NOWA STRATEGIA BEZPIECZEŃSTWA NARODOWEGO Z PODPISEM PREZYDENTA. SZCZEGÓLNA ROLA CYBERPRZESTRZENI ORAZ PRZESTRZENI INFORMACYJNEJ

Prezydent Andrzej Duda na wniosek Prezesa Rady Ministrów zatwierdził dziś nową Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Dokument szeroko omawia problematykę cyberbezpieczeństwa i przestrzeni informacyjnej.

Tekst Strategii Bezpieczeństwa Narodowego został podpisany przez Prezydenta Andrzeja Dudę w trakcie uroczystości w Pałacu Prezydenckim. Oznacza to, że dotychczasowa strategia z 2014 roku właśnie straciła moc. Pełen tekst dokumentu jest już dostępny na stronie BBN.

Strategia bardzo szeroko porusza kwestie cyberbezpieczeństwa i przestrzeni informacyjnej, którym poświęcono osobne działy, podkreślając tym samym ich rangę. Określono w nim również najważniejsze zagrożenia oraz wyzwania w tym obszarze.

Przedstawiając środowisko bezpieczeństwo Polski, strategia jako główne zagrożenie dla bezpieczeństwa kraju wskazuje na neoimperialną politykę władz Federacji Rosyjskiej, w tym prowadzenie działań, które zostały w dokumencie określone jako „wszechstronne i kompleksowe działania za pomocą środków pozamilitarnych (w tym: cyberataki, dezinformacja) celem destabilizacji struktur państw społeczeństw zachodnich oraz wywoływania podziałów wśród państw sojuszniczych”.

Podkreślono również konieczność przyjęcia założenia, że Rosja będzie w dalszym ciągu kontynuowała politykę podważania obecnego ładu międzynarodowego, opartego na prawie międzynarodowym, w celu odbudowy pozycji mocarstwowej i stref wpływów.

> *W kontekście rewolucji cyfrowej należy uwzględnić szczególną rolę cyberprzestrzeni oraz przestrzeni informacyjnej. Stwarza to również pole do dezinformacji i manipulacji informacją, co wymaga prowadzenia skutecznych działań z zakresu komunikacji strategicznej*
>
> *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*

Dokument podkreśla również, że działania poniżej progu wojny, w tym działania o charakterze hybrydowym, w dalszym ciągu będą pozostawać istotnym środkiem polityki, służącym zarówno

podmiotom państwowym, jak i pozapaństwowym do osiągania ich celów. Dlatego też, jak wskazuje nowa strategia „można spodziewać się dalszego rozwoju zdolności do prowadzenia działań w wielu wymiarach, w tym w cyberprzestrzeni i w przestrzeni kosmicznej".

Systemy łączności są kluczowym elementem zasobów bezpieczeństwa narodowego

W strategii wskazano na konieczność uwzględnienia postępu w dziedzinie technologii cyfrowych oraz efektywnego wykorzystania najnowszych technologii. „Rozwój rozwiązań opartych na szerokopasmowych sieciach łączności stacjonarnej i mobilnej (5G i kolejnych generacji), Internecie Rzeczy, chmurze obliczeniowej, technologii kwantowych, automatyzacji usług, uczeniu maszynowym, nanotechnologii i sztucznej inteligencji stwarza nowe możliwości rozwojowe dla Polski, równocześnie generując nieznane wcześniej zagrożenia" – czytamy w dokumencie. Jako wyzwanie dla Polski wskazano włączenie się w wyścig w obszarze wskazanych technologii, dającym Polsce możliwość wyjścia z roli wyłącznie użytkownika i dołączenie do grona krajów o efektywnie funkcjonującej gospodarce cyfrowej, dostarczających rozwiązania i współtworzących międzynarodowe standardy.

„Sieci łączności stacjonarnej i mobilnej są podstawą wymiany informacji" –określa dokument. Zaliczono do nich łączność głosową, transmisję danych, wideo i szeroko pojęty dostęp do Internetu dla wszystkich innych kluczowych sektorów gospodarki. Jednocześnie podkreślono, że systemy łączności są kluczowym elementem zasobów bezpieczeństwa narodowego i gotowości na wypadek sytuacji kryzysowych – są zatem ważnym elementem krajowej infrastruktury krytycznej. „W tym zakresie kluczowym wyzwaniem jest rozbudowa bezpiecznych i nowoczesnych sieci telekomunikacyjnych zdolnych obsłużyć coraz większą ilość użytkowników końcowych i systemów – czytamy w dokumencie.

