(CYBER)BEZPIECZNA POLSKA. STRATEGIA BEZPIECZEŃSTWA NARODOWEGO OKIEM EKSPERTÓW

Czy autorzy przyjętej w maju br. Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej w sposób odpowiedni zinterpretowali zagrożenia dla bezpieczeństwa narodowego w kontekście zagrożeń informacyjnych? O ocenę dokumentu poprosiliśmy ekspertów.

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. Jego zapisy wskazują, że dostrzeżono ich strategiczne znaczenie dla bezpieczeństwa państwa.

W ramach IV filarów, na które została podzielona treść dokumentu, cyberbezpieczeństwo zostało zaliczone do I z nich. Zauważa się w nim konieczność podniesienia odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji oraz działań edukacyjnych i promujących tzw. cyber higienę. Podkreśla się również ciągły rozwój krajowego systemu cyberbezpieczeństwa (KSC).

Strategia szeroko, jak na dokument tego typu, porusza kwestie cyberbezpieczeństwa i przestrzeni informacyjnej, którym poświęcono osobne działy, podkreślając tym samym ich rangę, jednak czy zapisy w niej zawarte właściwie interpretują polskie uwarunkowania w tym obszarze?

Zwróciliśmy się do wybranych ekspertów z prośbą o dokonanie oceny zapisów nowej strategii pod względem zawartych w niej treści odnośnie cyberbezpieczeństwa. Komentarza do sprawy zdecydowali się udzielić:

- doktor Dominika Dziwisz - Uniwersytet Jagielloński (UJ),
- Krzysztof Gawkowski - dyrektor Polskiego Instytutu Cyberbezpieczeństwa,
- inżynier Joanna Karczewska - Audytor SI, ISACA Warsaw Chapter,
- profesor Waldemar Kitler - Akademia Sztuki Wojennej (AszWoj),
- generał Stanisław Koziej - były wiceminister obrony narodowej, oraz były szef Biura Bezpieczeństwa Narodowego,
- generał broni rezerwy dr Mirosław Różański - prezes Fundacji Bezpieczeństwa i Rozwoju STRATPOINTS, doradca POLSKA 2050.

Do każdego eksperta skierowaliśmy trzy pytania odnoszące się do interpretacji zagrożeń, ocenę wskazania Rosji jako jedynego kierunku zagrożeń dla obszaru informacyjnego oraz kluczowych zagrożeń, które pominięto w dokumencie.

Jaka jest pani/pana opinia na temat zapisów strategii w kontekście zagrożeń w obszarze informacyjnym? Czy dokument interpretuje zagrożenia w obszarze informacyjnym we

właściwy sposób?

Dziwisz: „Cyberbezpieczeństwo oraz bezpieczeństwo informacyjne zostały wyodrębnione w Strategii jako dwa oddzielne cele pierwszego filaru. To słuszne rozwiązanie, bo dzięki temu te obszary działania, obok zarządzania bezpieczeństwem narodowym i podniesienia odporności państwa na zagrożenia, potraktowano priorytetowo. Jest to sygnałem, że SBN stara się nadążyć za zmianami i współczesnymi wyzwaniami bezpieczeństwa, a także akcentuje potrzebę rozwoju zdolności w tym zakresie […] Można odnieść wrażenie, że zapisy dotyczące bezpieczeństwa informacyjnego zostały potraktowane w Strategii poprawnie, ale w sposób standardowy, przewidywalny i nieco lakoniczny. Niestety, w przeciwieństwie do Strategii z 2014 r. brakuje zapisu o konieczności zbalansowania stosowania środków służących zachowaniu bezpieczeństwa państwa i wolności osobistej obywateli oraz ochrony praw jednostki, w tym przede wszystkim prawa do prywatności. W czasach powszechnej, elektronicznej inwigilacji powinno to być standardem".

Gawkowski: „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".

Karczewska: „Dokument nie uwzględnia zagrożeń wynikających z niedbalstwa, nieuctwa i nonszalancji osób odpowiadających za cyberbezpieczeństwo w sektorze publicznym i prywatnym oraz ich niechęci do przestrzegania polityk i procedur, standardów i dobrych praktyk we wszystkich warstwach przestrzeni informacyjnej".

Kitler: „W moim przekonaniu zagrożenia w obszarze informacyjnym, jak i inne, potraktowano dość ogólnikowo, nie tylko pod względem ilościowy, ale i jakościowym. Jest to dość dziwne, bowiem są w Polsce dokumenty strategiczne lub ich solidne projekty, które tę problematykę podejmują należycie […] Uważam, że nawiązania do zagrożeń w obszarze informacyjnym, choć są poprawne, to poczynione zostały w niezwykle skąpym i mało kompleksowym zakresie zważywszy na istotę bezpieczeństwa informacyjnego. […] Czy dokument interpretuje zagrożenia w obszarze informacyjnym we właściwy sposób? może być tylko jedna – nie. A wystarczyło, być może, zobaczyć jak to zrobili Amerykanie w swojej strategii z 2017 r.".

