OCENA ZAPISÓW STRATEGII BEZPIECZEŃSTWA NARODOWEGO RZECZYPOSPOLITEJ POLSKIEJ 2020_PROF. WALDEMAR KITLER

Polityka zdominowała dokument o charakterze strategicznym, a w strategii znalazły się zagadnienia będące wynikiem odreagowania na ich dotychczasowe zaniedbanie jak np.: tożsamość narodowa Rzeczypospolitej Polskiej czy tworzenie pozytywnego wizerunku Polski - stwierdził prof. Waldemar Kitler z Akademii Sztuki Wojennej 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 prof. Waldemara Kitlera, eksperta Akademii Sztuki Wojennej.

Uwagi natury ogólnej

Od samego początku polskie strategie bezpieczeństwa obciążone są brakiem stałej i precyzyjnej procedury ich opracowywania, cykliczności, koordynacji i struktury treści. I także ta ostatnia, z 2020 r., ma tę cechę, że opracował ją, na podstawie rekomendacji BBN, wyznaczony przez premiera międzyresortowy zespół po przewodnictwem wskazanego przez Ministra Obrony Narodowej sekretarza stanu albo podsekretarza stanu w Ministerstwie Obrony Narodowej. Chociaż co do składu zespołu nie można mieć zastrzeżeń, poza brakiem przedstawicieli świata nauki i organizacji typu *know-how* (przynajmniej nic mi o tym nie wiadomo), to jednak koordynacja z pozycji jednego z wiceministrów nie jest najlepszym rozwiązaniem. Chciałoby się powiedzieć, bez żadnej ironii, jaka strategia taki zespół. A to dlatego, że strategia bezpieczeństwa ma tylko rangę uchwały Rady Ministrów i tym samym jest dokumentem o małym znaczeniu prawnym, ale to już przedmiot innej dyskusji. Bez cienia wątpliwości koordynacja opracowania strategii powinna spoczywać na osobie z pozycji prezesa Rady Ministrów, np. na szefie KPRM lub innym ministrze – pełnomocniku premiera.

Współcześnie strategia bezpieczeństwa narodowego wyewoluowała bowiem do postaci dokumentu zawierającego o wiele więcej zagadnień niż tylko te dotyczące wykorzystywania bitew dla celów wojny (Carl von Clausewitz) lub rozdziału i użycia środków wojennych dla urzeczywistnienia celów polityki (Liddell Hart). Tym samym strategia bezpieczeństwa narodowego ma być obecnie wyborem przez najwyższe organy władzy wykonawczej środków (działań), narzędzi i sposobów ich osiągnięcia w ramach przemyślanej i konsekwentnie realizowanej koncepcji działania na rzecz zapewnienia wolnych od wszelkich wyzwań i zagrożeń warunków bytu im rozwoju narodowego, a także łagodzenia lub usuwania skutków w razie ich wystąpienia, ujmowanych w dużym horyzoncie czasowo-przestrzennym.

I chociaż są dwa odmienne stanowiska, co do zależności między polityką a strategią, to uważam, że strategia jest treściwo i hierarchicznie podporządkowana polityce państwa, stanowiąc narzędzie jej racjonalizacji. Polityka może wskazywać cele polityczne, zaś strategia ustalać sposoby ich realizacji.

Tym samym w SBN nie mogą dominować zagadnienia natury politycznej gdyż powinna ona stanowić wykładnię celów politycznych i interesów narodowych państwa, opartą na prognozie i ocenie środowiska bezpieczeństwa, wraz ze strategiczną koncepcją bezpieczeństwa narodowego (państwa) oraz sposobów realizacji tej koncepcji.

Bez wątpienia brakuje w Polsce strategii narodowej lub wielkiej strategii, której namiastką jest przyjęta przez Radę Ministrów 14 lutego 2017 r. *Strategia na rzecz odpowiedzialnego rozwoju do roku 2020 (z perspektywą do 2030 r.)* (SOR). Niewiele brakowało, by zaistniała właściwa korelacja między SOR a SBN. Tak się jednak nie stało i polityka zdominowała dokument o charakterze strategicznym, a w strategii znalazły się zagadnienia będące wynikiem odreagowania na ich dotychczasowe zaniedbanie (np.: Tożsamość narodowa Rzeczypospolitej Polskiej, Tworzenie pozytywnego wizerunku Polski). Niestety znaczna część treści SBN ma bardziej charakter postulatów natury politycznej niż wyboru środków (działań), narzędzi i sposobów ich osiągnięcia w ramach przemyślanej i konsekwentnie realizowanej koncepcji działania na rzecz bezpieczeństwa. Tak też jest w filarze pierwszym (Bezpieczeństwo państwa i obywateli) i działaniach strategicznych w zakresie „Cyberbezpieczeństwa" i „Przestrzeni informacyjnej".

