**aut. Grzegorz Małecki** 30.04.2018

# PŁK MAŁECKI: USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA WYMAGA POWAŻNEJ KOREKTY

**O Ustawie o krajowym systemie cyberbezpieczeństwa oraz roli Pełnomocnika ds. Cyberbezpieczeństwa mówi w rozmowie z Cyberdefence24.pl były szef Agencji Wywiadu pułkownik Grzegorz Małecki.**

**Jak Pan ocenia projekt Ustawy?**

Z mojej perspektywy ustawa ta jest o jakieś 80-90 % za długa. Ma 58 stron, a według mnie nie ma potrzeby, żeby ona była tak obszerna. Powinna zawierać 10 - 15 artykułów, regulujących kwestie systemowe i fundamentalne. Większość kwestii techniczno-organizacyjnych należy przenieść albo do rozporządzeń, albo do innych regulacji.

**Dlaczego?**

Należy kierować się przede wszystkim względami praktycznymi. Patrząc z zatem praktycznego punktu widzenia, jeśli cokolwiek w obszarze, którego dotyczy zmieni się, a mówimy o zjawiskach, w tym zagrożeniach, o bardzo zmiennej naturze, to konieczne będą nowelizacje ustawy.

Jestem przeciwnikiem stosowania praktyki, wedle której standardy i procedury, czyli tzw. dobre praktyki zawodowe opisywane i wdrażane są za pomocą aktów prawnych. Ta ustawa o której mówimy nie powinna zawierać regulacji odnoszących się do takich kwestii. Powinna być krótka i zwięzła, opisywać czym jest system, z czego się składa, jakie są jego podmioty plus oczywiście wprowadzać wymagania, które nakłada na nas dyrektywa NIS.

**Ustawa zakłada utworzenie trzech CSIRT-ów. Mają zostać także utworzone kolejne sektorowe. Czy to nie jest bezsensowne mnożenie ciał?**

Tor rozwiązanie jest oczywiście wadliwe. To jest pewna koncepcja, która idzie pod prąd współczesnym trendom i wyzwaniom rzeczywistości. Ustawa powinna odpowiadać na zasadniczą potrzebę, polegającą na tym, żeby skoordynować, uwspólniać, ujednolić i skupić w jednym ręku zarządzanie tymi procesami w cyberprzestrzeni o charakterze strategicznym. Ustawa idzie niestety pod prąd, mnożąc różne byty, które będą funkcjonowały według własnej logiki w swoich specyficznych warunkach.

Zakłada istnienie trzech CSIRTów: Gov.; Mil. i NASK. Nie potrafię zrozumieć dlaczego do ustawy włącza się konkretne rozwiązanie strukturalne w postaci NASKu, który nie jest instytucją rządową i który może być w każdej chwili zastąpiona inną. Zamiast CSIRT-NASKu powinno być wpisane CSIRT.PL, tak jak mają to zrobione np. Izraelczycy. Rozwiązanie polegające na upoważnieniu NASKu

do pełnienia funkcji CSIRTu Narodowego jest wadliwe, ponieważ powierza się to strukturze, która nie posiada przymiotów władzy publicznej. To jest prawdopodobnie rozwiązanie tymczasowe. Pamiętamy o tym, jak Minister Streżyńska mówiła, że stworzenie NC Cyber w ramach NASKu wynikało z faktu, że NASK dysponował środkami na cyberbezpieczeństwo, których nie posiadało Ministerstwo Cyfryzacji. To jest rozwiązanie absolutnie o charakterze tymczasowym. W związku z tym sankcjowanie tego rozwiązania w ustawie jest pomysłem bardzo kontrowersyjnym i uważam, że nie powinno się go popierać. Dlatego w tym miejscu zamiast NASK zaproponowałbym zapis CSIRT.pl i niezależnie od tego, kto nim będzie dysponował - jaka instytucja, to to będzie pasowało.

Proszę sobie wyobrazić sytuację, że ktoś zdecyduje, że zadania CSIRT narodowego należy powierzyć innej instytucji i  wówczas trzeba będzie zmieniać całą ustawę. Niepotrzebne jest więc wpisywanie, jaka instytucja ma się tym zajmować, to rozwiązanie w ustawie jest nieskuteczne i niefunkcjonalne.

