Rekomendacja Rady ds. Cyfryzacji stworzenia „cyfrowej ambasady RP" w celu zapewnienia suwerenności cyfrowej i bezpieczeństwa informacyjnego państwa oraz jego cyfrowych zasobów z 14 kwietnia 2022r.

Ciągłość państwa i zapewnienie jego funkcjonalności zależy od dostępu do danych, które w związku z postępującą transformacją cyfrową oraz wdrażaniem modelu „paperless" przy uruchamianiu usług sektora administracji publicznej (e-ZLA, e-Recepta, e-Toll itp.) przyjęły formę cyfrową. Te przemiany w istotny sposób zmieniają współczesne rozumienie bezpieczeństwa narodowego, które zależy także od utrzymania suwerenności cyfrowej. Bez dostępu do danych cyfrowych nie mogą funkcjonować kluczowe obszary państwa, w tym zwłaszcza bezpieczeństwo wewnętrze i zewnętrzne, finanse publiczne, ubezpieczenia społeczne, opieka zdrowotna, łączność, energetyka. Ta zależność i zagrożenie występuje w wymiarze centralnym, rządowym, jak i samorządowym.

Postępująca agresja Federacji Rosyjskiej na Ukrainę, treść ultimatum wystosowanego przez FR wobec Stanów Zjednoczonych[1] oraz treść oświadczenia Sekretarza Generalnego NATO z dnia 25 lutego 2022 r.[2] należy uznać także za przesłankę do **zabezpieczenia kluczowych zasobów informatycznych i informacyjnych** na wypadek zmasowanego cyberataku, ataku militarnego, a nawet zajęcia części terytorium Polski. W przypadku fizycznej utraty lub nieodwracalnego uszkodzenia kluczowych zakresów danych, przetwarzanych na terenie Polski, państwo utraci możliwość prawidłowego funkcjonowania w każdym obszarze, którego będzie dotyczyć utrata lub uszkodzenie danych. Zagrożenia dla bezpieczeństwa i integralności baz danych zlokalizowanych fizycznie w państwowych centrach danych wyłącznie na terenie Polski utrzyma się co najmniej tak długo, jak długo przy władzy w Rosji pozostaną przywódcy kontynuujący imperialistyczną i rewizjonistyczną linię geopolityczną.

Daleko idące działania mające na celu ochronę cyfrowej suwerenności kraju podjęła Estonia po cyberataku przeprowadzonym w 2007 r. przez Rosję - zbudowała „ambasadę danych", czyli specjalnie zabezpieczone centrum danych zlokalizowane w Luksemburgu, w którym przechowywane są zaszyfrowane kopie zapasowe danych cyfrowych państwa na wypadek ataku – cyfrowego i fizycznego, na ten kraj.

W celu zabezpieczenia i ochrony interesu Rzeczypospolitej Polskiej, rząd powinien:

- podjąć rozmowy z polskimi firmami posiadającymi wystarczający potencjał do współpracy w zakresie partnerstwa publiczno-prywatnego, a także poświadczenia bezpieczeństwa przemysłowego oraz z krajami leżącymi poza potencjalnym teatrem działań wojennych w

[1] https://www.pism.pl/publikacje/rosyjskie-zadania-gwarancji-bezpieczenstwa-wobec-usa-i-nato

[2] „The Kremlin's objectives are not limited to Ukraine.
Russia has demanded legally binding agreements to renounce further NATO enlargement.
And to remove troops and infrastructure from Allies that joined after 1997
https://www.nato.int/cps/en/natohq/opinions_192455.htm

Europie - takimi jak np. Luksemburg, Szwajcaria, Norwegia, Wielka Brytania, zasadzie wymiany lokalizacji danych, aby:

- zbudować ”cyfrową ambasadę” w postaci bezpiecznego ośrodka przechowywania kluczowych danych[3]

- stworzyć ramy mające na celu posiadanie kopii kluczowych rejestrów państwowych na wypadek uszkodzenia lub utraty danych przetwarzanych w kraju oraz zdolność do odtworzenia kluczowych zasobów informacyjnych, systemów i usług cyfrowych w przypadku ich uszkodzenia lub całkowitej utraty.

REKOMENDACJE CO DO UWARUNKOWAŃ PROJEKTU I KLUCZOWE WARUNKI SUKCESU „CYFROWEJ AMBASADY”

1. „Cyfrowa ambasada” powinna stanowić rozszerzenie polskiej chmury rządowej, głównie w zakresie kopii zapasowej kluczowych rejestrów państwowych przechowywanej poza fizyczną przestrzenią Polski.
2. Lokalizacja „cyfrowej ambasady” w kraju europejskim, możliwie wiarygodnym, stabilnym, demokratycznym i bezpiecznym.
3. Ośrodek i dane powinny podlegać jurysdykcji Polski. Dane i serwery powinny być chronione tymi samymi gwarancjami prawnymi, co dane i serwery w Polsce.
4. Za budowę, utrzymanie i bezpieczeństwo ośrodka powinny odpowiadać wyłącznie polskie organy państwa i polskie firmy.
5. Za koordynację wykonywania kopii zapasowych kluczowych rejestrów państwowych powinien odpowiadać jeden krajowy ośrodek centralny.
6. Zainicjowanie i ustanowienie centralnego procesu koordynacji wykonywania kopii zapasowych kluczowych rejestrów państwowych. Ośrodek centralny nie powinien wykonywać kopii zapasowych. Powinien jedynie koordynować poniższe zadania:
    a) okresowe (przykładowo kwartalne) przekazywanie kopii danych do centralnego ośrodka przez jednostki zobowiązane,
    b) transmisję danych do cyfrowej ambasady,
    c) nadzór nad prawidłowością działania cyfrowej ambasady.

[3] Do dookreślenia pozostają zadania takiej ambasady czy ma być **(a) tylko kopią zapasową danych,** to jest do bardzo szybkiego zrealizowania (b) miejscem, z którego dokonuje się odtworzenia funkcjonowania systemów, (c) pełnowartościowym ośrodkiem zapasowym, do którego władze Polski mogą się przełączyć w przypadku ataku. Każde z tych zadań jest inne, wymaga innego przygotowania, innej formuły „ambasady” – każde pociąga za sobą inne koszty i wymaga innego czasu na realizację.