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

Problematyka zagrożeń znalazła się w części pt. „Środowisko bezpieczeństwa". Jej treść czyta się jak dobrze przygotowany konspekt do artykułu naukowego lub artykułu prasowego w czasopiśmie popularnonaukowym. I tym razem w polskiej strategii bezpieczeństwa pojawia się narracja o zacięciu teoretycznym, co prawda trudno tego uniknąć, ale uogólnienia teoretyczne w strategii nie powinny raczej dominować. 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. Jednym z nich jest projekt *Doktryny bezpieczeństwa informacyjnego RP* z 2015 roku, w którego rozdziale drugim pt. „ŚRODOWISKO BEZPIECZEŃSTWA INFORMACYJNEGO RP" z dużą precyzją określono zagrożenia i wyzwania w przedmiotowej materii. Z problematyką bezpieczeństwa informacyjnego powiązane są, w pewnym sensie, zagadnienia cyberbezpieczeństwa. A w tym wypadku, poza ustawą z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. U. poz. 1560), mamy opracowaną w 2019 roku *Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej* na lata 2019–2024 (MP 2019, poz. 1037). A zatem opracowanie zagrożeń w obszarze informacyjnym nie powinno stanowić większego kłopotu, ze szczególnym naciskiem na projekt doktryny bezpieczeństwa informacyjnego.

Reasumując 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. A definiuję je jako „…transsektorową dziedzinę bezpieczeństwa narodowego (węziej: bezpieczeństwa państwa), będącą procesem polegającym na dążeniu do zapewnienia wolnego od zakłóceń funkcjonowania i rozwoju państwa, w tym władzy publicznej i społeczeństwa, podmiotów rynkowych i pozarządowych w przestrzeni informacyjnej, przez swobodny dostęp do informacji, z jednoczesną ochroną przed negatywnymi jego skutkami (materialnymi i niematerialnymi), ochronę zasobów
i systemów informacyjnych przed wrogimi działaniami innych podmiotów lub skutkami działania sił natury i awarii technicznych, przy jednoczesnym zachowaniu zdolności do informacyjnego oddziaływania na zachowania i postawy podmiotów międzynarodowych
i krajowych.

Odpowiedź na pytanie: 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.

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

Nie, 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 obwiązuje 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. Co do zasady tak było, jest i będzie w każdy obszarze rywalizacji między ludźmi.

Jakich kluczowych zagrożeń w obszarze informacyjnym zabrakło w dokumencie?

W odpowiedzi na to pytanie wskażę te najważniejsze, które wymieniono
w przywoływanym projekcie doktryny bezpieczeństwa informacyjnego RP, z którymi się
w pełni zgadzam[1]:

1. W wymiarze wewnętrznym (krajowym):

– 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),

– wzrost negatywnych postaw społecznych lub wystąpienie konfliktów społecznych, zgodnych z intencjami przeciwnika informacyjnego,

– istnienie (tworzenie) agentury wpływu (inspirowanie do zakładania oraz wsparcie finansowe formacji politycznych lub organizacji społecznych wspierających
i realizujących obce interesy w Polsce),

– wpływanie na opinię publiczną przez agentów zmiany sterowanych z zewnątrz, zwłaszcza aktywizacja wybranych grup społecznych przez inne państwo oraz realizacja interesów obcych państw, sprzecznych z interesem RP,

– obniżanie się morale społeczeństwa w razie agresji informacyjnopropagandowej,

– dezinformacja, trolling, wroga propaganda, zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego,

– ataki powodujące zakłócenia funkcjonowania sieci teleinformatycznych w sektorach i instytucjach o podwyższonym stopniu wrażliwości, w tym tworzących infrastrukturę krytyczną,

– monopolizacja rynku informacyjnego i jego poszczególnych struktur oraz niekontrolowany rozwój rynku informacyjnego, media masowe mogą być narzędziem dezinformacji,

– przejmowanie lub finansowanie mediów przez podmioty nieprzychylne lub wrogie Polsce,

– pojawienie się w przestrzeni informacyjnej mediów propagujących idee sprzeczne z interesem narodowym,

– aktywne uczestnictwo przeciwnika w polskich mediach społecznościowych

– nieświadome, niezamierzone powielanie przekazu informacyjnego sprzecznego z interesem narodowym przez użytkowników mediów społecznościowych lub media masowe

2. W wymiarze zewnętrznym:

– 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,

– utratę zdolności wpływania, dystrybucji informacji w środowisku informacyjnym,

– inspirowane z zewnętrz działania informacyjne podmiotów wewnętrznych mające na celu wywoływanie i pogłębianie podziałów społecznych i politycznych,

– wsparcie zewnętrzne dla podmiotów realizujących politykę przeciwnika,

– dezinformację obywateli innych państw, w tym tworzących wspólnoty organizacyjne w kwestiach dotyczących polskiej polityki zagranicznej,

– kształtowanie negatywnego obrazu Polski na arenie międzynarodowej, w tym wśród sojuszników, przede wszystkim w ramach NATO i UE,

– wywoływanie w społeczeństwach i elitach politycznych tych państw nastrojów antypolskich na przykład poprzez nagłaśnianie i akcentowanie jednostkowych wypowiedzi przedstawicieli polityki, sprzecznych z oficjalną linią polityki zagranicznej RP w kluczowych, strategicznych sprawach,

– dyskredytowanie polskiej polityki zagranicznej na arenie międzynarodowej,

– działanie zagranicznych struktur informacyjnych przeciwko interesom RP,

– szerzenie treści antypolskich za pośrednictwem mediów o zasięgu międzynarodowym, a w tym: tworzenie w obiegu informacyjnym na Zachodzie obrazu Polski jako kraju ksenofobicznego i antysemickiego.

Zgodnie z treścią pytania, wymieniłem literalnie najważniejsze zagrożenia. W SBN można by było to odpowiednio pogrupować w bloki tematyczne, żeby nie zajmowały tak dużo miejsca.