**A co z rozdziałem kompetencji między instytucjami. Czy jest to dobrze zrobione?**

W tej ustawie nie jest to rozdzielone w sposób jednoznaczny i może to doprowadzić do nakładania się kompetencji i sporów między instytucjami. Te rozwiązania w mają duży potencjał konfliktowy.

**Czyli zamiast rozwiązywać spory to je mnożymy?**

Niestety tak to wygląda. Wykonujemy krok w dobrym kierunku czyli wyodrębniamy cyberbezpieczeństwo z Ministerstwa Cyfryzacji, ale robimy to w sposób niekonsekwentny, nieśmiały i niepełny. W tym momencie efekt jest taki, że otrzymujemy system jeszcze bardziej skomplikowany niż dotychczas, bowiem zamiast jednogłowej władzy w postaci Ministerstwa Cyfryzacji, w ramach którego cyberbezpieczeństwo traktowane jest trochę po macoszemu z uwagi na brak środków, powstaje teraz dwugłowa władza: Ministra Cyfryzacji i Pełnomocnika.

**Smok dwugłowy jest zawsze gorszy, niż jednogłowy.**

Tym bardziej, że mamy w bardzo bliskim lokalizacji dwa inne smoki, czyli CSIRT MON i CSIRT GOV. To są rozwiązania niefunkcjonalne. W ustawie nie zawarto jednoznacznej, konsekwentnej koncepcji, wskazującej jednego gospodarza systemu, który wyznacza trendy, standardy i zawiaduje całą materią oraz wyznacza kierunki jej rozwoju. Tego nie ma w ustawie ani w dokumencie powołującym pełnomocnika.

Mamy za dużo technicznych rozwiązań, które niepotrzebnie wchodzą do dokumentu tej rangi, zaciemniając tak naprawdę obraz i utrudniając w gruncie rzeczy korzystanie z tego przepisu i jego aktualizowanie. Byłoby dużo łatwiej stworzyć jedną ustawę o charakterze ramowym, tworzącym fundamenty i objaśniającym co to jest system cyberbezpieczeństwa, kto za niego odpowiada i z jakich elementów się składa. Opis tych elementów powinien być jednak elastyczny, a nie stanowić zamknięty katalog.

**Ministerstwo Finansów stwierdziło ostatnio w komunikacie, że budujemy cyberbezpieczeństwo, ale nie może się to wiązać z dodatkowymi wydatkami. Wszystkie działania muszą być w ramach uchwalonego budżetu.**

To nie jest optymalne rozwiązanie i należy poszukiwać sposobów na jego zmianę w przyszłosci. Jednak na dzisiaj trzeba się odnaleźć w takich realiach jakie wynikają z decyzji MF. A więc w ramach obecnego budżetu państwa można wygospodarować całkiem pokaźne środki. Np. budżet MON na cyberbezpieczeństwo jest spory. Możemy też przesunąć z innych resortów, ale my musimy wyznaczyć pewien algorytm wyliczania budżetu na cyberbezpoieczeństwo, albo odsetek budżetu np. referencyjnego, np. Ministerstwa Cyfryzacji lub Ministerstwa Obrony. Dzięki temu kwota ta będzie jasna i pozwalała na długofalowe planowanie. Bez finansowania i określenia budżetu działania te będą

pozorne. Będą to działania doraźne i powierzchowne, która nie pozwolą na wykonanie zdecydowanego i stanowczego kroku do przodu. Moim zdaniem to powinno się znaleźć w tej ustawie.

Twórzmy pewne ramy, w których wskażmy na przykład, nie poszczególne instytucje, tylko parametry, kryteria jakie te instytucje muszą spełniać, żeby ustawa ich dotyczyła. My wymieniamy jakieś instytucje, w przyszłosci powstaną nowe, które nie są w tej ustawie ujęte i trzeba będzie je dodawać do niej w formie nowelizacji ustawy. Określmy parametry. Na to zwracają uwagę Izraelczycy. Oni nie tworzą ram formalnych, tylko kryteria i parametry, które wyznaczają sposób funkcjonowania ekosystemu w sposób elastyczny. To jest materia, która rozwija się najszybciej ze wszystkich dziedzin aktywności człowieka. Rok to jak generacja w życiu człowieka. Nie jesteśmy w stanie tego przewidzieć, dlatego stwórzmy ustawę elastyczną, która będzie tworzyła ramy, zasady, parametry, kryteria, wartości w sposób na tyle jednoznaczny i przejrzysty, żeby wspomagały rozwój systemu.