Koziej: „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".

Różański: „Strategia Bezpieczeństwa Narodowego (SBN) została zredagowana w taki sposób, by można ją było interpretować, a nie traktować jak swoisty „dekalog" bezpieczeństwa. Zapisy SBN w mają charakter postulatów, „zwiększyć zdolność" , „rozwijać zdolności", „dołączyć do grona". Dotyczy to również oceny zagrożeń, które zostały przepisane w literatury tematu, natomiast nie zostały agregowane do naszej rzeczywistości".

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

Dziwisz: „Strategia Bezpieczeństwa Narodowego z 2014 r. była przez niektórych krytykowana m. in. za brak jednoznacznego określenia relacji z Rosją. […] Dlatego dla zwolenników bardziej „ostrego" języka zapisy nowej Strategii z 2020 r. jednoznacznie wskazujące, kto jest naszym największym wrogiem, również w cyberprzestrzeni, są oczekiwanym i właściwym rozwiązaniem […] Wskazanie jedynie na Rosję jako źródło cyberzagrożeń może zamglić/zakłócić szersze postrzeganie problemów

cyberbezpieczeństwa. Trzeba pamiętać o tym, że strategie bezpieczeństwa są dokumentami przyjmowanymi na kilka lat, a cyberprzestrzeń jest środowiskiem w najmniejszym stopniu przewidywalnym. [...] Możliwe, że niedługo większe zagrożenie niż Rosjanie będą generować np. Chińczycy chcący osłabić NATO przez testowanie odpowiedzi państw członkowskich. Także państwa konkurujące gospodarczo z Zachodem, starające się osiągnąć przewagę poprzez wykradanie informacji albo osłabianie pozycji innych, będą wykorzystywać cyberprzestrzeń do przeprowadzania wrogich działań. I wreszcie, niekoniecznie atakującym musi okazać się konkretne państwo, ale na przykład organizacja terrorystyczna".

Gawkowski: „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".

Kitler: „[...] to nie jest właściwe rozwiązanie, bowiem zagrożenia informacyjne napływają ze strony wielu innych uczestników stosunków międzynarodowych, państw i podmiotów niepaństwowych. Jest to bez wątpienia efekt przyjęcia postawy politycznej, której głównym nurtem jest wskazywanie Federacji Rosyjskiej jako źródła wszelkiego zła. W polityce jednak, a w konsekwencji i w strategii obowiązuje stara zasada *szykuj się na najgorsze a doświadczysz lepszego.* A to oznacza, iż współcześnie każdy, kto zechce osiągać sukcesy polityczne, ekonomiczne i kulturowe na arenie międzynarodowej, nie zaniedba możliwości wykorzystania przestrzeni informacyjnej do stwarzania jak najlepszych warunków osiągnięcia przewagi nad innymi".

Koziej: „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 infosferze (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".

Różański: „Zagrożenie dla naszego bezpieczeństwa nie jest zamknięte granicami Federacji Rosyjskiej, radykalni islamiści, których zagrożenia bym nie bagatelizował sprawnie poruszają się cyberprzestrzeni, a wskazanie, że konkretny kraj jest ich siedzibą będzie błędem. Zagrożenia w obszarze informacyjnym muszą być widziane w ujęciu globalnym".

Jakich kluczowych zagrożeń w obszarze informacyjnym zabrakło w dokumencie?

Gawkowski: „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".

Dziwisz: „Niestety Strategia prezentuje zagrożenia w obszarze informacyjnym nazbyt powierzchownie i nie poświęca im wiele miejsca [...] Natomiast słusznie zauważono, że bezpieczne funkcjonowanie państwa i obywateli w przestrzeni informacyjnej zależy od zbudowania zdolności do ochrony przestrzeni informacyjnej, którą należy rozumieć jako przenikające się środowisko wirtualne, fizyczne oraz poznawcze. Innymi słowy, bezpieczeństwo w obszarze informacyjnym powinno być rozumiane jako nierozerwalnie związane z cyberbezpieczeństwem. [...] Ważnym zapisem Strategii jest zwiększanie świadomości społecznej o zagrożeniach związanych z manipulacją informacją poprzez edukację w zakresie bezpieczeństwa informacyjnego. W domyśle dotyczy to szczególnie dzieci, młodzieży oraz osób, które zawodowo zajmują się analizą informacji".

