Załącznik nr 2

AUTOREFERAT

przedstawiający opis dorobku i osiągnięć naukowych

1. Dane osobowe:

Monika Szyłkowska

2. Posiadane dyplomy i stopnie naukowe:

- *Magister prawa* – dyplom ukończenia jednolitych studiów wyższych drugiego stopnia na kierunku: *prawo*, Wyższa Szkoła Administracji i Prawa w Warszawie, 2004 r. Temat pracy magisterskiej: *Problemy dowodowe w sprawach o przestępstwa informatyczne;*
- Dyplom ukończenia studiów podyplomowych, Akademia Obrony Narodowej, Wydział Strategiczno-Obronny, kierunek: *bezpieczeństwo narodowe*, Warszawa 2006 r. Temat pracy dyplomowej: *Możliwości i potrzeby wykorzystania mediów w kształtowaniu bezpieczeństwa narodowego;*
- *Doktor w dziedzinie nauk społecznych* – dyplom doktora nauk społecznych w dyscyplinie nauki o bezpieczeństwie nadany uchwałą Rady Wydziału Bezpieczeństwa Wewnętrznego Wyższej Szkoły Policji w Szczytnie z dnia 18 listopada 2014 r. Tytuł rozprawy doktorskiej: *Ochrona cyberprzestrzeni w systemie bezpieczeństwa narodowego Rzeczpospolitej Polskiej.*

3. Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych

3.1. Umowy o pracę i równoważne – zajmowane stanowiska:

- obecnie od 2015 r. - Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego w Warszawie, Wydział Logistyki, Instytut Systemów Bezpieczeństwa i Obronności – Kierownik Zakładu Strategii i Systemów Obronnych.
- 2012-2013 r. - Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego w Warszawie, Wydział Mechaniczny – prowadzenie zajęć dydaktycznych (umowa – zlecenie).
- 2015 -2016 - Uczelnia Techniczno – Handlowa im. Chodkowskiej w Warszawie – prowadzenie zajęć dydaktycznych – wykładów i ćwiczeń (umowa – zlecenie).

3.2. Pełnione funkcje

Pełnione funkcje oraz członkostwo w organach uczelnianych:

- Kierownik Zakładu Strategii i Systemów Obronnych – Instytut Systemów Bezpieczeństwa i Obronności, Wydział Logistyki WAT (2016-obecnie),
- Członek Senackiej Komisji ds. Rozwoju i Współpracy WAT (2016 – obecnie),
- Członek Rady Wydziału Logistyki WAT (2017 – obecnie),
- Członek Wydziałowej Komisji ds. Finansów i Mienia WLO WAT (2017-obecnie),
- Członek Wydziałowej Komisji Wyborczej WLO WAT (2015-2016),
- Opiekun studentów studiów stacjonarnych I. stopnia odbywających praktyki adaptacyjne w ramach profilu praktycznego kierunku studiów: *obronność państwa* na Wydziale Logistyki WAT (2015-2016),
- Opiekun studentów studiów stacjonarnych I. stopnia odbywających praktyki doskonalące w ramach profilu praktycznego kierunku: *obronność państwa* na Wydziale Logistyki WAT (2015-2016).
- Opiekun studentów studiów stacjonarnych I. stopnia odbywających praktyki adaptacyjne w ramach profilu praktycznego kierunku studiów: *obronność państwa* na Wydziale Logistyki WAT (2016-2017),
- Opiekun studentów studiów stacjonarnych I. stopnia odbywających praktyki doskonalące w ramach profilu praktycznego kierunku: *obronność państwa* na Wydziale Logistyki WAT (2016-2017).
- Opiekun studentów studiów niestacjonarnych II. stopnia w ramach profilu praktycznego kierunku: *obronność państwa* na Wydziale Logistyki WAT (2018-2019),
- Członek redakcji: *Przeglądu nauk o obronności/Defence science review* – WLO WAT, Warszawa 2017, ISSN 2450-6869.

3.3. Zaliczenie do minimum kadrowego na studiach:

- Studia I stopnia na kierunku: *Obronność państwa* na Wydziale Logistyki w Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie w roku akademickim 2018/2019.
- Studia II stopnia na kierunku: *Obronność państwa* na Wydziale Logistyki w Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie w roku akademickim 2018/2019.

4. Wskazanie osiągnięcia wynikającego z art. 16 ust. 2 ustawy z 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz.U. z 2016 r., poz. 882 ze zm. w Dz.U. z 2016 r., poz. 1311.):

a) tytuł osiągnięcia naukowego:

Piąty wymiar bezpieczeństwa – cyberprzestrzeń. Wyzwania, zagrożenia, implikacje.

b) autor, tytuł publikacji, rok wydania, nazwa wydawnictwa, miejsce i rok wydania:

Szyłkowska Monika, *Piąty wymiar bezpieczeństwa – cyberprzestrzeń. Wyzwania, zagrożenia, implikacje,* 2019, Wydawnictwo *Sine qua non*, ss. 218. ISBN: 978-83-8129-557-4 (7,70 ark. wyd.), Kraków 2019.

Recenzenci naukowi:

Prof. dr hab. Michał Huzarski
Prof. dr hab. Ryszard Jakubczak

c) omówienie celu naukowego ww. pracy i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania:

Po pierwsze: bezpieczeństwo.

W tym krótkim stwierdzeniu zawiera się myśl przewodnia obszaru moich zainteresowań badawczych, z którą identyfikuję całą złożoność istoty nauki o bezpieczeństwie. Nauki rozumianej jako: *teorii tego, co rzeczywiste.* Nieustanna troska o rację stanu i fundamentalne interesy narodowe – istnienie, suwerenność, nienaruszalność przetrwania i rozwoju jest podmiotem, przedmiotem, celem i dążeniem *państwa i narodu*. Szczególny przejaw tej troski na niwie naukowej przekłada się w obszarze nieustannych, interdyscyplinarnych badań. Silnie i stabilnie ugruntowana teoria w obszarze bezpieczeństwa daje nie tylko inspirację i podstawy do kolejnych eksploracji naukowych, ale także spełnia kluczową funkcję – możliwość pragmatycznego zastosowania w kształtowaniu systemu bezpieczeństwa. Odniesienie do istoty rozważań nad bezpieczeństwem, wyrażone słowami F. Hölderlina: *Lecz gdzie jest niebezpieczeństwo – rośnie także ratunek*, pozwoliło mi na pogłębione rozważania - w innej, niż dotychczasowa - perspektywie. Identyfikowanie źródeł zagrożeń oraz ocena możliwości ich materializacji pozwalają na dostosowanie określonych i odpowiednich zarówno środków zaradczych, jak i restytucyjnych. M. Heidegger wyprowadza istotę *ratunku* od *pochwycenia czegoś zagrożonego upadkiem w celu*

