Warszawa, 7 sierpnia 2019r.

Dr hab. Joanna Taczkowska-Olszewska
Prof. Akademii Sztuki Wojennej w Warszawie

**Recenzja rozprawy doktorskiej**

**Mgr Sylwii Olczak nt. *„Koncepcja obiegu informacji o zagrożeniach i incydentach w systemie bezpieczeństwa państwa”* w dziedzinie nauk społecznych, dyscyplinie nauki o bezpieczeństwie przygotowanej pod kierunkiem prof. dr hab. Bogusława Jagusiaka**

## 1. Ogólna ocena rozprawy. Znaczenie podjętej tematyki, metodyka badań.

Potrzeba podjęcia badań naukowych, których przedmiotem jest, w szerokim ujęciu, bezpieczeństwo cyberprzestrzeni, posiada najbardziej fundamentalne uzasadnienie, na jakie wskazuje się w nauce tj. istnienie luki w wiedzy i niedostatek informacji na temat skutecznych rozwiązań, narzędzi i mechanizmów zapewniających ochronę cyberprzestrzeni identyfikowanej jako nowe pole rywalizacji i wpływu a zarazem nowy, nieznany wcześniej teatr wojny. Podjęta przez mgr Sylwię Olczak problematyka dotyczy zagadnień związanych z funkcjonowaniem krajowego systemu cyberbezpieczeństwo przy czym prowadzone badania ogniskują się wokół zagadnień związanych z obiegiem informacji, zgłaszaniem informacji o incydentach bezpieczeństwa a także monitorowaniem i zgłaszaniem zagrożeń przez organy do tego zobowiązane.

Potrzeba zapewnienie bezpieczeństwa w cyberprzestrzeni, wynika nie tylko z dostrzeżonych zagrożeń, jakie rodzi wykorzystanie systemów informacyjnych i sieci komputerowych w działalności państw i organizacji międzynarodowych na płaszczyźnie społecznej, politycznej i gospodarczej, ale także z nałożonych na Państwa członkowskie UE w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii została przyjęta

dnia 6 lipca 2016 r. (zwana dalej dyrektywą NIS albo dyrektywą 2016/1148) obowiązku zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa przez ustanowienie organów właściwych oraz pojedynczego punktu kontaktowego do spraw cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcia krajowych strategii w zakresie cyberbezpieczeństwa.

Wybór podjętej przez mgr Sylwię Olczak tematyki obarczony był wieloma ryzkami, w tym w szczególności ryzykiem szybkiej dezaktualizacji poczynionych spostrzeżeń ze względu na dynamikę rozwoju narzędzi informatycznych i towarzyszących im zmian w przepisach prawa a także ze względu na globalność i aterytorialność zarówno źródeł jak i skutków zagrożeń cybernetycznych a także ze względu na niedostatek modeli teoretycznych i brak jednolitej nomenklatury, które utrudniają wypracowanie jak i zgłoszenie koncepcji rozwiązań zapewniających bezpieczeństwo w cyberprzestrzeni o gwarantowanej i potwierdzonej skuteczności.

Autorka rozprawy nie bez obaw, ale zarazem z dużą odpowiedzialnością, jak wynika z treści rozprawy, tę tematykę podjęła mając świadomość fluktuacji i niepewności rozwiązań prawnych dotyczących cyberbezpieczeństwa. Należy zauważyć, że kiedy mgr Sylwia Olczak rozpoczynała pracę nad przygotowaniem rozprawy, wchodziły w życie rozwiązania zawarte w dyrektywie NIS, podczas gdy w momencie przekazania rozprawy do recenzji tj. na przestrzeni 3 lat, uchwalona została ustawa o krajowym systemie cyberbezpieczeństwo a obecnie w przygotowaniu jest projekt ustawy nowelizującej. Mamy zatem do czynienia – co świetnie uchwyciła Autorka – nie tyle z nową problematyką czy też nowymi zjawiskami, co z nowymi, a nawet prekursorskimi, rozwiązaniami, których celem jest stworzenie takich mechanizmów reagowania na zagrożenia i incydenty w cyberprzestrzeni, które będą posiadały charakter systemowy przez co rozumieć należy nie tylko wyodrębnienie i wskazanie rodzajów organów będących składnikami tego systemu, ale zakres oddziaływania określonych rozwiązań na inne podsystemy (dziedziny) bezpieczeństwa państwa.