Karczewska: „Zabrakło zagrożenia w postaci braku zaufania bądź utraty zaufania do poszczególnych

warstw przestrzeni informacyjnej. Zresztą pojęcie “zaufanie” w ogóle nie występuje w strategii. Należy przypomnieć, że dyrektywa NIS ma na celu poprawę funkcjonowania rynku wewnętrznego poprzez budowanie zaufania i pewności do sieci i systemów informatycznych na terytorium Unii. Również w RODO zaznaczono, jak ważna jest budowa zaufania, które pozwoli na rozwój gospodarki cyfrowej na rynku wewnętrznym. Zaufanie do systemów państwowych jest kluczowe dla dalszej cyfryzacji Polski”.

Kitler: Profesor Akademii Sztuki Wojennej wskazał zagrożenia pogrupowane w dwa bloki - w wymiarze wewnętrznym (krajowym) i zewnętrznym. Do wymiaru wewnętrznego zaliczył m.in. występowanie w społeczeństwie deficytów informacyjnych, skutkujących podatnością na wrogą perswazję; potencjalną dezinformację obywateli poprzez agresywne działania propagandowe; narzucanie obcych idei niezgodnych z interesem państwa; pojawienie się i rozwój postaw antypaństwowych, agresywnych, defetystycznych (np. islamofobia, szpiegomania) czy wzrost negatywnych postaw społecznych lub wystąpienie konfliktów społecznych, zgodnych z intencjami przeciwnika informacyjnego. Do katalogu zagrożeń zewnętrznych zaliczył m.in. deformowanie treści oraz wprowadzanie do systemów informacyjnych nieprawdziwych treści logicznych za pośrednictwem kanałów łączności rządowej czy wojskowych systemów dowodzenia; działalność służb specjalnych i podmiotów informacyjnych innych państw oraz aktorów niepaństwowych (w tym szpiegostwo); wrogą aktywność operacyjną struktur informacyjno-propagandowych aktorów państwowych i pozapaństwowych; działania propagandowe i dezinformacyjne; dominację potencjalnych agresorów w środowisku informacyjnym; penetrację środowiska informacyjnego RP przez wrogie struktury informacyjno-propagandowe. (pełen katalog zagrożeń wskazanych przez autora opinii został wskazany w pełnym tekście dostępnym tutaj).

Koziej: „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”.

Różański: „Jeżeli ktoś oczekiwałby listy zagrożeń w cyberprzestrzeni z jakimi należy się liczyć to ich nie znajdzie, bowiem nie pisze się o zagrożeniach systemu bankowego, danych osobowych gromadzonych przez różne agendy państwa, systemu pobierania opłat czy rozliczeń podatkowych opierających się dzisiaj na przekazie elektronicznym. Dla mnie jednak wystarczającym jest dostrzeżenie, iż zagrożenia w obszarze informacyjnym dotyczą zarówno sfery militarnej i niemilitarnej, ten bardzo ogólny podział powinien zostać rozwinięty w kolejnych dokumentach”.

Eksperci byli zgodni w tym, że podkreślenie kwestii cyberbezpieczeństwa i zagrożeń informacyjnych w Strategii Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej 2020 było dobrą decyzją. Ich zdaniem problem został jednak poruszony powierzchownie, schematycznie i przewidywalne. Nie podjęto również próby zintegrowanego podejścia do problematyki cyberbezpieczeństwa i infobezpieczeństwa. Wskazanie Rosji jako głównego zagrożenia także zostało skrytykowane przez ekspertów, którzy wskazali, że zagrożenia środowiska informacyjnego są globalne i nie mogą być ograniczane do jednego kierunku oraz jednego podmiotu. Brakuje również w strategii wyróżnienia aktorów niepaństwowych, jako potencjalnych źródeł zagrożeń w infosferze. Eksperci podkreślili ponadto, że w dokumencie nie znalazły się działania, które należy podjąć aby walczyć z dezinformacją.

Pełne odpowiedzi udzielone przez ekspertów znajdują się poniżej:

- doktor Dominika Dziwisz - Uniwersytet Jagielloński (UJ),

- Krzysztof Gawkowski - dyrektor Polskiego Instytutu Cyberbezpieczeństwa,
- inżynier Joanna Karczewska - Audytor SI, ISACA Warsaw Chapter,
- profesor Waldemar Kitler - Akademia Sztuki Wojennej (AszWoj),
- generał Stanisław Koziej - były wiceminister obrony narodowej, oraz były szef Biura Bezpieczeństwa Narodowego,
- generał broni rezerwy dr Mirosław Różański - prezes Fundacji Bezpieczeństwa i Rozwoju STRATPOINTS, doradca POLSKA 2050.