zabezpieczenia dotychczasowego tego czegoś istnienia[1]. W istocie myśl ta staje się uniwersalną i transponującą *teorię tego, co rzeczywiste.* Można przyjąć tezę, że zagrożenia mają najbardziej kreacyjną funkcję dla tworzenia systemu bezpieczeństwa – od minimalizacji materializacji zagrożeń począwszy. Podstawowym kryterium staje się zatem nieustanne poszukiwanie i identyfikacja *niebezpieczeństw.* Pod tym względem cyberprzestrzeń ma w zasadzie nieograniczone pokłady eksploracji, doskonale egzemplifikując przy tym także klasyczny paradoks poznawczy. Jednak sama identyfikacja i analiza zagrożeń to niepełne spektrum działań dla doskonalenia systemu bezpieczeństwa, ponieważ proces ten wymaga poszukiwania powiązań i relacji oraz normatywnego modelowania.

Wskazane myśli przewodnie, towarzysząc mi przez lata eksploracji naukowej, były kluczową inspiracją i asumptem do podjęcia badań nad materią zakreśloną tematem wskazanego osiągnięcia. Moje zainteresowania problematyką wpływu oddziaływania szeroko rozumianej cyberprzestrzeni na bezpieczeństwo jednostki i państwa – w tym badania empiryczne, których początek sięga roku 2000 oraz prowadzone w późniejszym czasie badania naukowe, w których uczestniczyłam zarówno jako członek zespołu, wykonawca, jak i organizator – pozwoliły na pogłębione eksploracje w tej materii.

Podjęcie przedstawionej tematyki stanowiło próbę kompleksowego odniesienia się do zagadnienia, które w literaturze naukowej nie znajduje jeszcze szerokiego pola zainteresowania w zaproponowanym ujęciu. Problematyka, która stała się przedmiotem moich badań, znajduje odniesienie w opracowaniach krajowych i zagranicznych, jednak jest jeszcze znacznie rozproszona w różnych dziedzinach i dyscyplinach nauki. Znaczenie pozyskiwania nowej wiedzy o zjawiskach oraz mechanizmach zjawisk zachodzących w sferze cyfrowej wpływających na poziom bezpieczeństwa oraz możliwości doskonalenia systemu bezpieczeństwa państwa przesądziły ostatecznie o wyborze przedmiotu badań zaprezentowanych w przedstawionej publikacji. Temat przewodni monografii stał się zarazem jej celem poznawczym i utylitarnym - próbą pokazania zarówno deterministycznej złożoności cyberprzestrzeni, jak i analizy jej wpływu na wybrane obszary bezpieczeństwa. W warstwie poznawczej celem stała się identyfikacja cyberprzestrzeni postrzeganej jako kolejny – piąty wymiar bezpieczeństwa oraz introjekcja mechanizmów kształtowania się zależności zjawisk i procesów zachodzących pomiędzy przestrzenią cyfrową a bezpieczeństwem państwa. Natomiast w warstwie utylitarnej - naukowe określenie zakresów wspólnych relacji zachodzących pomiędzy wybranymi zjawiskami w cyberprzestrzeni dla określenia ich potencjalnych konsekwencji dla bezpieczeństwa państwa.

[1] M.Heidegger, *Technika i zwrot*, s.37. Wyd. Baran i Suszczyński, Kraków 2002. ISBN 83-88575-35-X.

Przy tak sformułowanym celu, naukowej eksploracji należało poddać identyfikację obszarów funkcjonowania państwa w przestrzeni cyfrowej oraz czynniki determinujące kształtowanie systemu bezpieczeństwa państwa w tym wymiarze. Kolejnym elementem badań była identyfikacja przyczyn zagrożeń cyfrowych, ich rodzajów, przebiegu, zasięgu skutków oraz kierunków oddziaływania na bezpieczeństwo państwa. Pojawiła się także konieczność zidentyfikowania współczesnych konfliktów w przestrzeni cyfrowej oraz określenia możliwości – i zasadności – ich prawnego usankcjonowania w kontekście wpływu na kształtowanie środowiska bezpieczeństwa państwa. Niezbędnym elementem badań było także zidentyfikowanie potencjału proliferacji cyberzagrożeń z uwzględnieniem tzw. czynnika ludzkiego oraz określenie kierunków rozwoju. W celu uzyskania jak najszerszego obrazu badanej problematyki konieczne było także zidentyfikowanie i reasumpcja obszarów implikujących konieczność włączenia w proces projektowania systemu bezpieczeństwa państwa takich zagadnień, jak: suwerenność techniczna i technologiczna oraz kompetencje cyfrowe użytkowników (obywateli) w zakresie możliwości tworzenia niematerialnych sił i środków obrony narodowej. Dla osiągnięcia założonego celu niezbędne było również określenie kierunków możliwych zmian dla wielowymiarowego środowiska bezpieczeństwa wraz z oceną legislacyjnych *konieczności i możliwości* jako newralgicznego elementu działań podejmowanych w celu przeciwdziałania zagrożeniom o charakterze cyfrowym.

Realizacja przyjętego w badaniach celu wymagała sprecyzowania głównego problemu badawczego, który przybrał postać pytania: *W jakich obszarach i zakresach można skutecznie wykorzystać możliwości sieciowe cyberprzestrzeni (przestrzeni cyfrowej) w tworzeniu i funkcjonowaniu systemu bezpieczeństwa państwa, przy integralnym postrzeganiu cyberprzestrzeni jako jego piątego wymiaru?* Przyjęte założenie uwarunkowało konieczność przeanalizowania wybranych zjawisk oraz dostosowywania zakresu pojęciowego w określonych obszarach problemowych. Na potrzeby prowadzonych badań szczegółowe problemy badawcze zostały sformułowane w postaci następujących pytań: *Co jest istotą cyberprzestrzeni w wymiarze bezpieczeństwa? Jaki charakter mają zidentyfikowane zagrożenia w niej występujące? Jakie rodzaje cyberzagrożeń są kluczowe dla bezpieczeństwa państwa? Jakie znaczenie ma tzw. czynnik ludzki w proliferacji zagrożeń cyfrowych? Jakie wyzwania niesie cyberprzestrzeń w systemie obronnym państwa? Jakie są atrybuty cyfrowego konfliktu w porównaniu do klasycznych definicji? Jaka jest prawna możliwość wypowiedzenia cyfrowej wojny? Jakie inne obszary bezpieczeństwa implikuje cyberprzestrzeń? Jaka istnieje możliwość (i zasadność) ponoszenia odpowiedzialności*