Przedmiotem pracy – jak oznajmia Autorka (s. 9) – jest analiza obiegu informacji o zagrożeniach i incydentach wywołanych przez te zagrożenia oraz stosowanych sposobach opisów incydentów i zagrożeń dla zasobów informacyjnych w systemie bezpieczeństwa państwa. Określona w ten sposób tematyka pracy

nieuchronnie zbiegała się z zakresem przedmiotowym ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560), przy czym nie można było uznać, że jest z nim tożsama. Autorka celnie ustala, bazując na treści przepisów ustawy o krajowym systemie cyberbezpieczeństwo, że warunkiem *sine qua non* sprawności i użyteczności tego systemu jest efektywny (prawidłowy, szybki, przejrzysty) obieg informacji o zagrożeniach oraz o incydentach bezpieczeństwa. Autorka zasadnie przyjmuje, że nie można mówić o skutecznej wymianie informacji o incydentach i zagrożeniach bez właściwego ich opisania, za pomocą spójnych, zrozumiałych i ustandaryzowanych formularzy (s.9). Logiczną konsekwencją takiego stanowiska było przyjęcie przez Autorkę, że celem pracy jest opracowanie:1/ szablonu opisu zagrożenia (szablon zgłoszenia zagrożenia) oraz 2/szablonu opisu incydentu (szablon zgłoszenia incydentu) a także 3/ zaproponowanie koncepcji obiegu informacji o zagrożeniach w ramach krajowego systemu cyberbezpieczeństwa.

Zakres podjętych badań, zgromadzony materiał, dobór literatury i piśmiennictwa a także sposób dokonywania wykładni przepisów ustawy o krajowym systemie cyberbezpieczeństwa oraz innych aktów prawnych a także sposób prowadzenia wywodu zostały w całości podporządkowane realizacji postawionego przez Autorkę celu pracy. Zwraca uwagę różnorodność i komplementarność zastosowanych przez Doktorantkę metod. Zasługuje na aprobatę sposób prowadzenia dyskusji z dokonanymi, na różnych etapach prowadzonych badań, ustaleniami. W szczególności widoczny jest wysoki stopień obiektywizacji poczynionych ustaleń, co w efekcie, doprowadziło Autorkę do falsyfikacji jednej z przyjętych hipotez. Nie potwierdziło się zatem założenie, zgodnie z którym stosowane w ustawie rozwiązania w zakresie opisywania incydentów i zagrożeń miały nie pozwalać na międzysektorową współpracę (s. 189). Za miarodajne oraz zbieżne z innymi ustalenia Autorka słusznie przyjmuje opinie wyrażone przez część ekspertów w toku przeprowadzonych przez nią pogłębionych wywiadów.

Zwraca uwagę rzeczowość rozważań, logika wywodu a także skrupulatność z jaką Doktorantka przeprowadza analizę zebranego materiału badawczego, w tym dokumentów, formularzy, treści i formy zamieszczonych w nich pytań. W podobny sposób dokonuje ustalenia zakresu znaczeniowego używanych przez ustawodawcę, jak również stosowanych w doktrynie i piśmiennictwie, podstawowych dla podjętej problematyki, terminów takich jak: „zagrożenie", „incydent",