**Czyli powinniśmy zacząć ten dokument od nowa?**

Przynajmniej dokonać poważnej korekty.

**Z drugiej jednak strony mamy ograniczone ramy czasu, bo 25 maja wchodzi dyrektywa NIS, a ustawa ma ją implementować.**

Znam argumentację twórców tej Ustawy, że jest to rozwiązanie tymczasowe, przede wszystkim dostosowujące do dyrektywy NIS, mające charakter kompromisu pomiędzy stanowiskami różnych podmiotów i że jest to krok do rozwiązań docelowych.

W moim przekonaniu nie powinniśmy mówić o rozwiązaniach docelowych i ostatecznych, bo w tej materii nie ma takich. To jest proces. Nie widzimy końca i nie będziemy widzieli. Podążajmy za trendami i starajmy się uporządkować naszymi regulacjami dynamicznie rozwijającą się przestrzeń, tworząc cywilizowane warunki, powodując żeby się rozwijała w sposób uporządkowany i zgodny z interesami państwa i społeczeństwa, a nie w sposób żywiołowy i chaotyczny, który może uderzyć w fundamenty naszej działalności. Widzimy na przykładzie Facebooka, że rzeczy nieuregulowane prędzej czy później wybuchają. To są kwestie, o których mówi się od lat, że jest to bomba z opóźnionym zapłonem, ale nikt do tego na serio nie podszedł i musieliśmy czekać na kryzys, który się dopiero ujawnił. Podobnie sytuacja wygląda z tą Ustawą. Jestem wrogiem rozwiązań tymczasowych. W Polsce niestety taka prowizorka jest bardzo trwała  i antyrozwojowa.

**Moglibyśmy sobie wyobrazić sytuację, że skoro dyrektywa NIS została wprowadzona do polskiego porządku prawnego, wypełniliśmy zobowiązania wobec UE i to co było tymczasowe zostaje ostatecznie. To nie jest temat, na którym można zbudować polityczny kapitał.**

Absolutnie nie jest to coś politycznie atrakcyjnego. Jest to jedna z rzeczy, takich, które trzeba zrobić, ale nikogo tak naprawdę obok ekspertów nie zajmuje, ale dotyczy wszystkich. Mało kto zdaje sobie sprawę z konsekwencji, które będzie miało w naszym codziennym życiu.

**Czyli Pana zdaniem samo założenie ustawy jest złe?**

Nie jest skuteczną odpowiedzią na wymogi rzeczywistości. Głównym zastrzeżeniem nie jest jednak długość czy przeładowanie ustawy, ale brak jednoznacznego wskazania głównego gospodarza systemu cyberbezpieczeństwa. Przyjęto wprawdzie zgłaszany od dawna postulat utworzenia Pełnomocnika Rządu, ale jak zwykle zatrzymano się w połowie drogi. Przyjęto rozwiązanie połowiczne. Wyznaczono cyberbezpieczeństwo jako osobny dział, ale zostawiając Ministrowi Cyfryzacji kompetencje oraz obowiązek uzgadniania z nim wszelkich inicjatyw.  W efekcie Pełnomocnik będzie ponosił odpowiedzialność nominalnie, ale nie dostanie instrumentów do realizacji polityki, żeby

sprostać tej odpowiedzialności. Nie będzie miał ponadto budżetu czy zaplecza instytucjonalnego.

To rozwiązanie, które wprowadza Ustawa czyli powołanie Pełnomocnika w ramach Kancelarii Premiera należy uznać za błędne. Widać, po tym co się ostatnio dzieje, że Premier likwiduje tych pełnomocników, sekretarzy stanu w KPRM, których było 11 czy 12. Z punktu widzenia funkcjonowania tego podmiotu, nie ma znaczenia jaką będzie miał rangę, bo to są rzeczy, który mają drugorzędne znaczenie w codziennej działalności. Ani sekretarze ani podsekretarze nie są ministrami konstytucyjnymi i dlatego mają ograniczone pole działania.