prawnej za cyfrowy produkt? Jaki mechanizm powoduje, że usługi cyfrowe wymuszają pozorne udzielanie zgody przez użytkowników? Jakie znaczenie ma niepożądane wysyłanie informacji o użytkowniku przez oprogramowanie? Na ile jest możliwe znalezienie równowagi pomiędzy wolnością w sieci a bezpieczeństwem? Jakie są implikacje cybertożsamości? W jakim zakresie kompetencje cyfrowe obywateli mogą stanowić niematerialną siłę w tworzeniu obrony narodowej w tej sferze?

Przeprowadzona - na etapie wstępnego procesu badawczego - analiza ukazała interdyscyplinarny charakter podjętego problemu, w związku z czym powstała konieczność zastosowania różnych, adekwatnych metod, technik i narzędzi badawczych, identyfikowanych przede wszystkim w dyscyplinie nauk o bezpieczeństwie, ale także w naukach prawnych. W procesie badawczym szeroko korzystałam z jakościowych metod badawczych, m.in. w postaci: analizy (w tym: analizy prawno-instytucjonalnej, komparatystycznej, systemowej oraz metod: analizy i konstrukcji logicznej), syntezy, abstrahowania, porównania, uogólniania i wnioskowania. Metoda analizy pozwoliła przede wszystkim na ustalenie wzajemnych związków występujących pomiędzy istotą i cechami cyberprzestrzeni a *oddziaływaniem* na funkcjonowanie państwa oraz wpływem na kształtowanie systemu bezpieczeństwa. Wynika z tego kluczowy wniosek, iż cyberprzestrzeń stanowi obecnie kolejny obszar stanowiący nieodłączny element funkcjonowania państwa, a tym samym - wpływa na środowisko jego bezpieczeństwa. Z kolei wśród ilościowych metod badawczych intensywnie wykorzystywałam analizę statystyczną oraz sondaż diagnostyczny. Poza analizą literatury - istotnym wsparciem procesu badawczego było badanie dokumentów (m.in. przepisów prawa krajowego i międzynarodowego) oraz dostępnych źródeł wiedzy o badanych problemach. Wykorzystany materiał źródłowy obejmował zarówno opracowania zwarte, jak i opublikowane w czasopismach specjalistycznych. Wskazane metody pozwoliły na pozyskanie materiału badawczego o dużej złożoności. Na tym etapie badań zostały przeze mnie przeanalizowane obowiązujące regulacje prawne w obszarze bezpieczeństwa – w tym cyberbezpieczeństwa (krajowe i międzynarodowe), dokumenty strategiczne oraz wybrane *polityki ochrony*. W wyniku powyższego zweryfikowałam i zaprezentowałam w formie teorii w szczególności: *Pojęcie, istotę i charakterystykę cyberprzestrzeni* (1.3.1.); *zakres pojęciowy oraz charakterystykę cyberkonfliktów (1.2.) pojęcie, istotę oraz charakterystykę cyberzagrożeń (2.1.); ataki socjotechniczne (2.2.); możliwości proliferacji cyfrowych zagrożeń przez tzw. czynnik ludzki (2.3.); antytetyczność cyfrowej wolności (3.3.), cybertożsamość jako determinant ochrony (3.4.).* Analiza instytucjonalno-prawna została

wykorzystana do oceny rozwiązań krajowych w obszarze cyberprzestrzeni (1.4.1.;2.1.3.;3.2.;3.4.) oraz regulacji i postanowień zawartych na poziomie międzynarodowym (1.3.;3.1.;2.1.2). Analiza systemowa pozwoliła na ujęcie badanych zjawisk jako elementów systemu (1.1.). Analiza komparatystyczna pozwoliła z kolei na porównanie określonych procesów i zjawisk (1.2.;3.2.). Dzięki syntezie poszczególnych wyników badań w zakresie przyjętych problemów badawczych (obszarów) możliwe było wykorzystanie metody uogólnienia na wyższym poziomie – i tym samym – zidentyfikowanie uniwersalnych determinant. W trakcie procesu badawczego wykorzystałam także metodę delficką, która pozwoliła na zastosowanie uogólnionych ocen prognostycznych ekspertów. Z zastosowanych metod empirycznych należy wskazać przede wszystkim zasygnalizowany wcześniej: sondaż diagnostyczny – przeprowadzony w postaci ankiet z wykorzystaniem techniki *CAWI* - dotyczący: a.) kompetencji cyfrowych użytkowników oraz b.) wiedzy obywateli w obszarze obrony narodowej. Etap empiryczny badań polegał także na ocenie wykładni strategicznej warunkującej funkcjonowanie systemu bezpieczeństwa państwa oraz ocenie stanu prawnego, organizacyjnego i funkcjonalnego. Nasuwające się wnioski zostały skonfrontowane z poglądami prezentowanymi w publikacjach zarówno instytucji państwowych, jak i pozycjach zwartych. Nadmienione opracowania teoretyczne pozwoliły zarówno na poznanie najnowszych, obowiązujących i ukonstytuowanych poglądów dotyczących problematyki bezpieczeństwa, jak i stanowiły źródło analizy komparatystycznej – w szczególności w zakresie *atrybutów cyberkonfliktów* oraz *odpowiedzialności za produkt cyfrowy*. W całym zakresie prowadzonych badań odwoływałam się do analizy poglądów zaprezentowanych w literaturze związanej z przedmiotem badań, zaś podstawę procesu badawczego związanego z opracowaniem niniejszej monografii stanowiła teoria nauk o bezpieczeństwie oraz nauk prawnych. W procesie weryfikacji przyjętej hipotezy ważną rolę odegrały również rozmowy i konsultacje eksperckie, które stanowiły znaczące uzupełnienie wskazanych metod badawczych.