„bezpieczeństwo informacji", „bezpieczeństwo informacyjne", „zasoby informacyjne", „kluczowe zasoby informacyjne". W sposób przekonujący, logiczny, spójny oraz wyczerpujący Autorka dokonuje ustalenia zakresów tych terminów i proponuje ustalenie ich definicji nie pomijając przy tym dorobku piśmiennictwa i korzystając z wypracowanych i ugruntowanych wzorców. Autorka dowodzi w ten sposób zarówno tego, że posiada znajomość literatury przedmiotu, terminologii a także posiada wiedzę w zakresie nauk o bezpieczeństwie jak również dowodzi dużej dojrzałości badawczej. Dojrzałość ta ujawnia się także w postawie, jaką Autorka przyjmuje w toku badań i na wszystkich jego etapach, w szczególności wówczas, gdy rekomenduje (rozdział V) przyjęcie rozwiązań, które – co do zasady – nie są rewolucyjne bowiem wykorzystują rozwiązania znane, uzupełniając je lub dokonując ich korekty. Autorka zgłasza zatem – w pierwszej kolejności – uwagi *de lege lata* dokonując wykładni zawartych w ustawie o krajowym systemie cyberbezpieczeństwo rozwiązań a następnie formułuje szereg wniosków o charakterze *de lege ferenda*. Należy przypuszczać, że sformułowane wnioski stanowić mogą, o ile ustawodawca zechce je uwzględnić - znaczący wkład w poprawę operacyjności opisanych w ustawie narzędzi a także wpłynąć na poprawę funkcjonalności i skuteczności całego systemu.

Pomimo, że praca nie posiada charakteru ekspertyzy prawnej, to jednak Autorce udaje się utrzymać nie tylko w ryzach konwencji właściwych dla nauk o bezpieczeństwie ale także przyjmowanych na gruncie nauk prawnych. Nie będzie bowiem nadużyciem twierdzenie, że przeprowadzona przez Autorkę analiza – w niektórych co najmniej aspektach – stanowi propozycje wykładni językowej a także funkcjonalnej i systemowej przepisów ustawy o krajowym systemie cyberbezpieczeństwo. Okoliczność ta stanowić winna dodatkowy atut będącej przedmiotem recenzji pracy, bowiem wskazuje na posiadane przez Doktorantkę umiejętności dostrzegania, hierarchizowania oraz systematyzacji terminów prawnych, które posiadają znaczenie normatywne oddziałując na sposób ich stosowania w praktyce, w tym w toku czynności podejmowanych przez organy wchodzące w skład krajowego systemu cyberbezpieczeństwa.

## 2. Uwagi szczegółowe

Realizacja założonego celu pracy, co należy z całą stanowczością podkreślić, posiada niebagatelne znaczenie praktyczne. Autorka wykazała bowiem, z jednej strony, niespójność stosowanej terminologii, w tym niekonsekwentne jej

używanie zarówno w języku prawnym jak i w praktyce działania operatorów usług kluczowych i dostawców usług cyfrowych przekonująco przy tym dowodząc, że niedostrzeżenie przez ustawodawcę tych problemów i zaniechanie aktywności legislacyjnej może stanowić w przyszłości przeszkodę w zapewnieniu sprawnego działania krajowego systemu cyberbezpieczeństwa. Rozprawa stanowi kompleksowe, szczegółowo uzasadnione i wyczerpujące omówienie istotnego dla funkcjonowania systemu cyberbezpieczeństwa problemu, jakim jest wykrywanie i klasyfikowanie zagrożeń, zgłaszanie incydentów bezpieczeństwa oraz wzajemne informowanie się organów zarówno o wykrytych incydentach jak i działaniach podejmowanych w celu zapobiegania, wykrywania i neutralizowania incydentów i zagrożeń. Dla dokonanych przez Autorkę ustaleń i sformułowania ostatecznych wniosków kluczowe znaczenie posiadało poczynione spostrzeżenie, zgodnie z którym „właściwie opisane zagrożenie jest warunkiem niezbędnym do właściwie opisanego incydentu. W obu przypadkach zaś odpowiedni, czyli pełny i zrozumiały dla wszystkich podmiotów opis , stanowi podstawę skutecznej wymiany informacji" (s. 117). Spostrzeżenie to stanowiło zarazem asumpt dla dokonania rozgraniczenia zakresów pojęć „zagrożenie" i „incydent", a w dalszej kolejności dokonania klasyfikacji, na zasadzie rozłączności, rodzajów zagrożeń oraz zmodyfikowanie, w stosunku do istniejącej na gruncie ustawy o krajowym systemie cyberbezpieczeństwa, typów incydentów bezpieczeństwa. Nie bez znaczenia dla kierunku podjętych badań okazało się także dla Autorki ustalenie, że o ile ustawodawca poświęca wiele miejsca opisowi incydentów bezpieczeństwa, o tyle „trudno znaleźć uznane szablony opisu zagrożeń" (s. 121).