Znacznie ważniejsze jest jakie taki pełnomocnik będzie miał zadania, jakie będzie miał uprawnienia, narzędzia do wcielania w czyn tych uprawnień, narzędzia finansowe, ale też narzędzia instytucjonalne, krótko mówiąc jakim zapleczem instytucjonalnym będzie dysponował. Jeśli ulokujemy sekretarza stanu w Kancelarii Premiera, która głównie obsługuje premiera i Radę Ministrów, to w takiej kancelarii pełnomocnik dostanie do dyspozycji jeden departament składający się z 5 albo 10 osób. Nie będzie w stanie sam nim zarządzać, bo pracodawcą wszystkich pracowników, którzy obsługują sekretarzy stanu jest szef Kancelarii a tak naprawdę dyrektor generalny a nie ten minister. Tak naprawdę ten minister, pełnomocnik czy sekretarz stanu nie będzie miał wpływu jakich ludzi dostanie. W związku z tym będzie nominalnie za to odpowiadał, ale w praktyce nie będzie miał żadnych instrumentów, żeby to realizować.

Dla każdego, kto jest obeznany w meandrach funkcjonowania administracji państwowej to są rzeczy oczywiste. Wpisywanie takich pomysłów do Ustawy jest po prostu stratą czasu. To jest rozwiązanie kompletnie niefunkcjonalne.

**Co w takim razie spowodowało, że twórcy sięgnęli po takie rozwiązanie?**

Być może brak wiedzy na temat mechanizmu funkcjonowania administracji. Może przyjęto założenie zróbmy taki kroczek, bo jest to lepsze niż nic nie robienie, ale ten kroczek powoduje jeszcze większe zamieszanie.

Moim zdaniem nie jest to rozwiązanie szczęśliwe. Trzeba zabrać konsekwentnie wszystkie uprawnienia w zakresie cyberbezpieczeństwa z Ministerstwa Cyfryzacji i konsekwentnie upodmiotowić organ, który je przejmie, dając mu wprost zadania polegające na zarządzaniu, kreowaniu polityki, wyznaczaniu celów i standardów, oraz nadzorze nad rozwojem cyberbezpieczeństwa w Polsce. To musi być wprost rozpisane, bo w innym przypadku pogłębiamy chaos zamiast cokolwiek naprawiać.

**A co z pełnomocnikiem powołanym w MON, jak Pan ocenia tą decyzję? Czy to nie jest de facto danie kontroli MON-owi, albo dominującej pozycji jeśli chodzi o polski system cyberbezpieczeństwa?**

Tak to jest interpretowane, ale ja nie wiem czy taka była intencja autorów decyzji. Możemy próbować ją zrozumieć jeśli przyjmiemy maksimum dobrej woli. Jednocześnie odkładając tą interpretację, która się pojawiła w licznych komentarzach, np. na Twitterze, że krajowe cyberbezpieczeństwo zostało umundurowane.

Możemy przyjąć takie założenie, że to rozwiązanie jest takie, że Rada Ministrów powołuje pełnomocnika rządu. Nie jestem zwolennikiem tej konstrukcji, powstaje bowiem pytanie, pełnomocnik rządu czyli kogo konkretnie?

Krótko mówiąc nie jest to pełnomocnik premiera, czyli znowu mamy problem, o którym rozmawialiśmy ostatnio - problem przywództwa. Kto jest przywódcą w zakresie systemu cyberbezpieczeństwa. To jest rozwiązanie symboliczne, ja mówię o kwestiach praktycznych czyli to jest rozwiązanie mocno niepełne i takie, któremu trudno przyklasnąć. To jest jeden aspekt.

Załóżmy jednak sytuację, że to przywództwo jest jednoznaczne, że jest to w istocie pełnomocnik premiera. Uważam, że jest to najlepsze rozwiązanie.

Umieszczenie Pełnomocnika w MON ma jeden bardzo ważny plus. Finansowanie pełnomocnika zapewnia bowiem budżet resortu obrony, który dysponuje pokaźnymi środkami na cyberbezpieczeństwo. I to jest jeden plus na który niewątpliwe trzeba zwrócić uwagę.