Kognitywne i utylitarne przesłanki podjętej przeze mnie problematyki stanowią realizację przyjętej hipotezy: *Dynamiczny wzrost znaczenia złożonej problematyki cyberprzestrzeni dostarcza wielu przekonujących argumentów przemawiających za jej postrzeganiem jako piątego wymiaru bezpieczeństwa państwa w ujęciu systemowym, z uwzględnieniem generowanych wyzwań, zagrożeń i implikacji.* Tak określone założenie pozwoliło na ukierunkowanie wybranych obszarów problemowych. Analiza dynamiki *stałych zmian*, determinowanych przez *przestrzeń cyfrową* stała się wyzwaniem wymagającym nie tylko przyjęcia określonych obszarów badawczych, ale także uwzględnienia

ich *sieciowości problemowej* w systemie o niezliczonej - i niedającej się zamknąć w enumeratywną całość - ilości elementów i powiązań. Potwierdzenie przyjętego założenia można odnaleźć w obowiązujących dokumentach i koncepcjach strategicznych, jednak pogłębionej, wieloaspektowej analizy wymagały zarówno zagadnienia, które dopiero zarysowują się w zakresie pojęciowym, jak i te, które dotąd nie były przedmiotem poszerzonych badań.

Przyjęte założenia pozwoliły określić następujące hipotezy badawcze: *Cyberprzestrzeń stanowi nieodłączny element funkcjonowania państwa i tym samym komponent środowiska bezpieczeństwa wymagający komplementarności z pozostałymi w zakresie tworzenia systemu bezpieczeństwa. Cyberzagrożenia mogą mieć bezpośredni wpływ na funkcjonowanie państwa, dlatego determinują kształtowanie jego systemu bezpieczeństwa. Cyberprzestrzeń implikuje konieczność aktualizacji istniejących, zarówno krajowych, jak i międzynarodowych rozwiązań prawnych. Konsekwencją interferencji cyberzagrożeń na poziomie globalnym powinno być prawo do cyfrowej wojny. Dynamika rozwoju form funkcjonowania kreowana przez dostępne rozwiązania techniczne oraz nowe rodzaje zagrożeń determinują potrzebę określenia nowego paradygmatu bezpieczeństwa. Kompetencje cyfrowe użytkowników – obywateli mają wpływ na potencjalną proliferację zagrożeń, ale <a contrario> - mogą też stanowić istotny element w procesie minimalizacji ryzyka. Wiedza i umiejętności obywateli mogą stanowić niemilitarną siłę w tworzeniu obrony narodowej w sferze cyfrowej.*

Wskazane problemy badawcze wpłynęły zarówno na kolejność, jak i dobór obszarów, które umiejscowiono w trzech płaszczyznach: wyzwań, zagrożeń i implikacji determinowanych przez cyberprzestrzeń. Również struktura pracy została podporządkowana głównemu celowi, która składa się z trzech rozdziałów teoretycznych, odpowiadających wytypowanym obszarom. Proces badawczy został podzielony na etapy, odzwierciedlające dążenie do szerokiej eksploracji wskazanych obszarów i zjawisk z nimi związanych. Proces ten był konsekwencją złożoności samego obiektu badań, jak i jego relacji w wybranych obszarach problemowych.

Wstępny etap został poświęcony określeniu istoty cyberprzestrzeni, jej struktury, cech oraz korelacji w ramach systemu bezpieczeństwa państwa. Przyjęłam założenie, że na tym etapie badań ustalone zostanie znaczenie takich pojęć, jak: *cyberprzestrzeń* i *cyberkonflikt* oraz zidentyfikowane zostaną warstwy cyberprzestrzeni warunkujące tworzenie się określonych procesów i zagrożeń. W odniesieniu do zakresu pojęciowego punktem wyjścia była analiza definicyjna zawarta w krajowych regulacjach

oraz dokumentach strategicznych, na podstawie których przedstawiona została struktura cyberprzestrzeni (warstwa: materialna, logiczna i kognitywna) oraz scharakteryzowane zostały jej poszczególne cechy. Wypracowane w tej części wnioski pozwoliły na stwierdzenie, że zakres pojęciowy *cyberprzestrzeni* jest szeroki, ponieważ obejmuje: ogół środków i narzędzi komunikacyjnych oraz informacyjnych do użytku cywilnego i/lub wojskowego, w ramach których zawierają się: sieci (wszystkie rodzaje), urządzenia, techniki, technologie, aktorzy (usługodawcy, operatorzy i użytkownicy) oraz przestrzenie (komunikacyjne). Logiczną konsekwencję części wstępnej badania stanowiła teoretyczna analiza środowiska bezpieczeństwa państwa w wymiarze cyfrowym w oparciu o przepisy regulujące krajowy system cyberbezpieczeństwa. Przedstawiony w nim model organizacyjny wraz z usystematyzowanym zakresem kompetencji i zadań należy ocenić pozytywnie – jednak rozwiązaniem *idealnym* byłoby stworzenie kompleksowej, jednolitej architektury informatycznej dla wszystkich struktur na bazie krajowych rozwiązań (producentów), stanowiącego bazę integracyjną dla modułowych podsystemów. Wskazane rozwiązanie pozwoliłoby przede wszystkim na uniezależnienie od funkcjonujących obecnie, komercyjnych systemów globalnych producentów. Suwerenność techniczna i technologiczna jest i będzie stanowiła zarówno o przewadze, możliwościach rozwoju, jak i poziomie bezpieczeństwa całego systemu informacyjnego państwa. Przykładem może być brak dostępu do kodów źródłowych wykorzystywanych rozwiązań informatycznych. Komercyjne rozwiązania w tak newralgicznych systemach, jak *resorty bezpieczeństwa* powinny zwrócić szczególną uwagę decydentów na - nie tyle potencjalne, co realne zagrożenia dla przepływów informacyjnych. Łańcuch bezpieczeństwa każdego systemu informacyjnego bierze swój początek w posiadanych i wykorzystywanych rozwiązaniach technicznych. Z tego względu krytyczne i newralgiczne znaczenie posiada wspomniana wyżej suwerenność. W takim kontekście przyjęcie szerokiej definicji cyberprzestrzeni jako: *przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne (...) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*[2] wspiera argument przemawiający za stworzeniem państwowego systemu na bazie rodzimych rozwiązań. Wynikiem wypracowanych tej części wniosków jest konstatacja, że organizacja systemu bezpieczeństwa państwa w wymiarze bezpieczeństwa cyberprzestrzeni RP - stanowiącej część cyberbezpieczeństwa państwa obejmuje: siły, środki oraz *zespół przedsięwzięć organizacyjno-prawnych, fizycznych, technicznych i edukacyjnych,* w celu *zapewnienia niezakłóconego*

[2] Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne.* Dz.U. 2005 Nr 64 poz. 565.

funkcjonowania cyberprzestrzeni RP ze szczególnym uwzględnieniem bezpieczeństwa przetwarzanych w niej zasobów informacyjnych.

