Cyberdefence 24

01.09.2020

OCENA ZAPISÓW STRATEGII BEZPIECZEŃSTWA NARODOWEGO RZECZYPOSPOLITEJ POLSKIEJ 2020_KRZYSZTOF GAWKOWSKI

Niestety nowa strategia wydaje się być dokumentem w wielu miejscach niedopracowanym, a na pewno dotyczy to obszarów cyberbezpieczeństwa i ochrony informacji - stwierdził Krzysztof Gawkowski, dyrektor Polskiego Instytutu Cyberbezpieczeństwa 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 Krzysztofa Gawkowskiego, dyrektor Polskiego Instytutu Cyberbezpieczeństwa.

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

Strategia Bezpieczeństwa Narodowego powinna być podstawowym dokumentem ustanawiającym fundamenty systemu bezpieczeństwa narodowego. Niestety nowa strategia wydaje się być dokumentem w wielu miejscach niedopracowanym, a na pewno dotyczy to obszarów cyberbezpieczeństwa i ochrony informacji. Interpretacja zagrożeń informacyjnych jest na dużym poziomie ogólności, co oznacza nie mniej ni więcej, że powinniśmy robić dużo ale nic się nie stanie jak zrobimy mało.

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

Zagrożenia informacyjne to problem globalny. W zależności od operacyjnego zainteresowania różnych

państw, organizacji terrorystycznych czy transnarodowych korporacji, może być wykorzystywany do wywierania rożnego rodzaju presji zarówno na rządy jak i opinię społeczną. Wskazywanie zatem jednego konkretnego państwa jako ewentualnego miejsca, z którego można spodziewać się aktywnych działań dezinformacyjnych, jest dużym błędem. Niektórzy powiedzą nawet ostrzej, że to wyraz dużej niekompetencji autorów dokumentu.

Jakich kluczowych zagrożeń w obszarze informacyjnym zabrakło w dokumencie?

Luki w SBN na poziomie zabezpieczenia pola informacyjnego są dość duże. Nie zostały wskazane konkretne działania jakie powinniśmy jak państwo podejmować, w celu przeciwdziałania szerzeniu dezinformacji. Od wielu lat mówi się o specjalnych jednostkach, które na co dzień będą monitorowały przestrzeń informacyjną i przeciwdziałały ewentualnym atakom. W tej sprawie strategia milczy. Brak również szczegółów dotyczących kształcenia społeczeństwa w kwestii rozpoznawania nieprawdziwych informacji.