Możemy sobie wyobrazić, że premier nie chce żeby był to Pełnomocnik w Kancelarii Premiera, ponieważ jak wiemy stara się uporządkować administrację i w ramach tej misji optymalizacji chce się pozbyć pełnomocników i  sekretarzy stanu z Kancelarii, ograniczając zadania Kancelaria do obsługi przede wszystkim Rady Ministrów. W ramach pewnych oszczędności to jest logiczne. Należy tu dostrzec pewną wartość i załóżmy, że jest to po prostu pełnomocnik premiera, który jest tylko formalnie usytuowany w ramach MON-u, natomiast jest w pełni autonomiczny. Takie rozwiązania w różnych krajach zachodnich funkcjonują.

**Może Pan podać przykład?**

Przykładowo w Hiszpanii sekretarze stanu ulokowani w Ministerstwach samodzielnie nadzorują określone działy administracji i mają dużą autonomię. To że taka osoba jest w Ministerstwie nie oznacza, że podlega na co dzień kierownictwu danego Ministra. To jest kwestia pewnego porządku. Przykładowo szef sztabu generalnego w Hiszpanii jest jednym z 4 podsekretarzy stanu w Ministerstwie Obrony i ma swoje ustawowe zadania. Nie jest on wykonawcą poleceń Ministra. W państwach o uporządkowanej administracji, po prostu każdy sekretarz czy podsekretarz stanu czy wysoki urzędnik musi być przyporządkowany do określonego ministerstwa. Jeśli przyjmiemy takie założenie, że formalnie znajduje się w strukturach, ale ma pełną autonomię i realizuje działania pod kierownictwem premiera to jest to do zaakceptowania.

Mało tego jeśli jeszcze zostanie wyposażony w struktury aparatu administracyjnego, mające swoją odrębną lokalizację od Ministerstwa Obrony, tak żeby dać mu organizacyjną autonomię, to takie rozwiązanie jest bardzo dobre. Jeśli Pełnomocnik rzeczywiście będzie realizował zadania wyznaczone przez Premiera w zakresie cyberbezpieczeństwa korzystając z zaplecza MON i dzięki temu będzie w lepszym kontakcie z nim i będzie korzystał z jego budżetu to takiemu rozwiązaniu można tylko przyklasnąć.

Natomiast jeśli tak się nie stanie i będziemy mieli do czynienia z sytuacją, w której tym Pełnomocnikiem zostanie jeden z obecnych sekretarzy stanu w MON, zaangażowany w bieżące prace resortu, który będzie realizował zadania Pełnomocnika obok innych zadań resortu, przez pryzmat interesów, sposobu patrzenia MON to będzie bardzo źle. Zwłaszcza, że jak pamiętamy treść rozporządzanie o powołaniu Pełnomocnika, to musi większość rzeczy uzgadniać jeszcze z Ministrem Cyfryzacji. To nie jest szczęśliwe rozwiązanie. Ono więcej komplikuje niż rozwiązuje.

**Jak Pan mówił w poprzednim wywiadzie w Izraelu cyberbezpieczeństwo ma głównie charakter cywilny. Kwestia wojskowa jest ograniczona.**

Oczywiście tak jest, ale musimy jednocześnie pamiętać, że to państwo jest de facto tworzone przez armię, ponieważ większość obywateli jest rezerwistami.

**Dokładnie, weźmy pod uwagę sektor prywatny, który raczej nie będzie chętny współpracy z wojskiem.**

Dlatego powiedziałem jakie widzę plusy takiego rozwiązania i pod jakimi warunkami można uznać je za pożądane. Chodzi o to czy działalność takiego Pełnomocnika jest głównie motywowana i napędzana myśleniem wojskowym czy myśleniem cywilnym z elementami wrażliwości militarnej. Jeśli będzie to

