Stanisław Koziej

*Warszawa, 2.03.2016*

**UWAGI**

do projektu „ZAŁOŻEŃ STRATEGII CYBERBEZPIECZEŃSTWA DLA RZECZYPOSPOLITEJ POLSKIEJ” (z lutego 2016)

Dobrze, że rząd podejmuje wyzwanie zbudowania zintegrowanego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej. Zainicjowanie tego procesu jest – jak można zakładać – podstawowym celem niniejszego projektu. Z tego punktu widzenia warto zwrócić uwagę na następujące kwestie:

**1.**

Trudno uznać ten dokument za założenia do strategii cyberbezpieczeństwa. Zajmuje się raczej kwestiami wykonawczymi – poniżej poziomu strategicznego – i to dotyczącymi tylko jednej (z dwóch) części/dziedziny strategii, a mianowicie realizacji strategii preparacyjnej (przygotowanie, budowa, utrzymanie i rozwój systemu bezpieczeństwa) Nie odnosi się do interesów i celów, rodzajów i charakteru zagrożeń, głównych zadań operacyjnych itp. – co jest fundamentem treści każdej strategii bezpieczeństwa.

Warto zwrócić uwagę, że główne elementy strategii cyberbezpieczeństwa zawarte są w poszczególnych rozdziałach STRATEGII BEZPIECZEŃSTWA NARODOWEGO RP i następnie zostały rozwinięte oraz skonkretyzowane w DOKTRYNIE CYBERBEZPIECZEŃSTWA RP. Zgodnie z narodowym systemem planowania strategicznego STRATEGIA jest dokumentem koncepcyjnym, doktryna – pośrednim między koncepcyjnym i wykonawczym, reszta to dokumenty wykonawcze w sferze operacyjnej (dyrektywy, polityki, plany… dotyczące działań, funkcjonowania systemu bezpieczeństwa) lub preparacyjnej (programy, plany … dotyczące przygotowania i doskonalenia systemu bezpieczeństwa).

**Planowanie realizacyjne (wykonawcze)**

**Planowanie koncepcyjne**

Niniejsze założenia nie spełniają kryterium założeń strategicznych, są bliżej doktryny, ale w istocie dotyczą jeszcze bardziej szczegółowych i konkretnych zadań zarówno operacyjnych, jak preparacyjnych i dlatego najlepszą nazwą dla tego dokumentu byłaby np. **ZAŁOŻENIA KONCEPCJI PRZYGOTOWANIA I DZIAŁANIA SYSTEMU CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ.**

**2.**

Wątpliwości budzi generalne podejście pojęciowe (terminologiczne) odnoszące wszystkie niemal rozważania o bezpieczeństwie lub ochronie do samej cyberprzestrzeni, a nie do podmiotów działających w cyberprzestrzeni. Zgodnie z przyjętym w DOKTRYNIE CYBERBEZPIECZEŃSTWA RP (s. 7-8) podejściem to są różne kategorie pojęciowe, przy czym „bezpieczeństwo w cyberprzestrzeni (cyberbezpieczeństwo danego podmiotu, np. państwa)” jest pojęciem szerszym niż „bezpieczeństwo cyberprzestrzeni”. Patrz pojęcia przyjęte w DOKTRYNIE CYBERBEZPIECZEŃSTWA:

**„***Cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni)*– proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni (s.7-8).

*Bezpieczeństwo cyberprzestrzeni RP*– część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych (s..8).”

Należałoby więc i w tych założeniach ***odróżniać pojęcia „bezpieczeństwo RP w cyberprzestrzeni” i „bezpieczeństwo cyberprzestrzeni RP”,*** a nie ograniczać się tylko do tego drugiego, węższego znaczeniowo. Tym bardziej, że tak naprawdę to idzie o bezpieczeństwo Polski, Polaków, ich zasobów itp. w cyberprzestrzeni. Bezpieczeństwo/ochrona samej cyberprzestrzeni to część szerszej problematyki, mieszcząca się w pewnym sensie w obszarze bezpieczeństwa infrastruktury krytycznej. To tak jak z bezpieczeństwem drogowym – idzie tu o bezpieczeństwo podmiotów/użytkowników ruchu drogowego, a nie tylko o bezpieczne samochody.

W założeniach zakłada się doprecyzowanie samego pojęcia cyberprzestrzeni, więc byłaby to okazja do ustalenia sposobu rozumienia także innych pojęć, w tym tych dwóch kluczowych.

**3.**

Założenia koncentrują się na państwowym, publicznym wymiarze cyberbezpieczeństwa. **Za mało uwagi poświęcają sektorowi prywatnemu, a w ogóle pomijają sektor obywatelski**.

Warto więc uzupełnić założenia o problematykę tych pozostałych sektorów i kwestie ich koordynacji z sektorem państwowym, publicznym.