Dalsza część procesu badawczego w obszarze wyzwań - obejmowała odniesienie do zjawiska *cyberkonfliktu* – jego istoty i atrybutów. Analiza komparatystyczna oparta została o teorię *klasycznych* definicji, które w literaturze przedmiotu znalazły liczne opracowania. Również materiały dokumentów prawa międzynarodowego pozwoliły na pogłębione rozważania w zakresie typologii konfliktów oraz ich własności. W wyniku przeprowadzonych badań istotne znaczenie miało ukazanie konfliktów, które wcześniej nie były przedmiotem licznych analiz - określanych mianem: *długich* (czas) i *nierozwiązanych* (brak zawartego porozumienia) oraz tzw. *wojen bez końca*, których istotą jest *brak zainteresowania (interesu) stron (lub strony) do rozwiązania konfliktu*. Identyfikacja wskazanej typologii pozwoliła na zaproponowanie definicji pojęcia *cyberkonfliktu* jako: *konfliktu asymetrycznego, którego cechami charakterystycznymi są: skrytość, zmienność, zaskoczenie, rozproszenie oraz nieograniczony zasięg*. Dokonana analiza pozwoliła na konstatację, iż do cech wyróżniających cyberkonflikty spośród ich klasycznych odpowiedników należą: przestrzeń działania, forma oraz wykorzystywane narzędzia walki – niezmienne natomiast pozostają: cele, motywy i skutki. Wypracowane w tej części wnioski pozwoliły również na stwierdzenie, że wyzwaniem teraźniejszości staje się konieczność usankcjonowania *operacji cybernetycznych* na poziomie międzynarodowym (*cyfrowe konwencje*) oraz *prawa do cyfrowej wojny* w dwóch odniesieniach: *cyfrowej* reakcji na cyberatak oraz możliwości reakcji przy użyciu konwencjonalnych metod w odpowiedzi na atak cybernetyczny. Pomimo istniejących barier technicznych oraz tych wynikających z samej istoty i atrybutów konfliktów cyfrowych – pozostawanie biernym wobec wyzwań strategicznych w niedalekiej przyszłości może doprowadzić do *bezbronności reaktywnej*.

Kolejny etap badań ukierunkowany został na identyfikację determinant cyberprzestrzeni w obszarze zagrożeń. W jego ramach dokonałam analizy i klasyfikacji zagrożeń według przyjętych wcześniej kryteriów. Punktem wyjścia stały się dedykowane dokumenty oraz propozycja przyjęcia zakresu pojęciowego cyberprzestrzeni jako: *obszaru infrastruktury technicznej, logicznej i kognitywnej, w którym funkcjonują systemy informacyjne, umożliwiające operowanie danymi oraz przetwarzanie i wymianę informacji opartą na relacjach i powiązaniach użytkowników*. Konsekwencją tak przyjętego założenia stała się propozycja ujęcia *cyberzagrożenia* według kryterium technicznego jako: *bezprawnego działania mającego na celu: modyfikację, przejęcie kontroli lub destrukcję infrastruktury technicznej, logicznej i kognitywnej – w szczególności na funkcjonowanie*

systemów informacyjnych. Uwzględniając dyskusyjny charakter ogólnego ujęcia zakresu przedmiotowego przyjęłam kryterium techniczne, ponieważ nawet nieintencjonalna proliferacja tego rodzaju zagrożenia posiada określony cel umiejscowiony w kodzie binarnym. Przy bardzo dużej ostrożności można wyłączyć z tej grupy jedynie błędy programistyczne oraz awarie, które jednak nie zwalniają od konieczności ich uwzględniania w projektowaniu systemów bezpieczeństwa. Kluczowym wynikiem przeprowadzonych badań była możliwość stwierdzenia, że katalog zagrożeń cyfrowych jest zbiorem otwartym i - z przyczyn obiektywnych - niewyczerpanym. Natomiast możliwe stało się określenie głównych kategorii zagrożeń, których przykład mogą stanowić dychotomiczne podziały: konieczności reakcji użytkownika lub braku konieczności działania, aby doszło do materializacji zagrożenia. W dalszej części procesu badawczego analizie poddałam dokumenty źródłowe w obszarze klasyfikacji zjawiska cyberprzestępczości – w tym szczegółowej analizie dwie formy: podrobienia i przerobienia dokumentu na gruncie prawa polskiego. Biorąc pod uwagę statystyki obrazujące skalę strat finansowych tak jednostek, jak i instytucji - wskazane rodzaje przestępstw w przestrzeni cyfrowej nabierają istotnego znaczenia. Szersza perspektywa pozwala dostrzec kierunki możliwych interakcji na poziomie systemu bezpieczeństwa, szczególnie w odniesieniu do płaszczyzny ekonomicznej. W ramach wskazanego procesu badawczego pogłębionej analizie komparatystycznej poddałam również zjawisko cyberterroryzmu, w wyniku której zaproponowałam definicję zakładającą, iż będą to: *wszelkie bezprawne, niezależne od motywów, intencjonalne działania (użycie lub groźba użycia przemocy albo siły) podejmowane przez osobę lub grupę osób wbrew obowiązującemu porządkowi prawnemu danego państwa w celu wymuszenia na jego władzach określonego zachowania (działania lub zaniechania) z wykorzystaniem metod zastraszenia lub wywołania poczucia zagrożenia, które to działania nie wyczerpują znamion międzynarodowego prawa do obrony własnej (samoobrony) - obejmujące zarówno działalność w systemach teleinformatycznych, jak i wszelką działalność terrorystyczną związana z cyberprzestrzenią.* Kolejny etap badań stanowiła próba identyfikacji i analizy cyfrowych zagrożeń dla bezpieczeństwa państwa, w której przyjęłam założenie, że należą do nich wszelkie nielegalne operacje elektroniczne wymierzone przeciwko odporności (bezpieczeństwu) systemów informacyjnych państwa lub procesowanym przez te systemy danym. Operacje te mogą być *popełnione za pomocą systemów lub sieci, lub mogą dotyczyć systemów lub sieci.* Przeprowadzona analiza pozwoliła na konstatację, iż w informacyjnym wymiarze bezpieczeństwa państwa zagrożenia mogą oddziaływać negatywnie na wszystkie sfery i obszary działalności - w szczególności w kontekście infrastruktury krytycznej.