rozwiązanie bardzo zmilitaryzowane to pamiętajmy, że wojsko ma bardzo specyficzny sposób działania i postrzegania świata. Cechuje je przede wszystkim kult sekretyzmu, dyscypliny, ręcznego sterowania, które absolutnie się nie sprawdzają w życiu cywilnym a tym bardziej w kwestiach technologicznych, gdzie jest potrzebna dociekliwość, innowacyjność, bardzo dobra komunikacja i najważniejsza rzecz czyli zaufanie. Tego nie da się zbudować w sytuacji, kiedy główny kreator i gospodarz będzie miał charakter zmilitaryzowany z takim solidnym backgroundem wojskowym i dominującą specyfiką, mentalnością czy metodologią wojskową. To nie przyniesie dobrego rezultatu. To rozwiązanie spowoduje, że Pełnomocnik będzie hamował rozwój cyberprzestrzeni, współpracy sektora prywatnego z państwem i sektorem bezpieczeństwa i obronności zamiast go rozwijać i otwierać.

Zamiast otworzyć sektor wojskowy na sektor cywilny i ułatwić współpracę, będziemy go zamykać i tą współpracę będziemy tak naprawdę blokować i powstrzymywać zamiast ją otworzyć na sferę prywatną, która jest wielokrotnie większa niż sektor wojskowy i bezpieczeństwa.

**Czyli np. CERT ABW może zacząć podlegać pod MON? Jak zostanie rozwiązana ta sprawa?**

To jest dobre pytanie. Mamy narzędzie w postaci CSIRT.pl, załóżmy, że jest on ciągle w NASKu. Czyli on podlega Ministrowi Cyfryzacji, a Pełnomocnik ds. Cyberbezpieczeństwa  jest w ramach MONu i ma do dyspozycji narzędzie w postaci CERTu wojskowego. To jest rozwiązanie niefunkcjonalne.

Ten Pełnomocnik, o którym mowa w rozporządzeniu Rady Ministrów z 16 marca nie ma żadnych instrumentów i de facto nie ma wyznaczonych precyzyjnych zadań. Z rozporządzenia wynika, że jest on koordynatorem działań instytucji publicznych i wykonawcą polityki rządu. Powstaje jednak pytanie kto określa tę politykę? Czyli ciągle nie mamy kreatora, który wyznaczana cele, który kreuje strategię? Rząd czyli kto? Rząd jest organem kolegialnym.

Uważam, że Pełnomocnik musi zostać wyposażony w jednoznacznie sformułowane, podmiotowe, kreatywne, sprawcze uprawnienia, niech będzie tzw. cybercarem czyli głównym gospodarzem systemu cyberbezpieczeństwa, który ma wyznaczać politykę i  ją realizować po zatwierdzeniu przez rząd, ale niech on ją tworzy. Niech on będzie tym, kto kreuje i odpowiada za jej realizację. Jak będziemy chcieli go rozliczyć to z czego będziemy go rozliczać? Z tego czy on dobrze koordynował? Tego się nie da zrobić. Trzeba mu stworzyć zadania, które będą kwantyfikowalne, które będziemy w stanie precyzyjnie określić i rozliczyć go z tych zadań. Tego w rozporządzeniu nie ma. Dalej brniemy w rozwiązanie nieskuteczne. Ponadto rozporządzenie milczy na temat narzędzi. Brak zapisów informujących w jaki sposób Pełnomocnik ma  realizować swoje zadania i jakimi siłami, jakimi instrumentami organizacyjnymi, prawnymi, funkcjonalnymi. Można założyć, poprzez domniemanie, że mają to być zasoby, które mu oferuje MON, ale to jest rozwiązanie połowiczne, które nie rozwiązuje problemu. Aby był skuteczny, musi zostać wyposażony we władzę premiera, czyli część jego uprawnień powinna zostać na niego scedowana. Pełnomocnik musi być kreatorem dysponującym uprawnieniami dającymi mu władzę nad administracją, pozwalającą na wymuszanie na instytucjach konkretnych działań, a nie tylko koordynować ich prace według własnego uznania. Do urzeczywistnienia tej władzy niezbędny mu będzie wyspecjalizowany aparat ekspercko-urzędniczy oddany do jego wyłącznej dyspozycji.

**Dziękuję za rozmowę.**

---

**płk Grzegorz Małecki** - były Szef Agencji Wywiadu, były Sekretarz Kolegium ds. Służb Specjalnych, dyrektor Programów Cyberbezpieczeństwo oraz Gospodarka i Energetyka Fundacji im. Kazimierza Pułaskiego.