**4.**

Należałoby także uporządkować, stosownie do podejścia przyjętego w STRATEGII BEZPIECZEŃSTWA NARODOWEGO i DOKTRYNIE CYBERBEZPIECZEŃSTWA, **instytucje (ogniwa) składające się na system cyberbezpieczeństwa,** z uwzględnieniem podsystemu kierowania (koordynowania) i podsystemów wykonawczych, w tym operacyjnych (wyspecjalizowanych) i wsparcia (ogólnych). Powinno to ułatwić tworzenie spójnego systemu całościowego.

**5.**

Słusznie akcentuje się w założeniach potrzebę **koordynacji** bardzo dziś rozproszonego, luźnego systemu cyberbezpieczeństwa RP. Przy czym wydaje się, że sam system koordynacji w kierowaniu cyberbezpieczeństwem państwa to za mało. W odniesieniu do publicznej, rządowej części systemu cyberbezpieczeństwa potrzebne jest coś więcej – **integracja** systemu kierowania nim.

Natomiast koordynacja dotyczyć powinna makrosfery kierowania obejmującej także podmioty niepaństwowe, niepubliczne, cały sektor prywatny i obywatelski – dla zapewnienia, poprzez koordynację właśnie, spójnego działania tych wszystkich sektorów w imię wspólnych celów bezpieczeństwa Polski (państwa, podmiotów prywatnych i obywateli) w cyberprzestrzeni.

**6.**

Poważnego przedyskutowania wymaga przyjmowana w założeniach instytucjonalna struktura systemu kierowania cybebezpieczeństwem na poziomie rządowym. Prowadzenie spraw cyberbezpieczeństwa odbywa się i ma nadal odbywać się poza (obok) systemem kierowania bezpieczeństwem narodowym (poza tym systemem jest zarówno Komitet RM ds. Cyfryzacji, jak i Ministerstwo Cyfryzacji). Prowadzić to może do dalszego alienowania się cyberbezpieczeństwa z całego systemu bezpieczeństwa narodowego, do czego nie powinno się dopuścić.

Jest to w znacznej mierze konsekwencją wadliwej struktury kierowania bezpieczeństwem narodowym na poziomie rządu, która nie zapewnia ponadresortowej koordynacji spraw bezpieczeństwa: brak rządowego Komitetu Bezpieczeństwa Narodowego i ograniczone tylko do zarządzania kryzysowego kompetencje Rządowego Centrum Bezpieczeństwa.

Dlatego wydaje się zasadne zaproponowanie przy tej okazji korekty (reformy) ponadresortowego zarządzania bezpieczeństwem na poziomie rządowym: **utworzenie Rządowego Komitetu Bezpieczeństwa Narodowego i Rządowego Centrum Bezpieczeństwa Narodowego (na bazie obecnego RCB), aby włączyć weń także kompetencje dotyczące ponadresortowych kwestii cyberbezpieczeństwa** (podobnie zresztą jak innych transsektorowych dziedzin bezpieczeństwa, jak sprawy służb specjalnych, przemysłu obronnego, bezpieczeństwa informacyjnego, energetycznego itp.).

**7.**

Warto zastanowić się nad proponowanymi poziomami struktury systemu cyberbezpieczeństwa: strategiczny, operacyjny i … techniczny(?). Ten trzeci poziom wyróżniony jest z punktu widzenia zupełnie innego kryterium niż dwa pierwsze. Lepsze byłoby określenie go jako **poziom taktyczny.**

Oczywiście w cyberbezpieczeństwie, jak w każdym procesie bezpieczeństwa, można wyróżniać także sferę techniczną. Ale ona występuje na wszystkich poziomach: i strategicznym, i operacyjnym, i taktycznym. Podobnie jak inne tego typu kategorie, np. sfera kadrowa, organizacyjna, szkoleniowa itp.

**8.**

Zmienić należy termin „**Pojedynczy Punkt Kontaktowy**”. Nie oddaje on istoty rzeczy. To jest niezbyt szczęśliwie przetłumaczenie terminu angielskiego. Lepsze byłoby chyba … *wyodrębniony, wydzielony* (spośród innych do określonego zadania) lub *scalony, zintegrowany, jednolity* (zbierający, łączący różne informacje i funkcje).

**9.**

W strukturze krajowego systemu cyberbezpieczeństwa podkreśla się i eksponuje jego hierarchiczność w sensie ostrzegania, przekazywania informacji, reagowania. Wydaje się wskazane uwzględnienie w większym stopniu także jego **sieciowości.**

**10.**

Słusznie zakłada się konieczność ulokowania centrum koordynacji **poza służbami specjalnymi**, w cywilnej części kierowania. Cyberbezpieczeństwo jest kategorią powszechną, działania służb specjalnych w cyberprzestrzeni jest tylko jednym z jego elementów.

**11.**

BBN nie jest organem doradczym Prezydenta. Organem doradczym jest RBN (Rada Bezpieczeństwa Narodowego).

**12.**

Założenia wymagają poważnej korekty redakcyjnej: stylistycznej, językowej.

===================================