Fakt ten pozwolił na ogólną diagnozę pozwalającą przyjąć, iż stopień zagrożeń systemów informacyjnych jest proporcjonalny do stopnia technicznego zaawansowania państwa i uzależnienia funkcjonowania przepływów informacji w całym obszarze gospodarki informacyjnej zachodzących w tych systemach. W ramach pogłębionych badań wskazałam wybrane rodzaje zagrożeń w środowisku informacyjnym państwa. Natomiast przyjęte kryterium - wraz z analizą komparatystyczną istniejących definicji - umożliwiło zaproponowanie zakresu pojęciowego *walki informacyjnej* zawierającego: *kompleksowe działania defensywne i ofensywne w celu uzyskania przewagi informacyjnej nad przeciwnikiem z wykorzystaniem systemów informacyjnych oraz sieci komputerowych wraz z możliwością neutralizacji lub zniszczenia sieci przeciwnika przy jednoczesnej ochronie własnych.*

Kolejny etap badań w obszarze zagrożeń został poświęcony zjawiskom: ataków socjotechnicznych oraz proliferacji zagrożeń cyfrowych, które do tej pory nie znalazły jeszcze szerokiego pola zainteresowania w literaturze naukowej. Należy podkreślić, że obecnie obowiązujące regulacje i dokumenty strategiczne w zasadzie tylko sygnalizacyjnie wskazują na konieczność podnoszenia poziomu świadomości użytkowników, podkreślając ich znaczenie, jednak bez precyzyjnie określonych rozwiązań. Mając na względzie określony cel szczegółowy, za niezbędne uznałam przeprowadzenie badań ilościowych w obszarze *kompetencji cyfrowych użytkowników*. Ich wyniki pozwoliły m.in. na stwierdzenie, iż pomimo zadowalającego poziomu w zakresie wiedzy respondentów dotyczących istnienia oraz rodzajów cyberzagrożeń, nadal pozostaje wiele do zrobienia w zakresie wzmocnienia wiedzy, np. sposobów minimalizacji ryzyka. W kontekście walki informacyjnej i związanym z nią zjawiskiem (nierzadko już narzędziem) określanym mianem: *fake news* - interesujące wyniki dotyczą wiedzy badanych o ich istnieniu (ponad 80%) oraz możliwości wykorzystania portali społecznościowych do działań propagandowych (ponad 90%), z których jednak niewiele ponad połowa weryfikuje informacje pozyskane z sieci. Kluczowe znaczenie w tym zakresie posiada inna z wyróżniających cech cyberprzestrzeni – możliwość tworzenia treści przez użytkowników. Fakt ten powoduje znaczące spektrum możliwości wykorzystania defensywnych i ofensywnych środków walki informacyjnej. Otrzymane wyniki pozwoliły również na stwierdzenie, że poziom proliferacji zagrożeń będzie proporcjonalny do wiedzy i umiejętności cyfrowych użytkowników. Ten sam współczynnik dotyczy możliwości materializacji ataku socjotechnicznego. Wskazane wyniki badań pozwoliły na zidentyfikowanie konieczności szerszego uwzględnienia tzw. czynnika ludzkiego w procesie kształtowania systemu bezpieczeństwa, w szczególności biorąc

pod uwagę fakt, iż użytkownicy pełnią również różne role zawodowe, a ich nawyki *przenoszą się* symultanicznie do sfery zawodowej.

Ostatni obszar badań stanowiły wybrane implikacje określane przez cyberprzestrzeń. Dla realizacji procesu badawczego wyselekcjonowałam zagadnienia związane z podstawą wykorzystywania urządzeń elektronicznych w warstwie programowej – wraz z analizą kluczowych kwestii, tj.: pozornego udzielania zgody przez użytkowników *wymuszane* przez urządzenia i aplikacje oraz brak kontroli nad rodzajem, czasem i zakresem informacji wysyłanych przez urządzenia bez wiedzy użytkowników. Ten sam proces dotyczył możliwości, potrzeb i barier związanych z odpowiedzialnością za *produkty cyfrowe.* Przenalizowany przeze mnie empirycznie proces korzystania z wybranego urządzenia elektronicznego od momentu pierwszej aktywacji pozwolił na odkrycie pozornego wyrażania zgody przez użytkownika. W przypadku braku akceptacji (poprzez zaznaczenie) - określonych przez producenta regulacji wyświetlonych na ekranie urządzenia, nie istnieje możliwość uruchomienia jego pełnej funkcjonalności pozwalającej na korzystanie z niego bez dodatkowej ingerencji w oprogramowanie systemowe. Innym zidentyfikowanym przejawem *pozorności* jest brak precyzyjnych informacji producenta w zakresie rodzaju, czasu i sposobu przesyłania danych z urządzenia użytkownika. Krytyczne znaczenie posiadają - zastrzeżone przez producenta -możliwości przesyłania przez posiadane urządzenia *informacji potrzebnych do działania ważnych usług* - nawet w przypadku wyłączenia określonych funkcji przez użytkownika. Przeprowadzona analiza pozwoliła na stwierdzenie, że obecnie brakuje rozwiązań prawnych chroniących użytkowników w tym względzie - obligujących producentów urządzeń oraz programów do należytej staranności i dbałości o wyczerpujące informacje w tym zakresie. Wśród zidentyfikowanych luk należy także wskazać brak jasno określonego zakazu instalowania ukrytych funkcji programów (też w znaczeniu: systemów operacyjnych) oraz odpowiedzialności w przypadku ich nielegalnego rezydowania. Dokonana analiza przepisów normatywnych z zakresu przetwarzania danych pozwoliła stwierdzić, że zawarte w nich zasady ochrony nie mają zastosowania – bez wyjątku - do informacji anonimowych (*w tym przetwarzania do celów statystycznych lub naukowych).* Wyjątek powinny stanowić urządzenia mobilne, ponieważ istniejąca na gruncie prawa polskiego konieczność rejestracji każdej karty SIM (ang. *subscriber identity module*) powoduje jednoznaczną i precyzyjną identyfikację właściciela urządzenia, w którym jest instalowana. Wynikiem przeprowadzonych badań jest konstatacja potwierdzająca słuszność argumentów przemawiających za koniecznością dostosowania regulacji prawnych do realnych zjawisk.

Przesadnie ogólne zapisy pozostawiają zbyt duży margines interpretacyjny ze szkodą dla ochrony praw użytkowników.