Poczynienie przez Doktorantkę powyższych spostrzeżeń było możliwe – na co należy zwrócić uwagę – nie tylko ze względu na zastosowanie przez nią właściwej, odpowiadającej przedmiotowi badania metodologii, ale przede wszystkim ze względu na jej szczególną dociekliwość badawczą a nadto – ze względu na wyjątkowo cenne na gruncie nauk o bezpieczeństwie zapatrywanie, jakie przejawia się w całej pracy, pomimo, że nie zostało ono wyrażone wprost przez Autorkę, wskazujące że opowiada się ona, w dziedzinie bezpieczeństwa informacyjnego, za potrzebą podejmowania działań ofensywnych i odmawia skuteczności działaniom pasywnym, reaktywnym, zachowawczym lub wyłącznie defensywnym.

Dwa z pięciu rozdziałów pracy tj. rozdział IV i rozdział V stanowią szczegółowe przedstawienie wniosków oraz omówienie proponowanych nowych,

postulowanych rozwiązań. Trzon pracy stanowi rozdział czwarty, w którym dokonano rozstrzygnięcia jednego z głównych problemów badawczych dotyczących oceny stosowanych na gruncie aktualnych rozwiązań prawnych standardów opisów incydentów i zagrożeń. Rozdział zamyka koncepcja opisów incydentów i zagrożeń stanowiąca gotowy szablon zaproponowany do stosowania w miejsce istniejących i wykorzystywanych w praktyce CSIRT NASK, CSIRT GOV i CSIRT MON formularzy zgłaszania incydentów. Autorka opracowała i przedstawiła zarówno w formie opisowej jak i w ujęciu graficznym formularze opisów (szablony) incydentów bezpieczeństwa przeznaczone do stosowania w sposób uniwersalny tj. przez wszystkie organy i podmioty wchodzące w skład krajowego systemu bezpieczeństwa a zatem zarówno operatorów usług kluczowych jak i dostawców usług cyfrowych a także podmioty publiczne.

W tym samym rozdziale Autorka dokonała, w oparciu o wnioski płynące z analizy stosowanych rozwiązań w innych systemach prawnych, w szczególności w systemie francuskim oraz na gruncie rozwiązań federalnych w USA, ustaleń w zakresie sposobów klasyfikowania zagrożeń. Przyjęła zarazem, że pod pojęciem zagrożenia należy rozumieć (za K. Lidermanem) „materialny i/lub niematerialny czynnik mogący spowodować niepożądaną zmianę wymaganych wartości istotnych kryteriów informacji" (s. 98). Kryteria te to: tajność, integralność i dostępność. Autorka dostrzegła przy tym nie tylko, że organy odpowiedzialne za zapewnianie cyberbezpieczeństwa w sposób nieuprawniony dokonują utożsamienia pojęcia „incydent" z pojęciem „zagrożenie", ale także wykazała, że dokonują niejednolitej klasyfikacji incydentów. Autorka słusznie wskazuje, że niewłaściwe i utrudniające działanie systemu jest przyjęte bez podstawy prawnej, w sposób dowolny stanowisko, w myśl którego za incydent bezpieczeństwa nie jest uznawane uszkodzenie (zakłócenie) spowodowane przez zdarzenia losowe (CSIRT MON). Autorka poddaje krytyce także takie unormowanie, które w sposób niejasny opisują zgłaszanie zdarzeń nieuznawanych za incydent działom obsługi technicznej bez wskazania konkretnego adresata zgłoszenia (s. 164).

