OCENA ZAPISÓW STRATEGII BEZPIECZEŃSTWA NARODOWEGO RZECZYPOSPOLITEJ POLSKIEJ 2020_GEN. STANISŁAW KOZIEJ

"W odniesieniu do spraw cyber-, jak i info- Strategia Bezpieczeństwa Narodowego ogranicza się tylko do zadań przygotowawczych (w zakresie strategii preparacyjnej: budować, organizować potencjał, rozwijać zdolności, doskonalić…), bez formułowania zdań co do sposobów strategicznego działania państwa w stosunku do wyzwań, ryzyk, zagrożeń i szans (czyli zadań strategii operacyjnej)" - stwierdził generał Stanisław Koziej, były wiceminister obrony narodowej, oraz były szef Biura Bezpieczeństwa Narodowego w ramach oceny Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020.

12 maja 2020 prezydent Andrzej Duda zatwierdził tekst nowej Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020. Wydaje się, że ważnym elementem tego dokumentu jest cyberbezpieczeństwo i bezpieczeństwo informacyjne. Jak wskazują zapisy dokumentu, dostrzeżono ich strategiczne znaczenie dla bezpieczeństwa państwa.

CyberDefence24.pl skierował prośbę do wybranych ekspertów z prośbą o dokonanie oceny zapisów nowej strategii pod względem zawartych w niej zapisów odnośnie cyberbezpieczeństwa. skierowaliśmy trzy pytania odnoszące się do interpretacji zagrożeń, ocenę wskazania Rosji jako jedynego kierunku zagrożeń dla obszaru informacyjnego oraz jakie są kluczowe zagrożenia, które pominięto w dokumencie.

Zestawienie opinii wszystkich ekspertów zawarte zostało w ramach analizy: "(Cyber)bezpieczna Polska. Strategia Bezpieczeństwa Narodowego okiem ekspertów"

Poniżej dostępna jest pełna treść oceny generała Stanisława Kozieja - byłego wiceministra obrony narodowej, oraz byłego szefa Biura Bezpieczeństwa Narodowego

Jaka jest Pana opinia na temat zapisów strategii w kontekście zagrożeń w obszarze informacyjnym? Czy dokument interpretuje zagrożenia w obszarze informacyjnym we właściwy sposób?

Bardzo dobrze, że problematyka ta została szczególnie wyeksponowana w Strategii Bezpieczeństwa Narodowego. Szkoda jednak, że nie podjęto próby zintegrowanego podejścia do problematyki cyberbezpieczeństwa i infobezpieczeństwa. Sygnalizowaliśmy w BBN taką potrzebę już w projekcie Doktryny bezpieczeństwa informacyjnego w 2015 roku (https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf), w nawiązaniu do Doktryny Cyberbezpieczeństwa (https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf) – sugerując w przyszłości zintegrowanie tych dwóch dokumentów. Trudno bowiem prowadzić odrębne operacje, a tym bardziej budować odrębne podsystemy w dziedzinie bezpieczeństwa informacyjnego i

cyberbezpieczeństwa. Myślę, że można było skorzystać z tej sugestii.

Po drugie – zarówno w odniesieniu do spraw cyber-, jak i info- Strategia Bezpieczeństwa Narodowego ogranicza się tylko do zadań przygotowawczych (w zakresie strategii preparacyjnej: budować, organizować potencjał, rozwijać zdolności, doskonalić…), bez formułowania zdań co do sposobów strategicznego działania państwa w stosunku do wyzwań, ryzyk, zagrożeń i szans (czyli zadań strategii operacyjnej). Wiąże się to z podstawową ułomnością całej strategii, w której w ogóle nie ma strategii operacyjnej (!!!). Więcej na ten temat: https://pulaski.pl/wp-content/uploads/2020/05/Pulaski_Policy_Paper_Nr_04_20.pdf

Czy w Pana opinii bezpośrednie wskazanie jedynie na Rosję jako na jedyny kierunek zagrożeń dla obszaru informacyjnego jest właściwym rozwiązaniem?

Prawdę mówiąc nie widzę w Strategii Bezpieczeństwa Narodowego takiego ograniczenia kierunków, czy też źródeł zagrożeń informacyjnych, w tym cyberzagrożeń. Raczej w ogóle nie wskazuje się podmiotów mogących takie zagrożenia dla Polski generować. Ale gdyby tak interpretować wzmiankę w tym kontekście o Rosji w I Rozdziale, gdzie omawia się środowisko bezpieczeństwa, czyli jako ograniczenie się tylko do zagrożeń rosyjskich, to byłoby to rzeczywiście zdecydowanie za mało. Infosfera ma wymiar globalny (a praktycznie - nawet ponadglobalny) i kierowanie się tradycyjną metodą podejścia typową dla obecności w przestrzeni fizycznej (geograficznej) nie wydaje się właściwe. Oczywiście także w infosterze (jak w geosferze) Rosja generuje dla nas zagrożenia bezpośrednie, intencjonalne (celowe) i musi być priorytetowym punktem odniesienia, ale wszelkie inne podmioty (polityczne i… niepolityczne!, o których w tej strategii się zapomina) są dla nas także „infosąsiadami" (na dobre i na złe) w infosferze i mogą na naszą świadomość informacyjną łatwo oddziaływać pośrednio, nawet nieintencjonalnie, ale ze szkodą dla naszych interesów narodowych. Warto byłoby zatem ten aspekt uwzględnić w ocenie zagrożeń info/cyber.

Jakich kluczowych zagrożeń w obszarze informacyjnym zabrakło w dokumencie?

Przede wszystkim na bezpieczeństwo informacyjne, w tym cyberbezpieczeństwo, podobnie jak na wszystkie inne dziedziny bezpieczeństwa, patrzeć należy nie tylko przez pryzmat zagrożeń, ale także szans (korzystnych dla nas okazji zewnętrznych lub stwarzanych przez własne przewagi) oraz ryzyk (związanych z własnymi słabościami i błędami). Gdzie jak gdzie, ale w infobezpieczeństwie, gdzie ważny jest nie tylko „twardy" potencjał, ale także środki i metody z arsenału „soft power", takie podejście jest jak najbardziej potrzebne. Zabrakło go w obecnej Strategii Bezpieczeństwa Narodowego.

Po drugie – punktem odniesienia są tylko zewnętrzne zagrożenia informacyjne, nic nie mówi się o zagrożeniach (oczywiście także szansach i ryzykach) wewnętrznych.

I po trzecie - brakuje odniesienia do podmiotów (firm) prywatnych, zarówno w kontekście generowania przez takie obce podmioty zagrożeń istotnych dla interesów narodowych (np. gospodarczych), jak i wrażliwości na zagrożenia własnych podmiotów prywatnych, a także – co szczególnie istotne – brak uwzględnienia ich w celach i zadaniach info/cyber/bezpieczeństwa, w kontekście ich udziału w przeciwdziałaniu zagrożeniom, redukowaniu ryzyk i wykorzystywaniu szans dla bezpieczeństwa Polski.