W kolejnym etapie badawczym wykonałam pogłębione badania natury refleksyjnej relacji: *cyberwolności* i *cyberbezpieczeństwa*. Dla realizacji procesu badawczego oba zjawiska zostały usytuowane jako kontrapunkty w celu ustalenia możliwości osiągnięcia równowagi w tej mierze.

W wyniku przeprowadzonych badań ustaliłam, że immanentnymi atrybutami cyberwolności są:

- możliwości nieodpłatnego korzystania z zasobów sieci - w tym dostępu do informacji, dóbr kultury, nauki, rozrywki,
- możliwości *wyrażania siebie* w dowolny sposób w przestrzeni cyfrowej,
- brak kontroli i nadzoru (jedyne ograniczenia stanowią postanowienia regulaminów poszczególnych usług).

Drugim przejawem cyfrowej *wolności* jest zakres oraz formy wykorzystania tej przestrzeni w działaniach przestępczych – również dedykowanych dla tej sfery. Fakt ten powoduje pilną konieczność dokonania fundamentalnych zmian zarówno w postrzeganiu swobody korzystania z przestrzeni cyfrowej, jak i możliwości (konieczności) wprowadzenia ograniczeń na rzecz bezpieczeństwa. Wyniki przeprowadzonych badań pozwalają na stwierdzenie, że zmiany, które powinny nastąpić winny dotyczyć przede wszystkim powstania regulacji na poziomie międzynarodowym wraz z ustanowieniem transparentności działania i odpowiedzialności w zakresie usług. Można przyjąć ostrożne założenie, że osiągnięcie pożądanej równowagi w relacji: wolność – bezpieczeństwo w przestrzeni cyfrowej byłoby teoretycznie możliwe pod warunkiem zmiany mentalności i nastawienia samych użytkowników, którzy – zgodnie z wynikami badań sondażowych – byliby skłonni zaakceptować wprowadzenie określonych regulacji (np. w odniesieniu do nielegalnych treści) na rzecz podniesienia poziomu bezpieczeństwa. Zmiany te następują w wolniejszym tempie, niż dynamika determinowana przez coraz to nowe rozwiązania i usługi techniczne, niemniej - każdy początek- to właściwy krok w kierunku bezpieczeństwa. Stąd po raz kolejny pojawia się postulat konieczności podnoszenia wiedzy i świadomości użytkowników już na poziomie edukacji podstawowej. Tylko kompleksowe działania w tym zakresie mają szansę urzeczywistnić w przyszłości ideę wolności i bezpieczeństwa w przestrzeni cyfrowej. Obecnie dla części użytkowników sieć internetowa jest jeszcze *światem bez konsekwencji*, jednak zauważalne przemiany społeczne oraz pojawiające się wraz z nimi wyzwania powinny stanowić stały punkt analiz, prognoz i pragmatycznych rozwiązań.

W ostatnim z wyselekcjonowanych obszarów problemowych etap procesu badawczego zamykają badania sondażowe przeprowadzone w aspekcie niematerialnych sił i środków obrony narodowej - związane ze społecznym odbiorem i identyfikacją pojęć związanych z *bezpieczeństwa państwa* i *obrony narodowej w obszarze cyberprzestrzeni.* Wyniki przeprowadzonych badań potwierdziły wstępnie, że w cyfrowym wymiarze środowiska bezpieczeństwa poziom wiedzy oraz kompetencje cyfrowe użytkowników – obywateli pozwalają na możliwość wykorzystania niemilitarnych środków obrony narodowej w tworzeniu nowego modelu bezpieczeństwa w strukturze państwa. Ponadto badania wykazały istnienie znaczącej świadomości użytkowników w tym zakresie (na przykład możliwość oficjalnego ogłoszenia wojny cyfrowej). Zakres wyzwań stojących przed możliwością wykorzystania kompetencji użytkowników w tworzeniu obrony narodowej dopiero się zarysowuje i wymaga pogłębionych badań, jednak został już jednoznacznie zidentyfikowany i może stanowić motor postępu w sposobie myślenia. Podjęte w tej mierze działania docelowo powinny umożliwić udoskonalenie koncepcji tworzenia systemu bezpieczeństwa państwa – o tak newralgiczny element, jak niemilitarne środki obrony narodowej w cyberprzestrzeni z szerokim spektrum ich zastosowania.

Całość przeprowadzonego procesu badawczego zamykają uogólnione wnioski oraz podsumowanie. Wśród refleksji kończących rozważania jedno z najważniejszych przesłań zawiera się w konstatacji, iż zrozumienie coraz bardziej skomplikowanego środowiska bezpieczeństwa oraz tworzenie systemu bezpieczeństwa państwa wymaga uwzględnienia *sieciowości problemowej* implikowanej przez cyberprzestrzeń. Z kolei osiągnięcie a*daptacyjnej elastyczności* wymagać będzie zmian na poziomie organizacyjno – funkcjonalnym, co można uznać obecnie za istotną barierę, biorąc pod uwagę złożoność problemów ukazanych *tylko* w wybranych obszarach monografii. Wnioskowane podjęcie działań i – docelowo - prac legislacyjnych - z pewnością przyczyniłoby się nie tylko do zwiększenia *cyfrowej* świadomości społecznej, ale przede wszystkim - ukonstytuowałoby w tym zakresie normatywne podstawy ochrony. Ponadto wyniki przeprowadzonych badań mogą stać się przydatne dla organów i instytucji państwa – w tym decydentów szczebla strategicznego. Z kolei propozycje możliwych zmian, przedstawione z zamiarem dążenia dostosowania istniejących rozwiązań do dynamiki przemian oraz powstawania nowych zjawisk (tak w zakresie ich wieloaspektowości, jak i uwarunkowań) determinujących pojawiające się wyzwania, wnoszą stosowne pojęcia teoretyczne do nauk społecznych oraz dają możliwość ich pragmatycznego wykorzystania, w szczególności w obszarze nauki o bezpieczeństwie. Definiowanie pojęć i zjawisk pozwala na uzyskanie możliwości

przewidzenia skutków i określenia środków zaradczych, ale szczególnie – na pragmatyczne działania prewencyjne. Zaproponowane ujęcie tematu może również zarysować przyszłościowe nurty badawcze, przyczyniając się do stworzenia nowego paradygmatu w naukach społecznych.