Metodologicznie poprawnie Autorka dokonuje klasyfikacji zagrożeń prawidłowo przyjmując, że opis zagrożeń możliwy jest tylko wówczas, gdy zostanie on poprzedzony ich wyczerpującą klasyfikacją. Wymaga się zarazem, by klasyfikacja ta przebiegała w taki sposób, który prowadzi do wyodrębnienia terminów, których

desygnaty stanowią rozłączne, niekrzyżujące się grupy. Za właściwy, aczkolwiek nie zawsze wystarczający i przydatny przyjmowany jest podział dychotomiczny. Doktorantka, podążając śladem obecnych w nauce propozycji i koncepcji, zaproponowała wyodrębnienie dwóch, rozłącznych grup zagrożeń a w ramach tych grup - dodatkowych, bardziej szczegółowych podzbiorów. W pracy proponuje się podział zagrożeń na dwie grupy tj. „siły wyższe" i „działania ludzi", przy czym zarówno w jednej jak i drugiej grupie wskazane zostają podklasy takiej jak – odpowiednio – „zjawiska przyrodnicze"; „zjawiska społeczno - polityczne" oraz „nieuprawnione i przestępcze działania ludzi" oraz działania ludzi obarczone błędem.

Nie można nie zgodzić się z Autorką, która podnosi, że dla prawidłowości działania systemu cyberbezpieczeństwo konieczne jest nie tylko, co ma aktualnie miejsce, opracowanie szablonu opisu incydentów bezpieczeństwa (pomimo jego niedoskonałości, na co także zwrócono w pracy uwagę i szczegółowo to stanowisko uzasadniono) ale także szablonu opisu zagrożeń, którego stosowania ustawodawca nie przewidział pomimo, że na gruncie ustawy operuje pojęciem zagrożenia a nadto nakłada na operatorów usług kluczowych i dostawców usług cyfrowych obowiązek monitorowania zagrożeń i ich wykrywania. Zawarty w pracy postulat opracowania odpowiedniego szablonu wraz ze wskazaniem jego niezbędnych elementów należy uznać za trafny i wartościowy z puntu widzenia celu, jaki chciał osiągnąć ustawodawca tj. zapewnienia bezpieczeństwa cyberprzestrzeni.

Struktura pracy odzwierciedla przyjęty zamysł badawczy a poszczególne części pracy zostały wypełnione bogatą treścią i poprawnie metodologicznie sformułowanymi wnioskami. Praca ma zatem nie tylko charakter deskryptywny ale w obszernych jej fragmentach przybiera postać wypowiedzi postulatywnych (przykładowo s. 172, 176-190). Zarazem zaproponowana przez Autorkę koncepcja zmierzająca do poprawy i wzmocnienia efektywności działania organów wchodzących w skład systemu cyberbezpieczeństwo na płaszczyźnie wykrywczej a także podejmowanych przez te organy działań *ex post* obejmuje całościowo problematykę związaną z wykorzystaniem, przetwarzaniem i obiegiem informacji równomiernie rozkładając akcenty i dostrzegając potrzebę nadawania równoprawnego znaczenia informacjom o zagrożeniach jak i informacjom o incydentach bezpieczeństwa.

### 3. Ocena końcowa – wnioski i konkluzja

Przedstawiona do recenzji rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego oraz wskazuje, że Autorka posiada wiedzę teoretyczną w dyscyplinie nauki o bezpieczeństwie a nadto wykazuje umiejętność samodzielnego prowadzenia pracy naukowej. W konsekwencji stwierdzam, że rozprawa doktorska mgr Sylwii Olczak spełnia wymagania wskazane w ustawie z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (t.j. Dz. U. z 2017 r. poz. 1789 z późn. zm.). Niniejszym wnoszę o dopuszczenia mgr Sylwii Olczak do kolejnych etapów postępowania o nadanie stopnia doktora w dziedzinie nauk społecznych, dyscyplinie nauki o bezpieczeństwie i dopuszczenie rozprawy, której jest ona Autorką, do publicznej obrony