CEL: Uzyskać zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni

Nowa Strategia Bezpieczeństwa Narodowego została podzielona na 4 filary:

- FILAR I - BEZPIECZEŃSTWO PAŃSTWA I OBYWATELI
- FILAR II - POLSKA W SYSTEMIE BEZPIECZEŃSTWA MIĘDZYNARODOWEGO
- FILAR III - TOŻSAMOŚĆ I DZIEDZICTWO NARODOWE
- FILAR IV - ROZWÓJ SPOŁECZNY I GOSPODARCZY. OCHRONA ŚRODOWISKA

W ramach pierwszego filaru zawarto osobny dział poświęcony cyberbezpieczeństwu i przestrzeni informacyjnej.

Strategia za cel główny w dziale „cyberbezpieczeństwo" określiła przyczynienie się do podniesienia poziomu odporności na cyberzagrożenia a także zwiększenia poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. Zapewnienie go ma nastąpić poprzez realizację 6 rodzaju działań:

- zwiększanie poziomu odporności systemów informacyjnych wykorzystywanych w sferze publicznej, prywatnej oraz militarnej i cywilnej oraz osiągnąć zdolność do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia;
- wzmacnianie defensywnego potencjału państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa;
- pozyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni;
- rozwijanie krajowych zdolności w obszarze testowania, badania, oceny i certyfikacji rozwiązań i usług z obszaru cyberbezpieczeństwa;

- rozwijanie kompetencji, wiedzy oraz świadomości zagrożeń i wyzwań wśród kadr administracji publicznej oraz w społeczeństwie w obszarze cyberbezpieczeństwa;
- wzmacnianie i rozbudowywanie potencjału państwa, które rozumiane jest jako wspieranie rozwoju rodzimych rozwiązań w zakresie cyberbezpieczeństwa oraz prowadzenie finansowanych przez państwo prac badawczo-rozwojowych w obszarze nowoczesnych technologii, m.in. uczenia maszynowego, Internetu Rzeczy, szerokopasmowych sieci łączności stacjonarnej i mobilnej (5G i kolejnych generacji), w tym także współpracę z uczelniami i instytucjami naukowymi oraz przedsiębiorstwami – zarówno z sektora publicznego, jak i prywatnego.

W dziale „przestrzeń informacyjna" za cel główny określono „zapewnienie bezpiecznego funkcjonowania państwa i obywateli w przestrzeni informacyjnej". Do realizacji tego celu strategia wskazuje na konieczność realizacji działań w zakresie:

- zbudowania zdolności do ochrony przestrzeni informacyjnej (w tym do systemowego zwalczania dezinformacji) na poziomie strategicznym. Przestrzeń informacyjna rozumiana jest jako przenikające się warstwy przestrzeni: wirtualnej (warstwa systemów, oprogramowania i aplikacji), fizycznej (infrastruktury i sprzętu) i poznawczej (kognitywnej);
- stworzenia jednolitego systemu komunikacji strategicznej państwa, którego zadaniem powinno być prognozowanie, planowanie i realizowanie spójnych działań komunikacyjnych, przy wykorzystaniu szerokiej gamy kanałów komunikacji i mediów oraz wykorzystywać narzędzia rozpoznania oraz oddziaływania w różnych obszarach bezpieczeństwa narodowego;
- aktywnego przeciwdziałania dezinformacji. Działanie to ma zostać osiągnięte poprzez budowę zdolności i stworzenie procedur współpracy z mediami informacyjnymi oraz społecznościowymi, przy zaangażowaniu obywateli i organizacji pozarządowych;
- dążenia do zwiększenia świadomości społecznej o zagrożeniach związanych z manipulacją informacją poprzez edukację w zakresie bezpieczeństwa informacyjnego.

CEL: Uzyskać zdolności operacyjne do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, rozwijać wojska obrony cyberprzestrzeni oraz zbudować zdolności do prowadzenia działań w przestrzeni kosmicznej, jak również do działań informacyjnych.

W dokumencie wykazano konieczność zintegrowania wszystkich systemów zarządzania bezpieczeństwem narodowym w tym systemu cyberbezpieczeństwa.

W zakresie wzmocnienia zdolności operacyjnych sił zbrojnych wskazano na niezbędny element jakim jest uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, rozwijania wojska obrony cyberprzestrzeni oraz budowy zdolności do prowadzenia działań w przestrzeni kosmicznej, jak również do działań informacyjnych.

Jednocześnie położono nacisk na konieczność wykorzystania bezzałogowych i autonomicznych systemów, zautomatyzowanych i zrobotyzowanych platform uzbrojenia wykorzystujących sztuczną inteligencję, a także systemów broni precyzyjnego rażenia na dalekie odległości, w tym rakiet balistycznych i manewrujących. "Za szczególnie niebezpieczny uznaje się wzrost prawdopodobieństwa użycia taktycznej broni jądrowej w klasycznej operacji zbrojnej, w tym jako elementu deeskalacji konfliktu" - czytamy dalej.

Z dniem zatwierdzenia nowej Strategii przez Prezydenta Rzeczypospolitej Polskiej traci moc Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej wydana w 2014 roku.