznego. Założenia dotyczące powstania WTS oraz OSSB stanowią odpowiedź nie tylko na wskazane powyżej potrzeby, ale także wypełniają naturalne i oczywiste oczekiwania społeczne.