W ramach konkluzji pragnę podkreślić, że wskazane osiągnięcie jest opracowaniem konsumującym wyniki badań wybranych zagadnień cyberprzestrzeni w wymiarze bezpieczeństwa wraz z ich reasumpcją, stanowiąc próbę systematyzacji moich badań dotyczących problemu naukowego odzwierciedlonego tytułem monografii. Stąd na *wybrane problemy* składają się badania, których wyniki znalazły się po części na łamach czasopism o zasięgu krajowym i międzynarodowym. Tematyka ta nie tylko nie traci na aktualności, ale znajduje coraz szersze zrozumienie, tak w aspekcie teoretycznym, jak i praktycznym. Pojawiające się teorie naukowe służą wzmocnieniu poziomu bezpieczeństwa zarówno jednostek, jak i państw, stanowiąc wsparcie dla praktycznych możliwości doskonalenia systemu bezpieczeństwa (co stanowiło również moją intencję jako autorki niniejszej monografii). Opracowanie zapewne nie jest wolne od niedoskonałości w zakresie rozwiązywanego problemu, jednak nie są one wynikiem nierzetelności metodologicznej czy niedbałości, lecz dynamiką zmian w tej mierze w trakcie realizacji procesu badawczego.

Podsumowując omówienie wskazanego osiągnięcia, odnosząc się przy tym do istoty i dążeń moich badań nad deterministyczną złożonością cyberprzestrzeni, posłużę się parafrazą sentencji: *Wszystko jest możliwe, ale nie wszystko pewne.* Z tego powodu analiza nowych zjawisk w tempie dynamiki zachodzących zmian w systemowym, pięciowymiarowym ujęciu bezpieczeństwa państwa może umożliwić doskonalenie jego systemu, czyniąc go tym samym efektywnym i bardziej odpornym.

5. **Omówienie pozostałych osiągnięć naukowo – badawczych:**

W ramach pracy naukowo – badawczej swoje zainteresowania koncentruję wokół problematyki bezpieczeństwa w ujęciu interdyscyplinarnym, w szczególności w obszarze: *cyberbezpieczeństwa i prawa bezpieczeństwa.* Inspirację i asumpt do podjęcia badań w pierwszym z przedstawionych obszarów stanowiła nie tylko moja fascynacja nowoczesną techniką, jej możliwościami oraz wpływem na zakres i formy funkcjonowania, ale także zamiłowanie do jej poznawania i analizowania w połączeniu z wiedzą zdobywaną poprzez praktykę oraz teorię w trakcie studiów, co znalazło swoje odzwierciedlenie zarówno

w wybranym temacie pracy magisterskiej (*Problemy dowodowe w sprawach o przestępstwa informatyczne)*, jak i w rozprawie doktorskiej (*Ochrona cyberprzestrzeni w systemie bezpieczeństwa narodowego Rzeczpospolitej Polskiej).* Badania empiryczne zostały zapoczątkowane poprzez korzystanie z nowoczesnych narzędzi na poziomie prywatnym jako użytkownik. Wyniki pierwszych eksperymentów, które stały się późniejszą inspiracją i asumptem do podjęcia badań naukowych, zakończyły się uniemożliwieniem dalszego korzystania z urządzeń elektronicznych. Cyfrowe narzędzia, które posłużyły do badań empirycznych stanowiły: a.) złośliwy program – pobranie i uruchomienie załącznika z niewiarygodnego źródła, b.) zamierzona infekcja złośliwym programem wygenerowanym za pomocą dedykowanego oprogramowania, c.) instalacja oprogramowania o innym, niż określone, przeznaczeniu, d.) zamierzona instalacja oprogramowania monitorującego działania użytkownika. Zwieńczeniem podjętej w kolejnym etapie - pracy badawczej było przeprowadzenie badań oraz publiczna obrona rozprawy doktorskiej przygotowanej pod kierownictwem prof. dr. hab. Ryszarda Jakubczaka: *Ochrona cyberprzestrzeni w systemie bezpieczeństwa narodowego Rzeczpospolitej Polskiej* [Archiwum WSPoL, ss. 483. WSPoL, Szczytno 2014,]. Zaproponowane w rozprawie propozycje zdefiniowania pojęć:

- *cyberprzestrzeni* – jako *obszaru* (systemy, sieci, urządzenia), *w którym funkcjonuje zdigitalizowana informacja wytworzona przez człowieka* (twórcę informacji) *w dowolnej formie* (dźwięk, obraz, dane), w którym to obszarze *informacja może być: wytwarzana, przetwarzana, transmitowana i przechowywana – determinując dalsze powiązania i działania poprzez cele (cel powstania) i funkcje (przekazanie informacji), aby osiągnąć za jej pomocą określony skutek (lub zmianę),*
- *ochrony cyberprzestrzeni, którą stanowi ochrona informacji w niej funkcjonujących przed celowym (lub niecelowym): naruszeniem, zniekształceniem, modyfikacją, uszkodzeniem lub zniszczeniem, niezależnie od obiegu (zamkniętego lub otwartego) oraz formy, w jakiej funkcjonuje* – stały się dla mnie wyznacznikiem do pogłębionych badań zarówno pod względem funkcjonalnym, jak normatywnym. Możliwości prawnych regulacji *wirtualnych* zjawisk również stanowią część mojego zamiłowania do badań w tej dziedzinie, stanowiąc inspirację do poszukiwania rozwiązań w tym zakresie - przede wszystkim na rzecz bezpieczeństwa. Argumentem przemawiającym za potrzebą ich istnienia jest stopień zaawansowania i wykorzystywania techniki w każdej dziedzinie oraz skala, rodzaje i potencjalne skutki materializacji przestępstw cyfrowych.

Rozwój naukowy oraz doskonalenie warsztatu badawczego nastąpił od momentu podjęcia przeze mnie pracy w Wydziale Logistyki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie w Instytucie Systemów Bezpieczeństwa i Obronności, w którym od 2016 r. jestem również kierownikiem Zakładu Strategii i Systemów Obronnych. W trakcie dotychczasowej działalności naukowo-badawczej (poza dydaktyką, w ramach której wykorzystywałam wyniki przeprowadzonych badań) – byłam także zaangażowana w badania podstawowe w tym obszarze. Wieloaspektowe podejście do problemów z obszaru: prawa, bezpieczeństwa, obronności czy logistyki oraz odbyty staż naukowy w Instytucie Transportu Samochodowego w Warszawie (2018 r.) pozwoliły na zbudowanie potencjału wiedzy, który umożliwia holistyczne ujmowanie wielu zjawisk determinowanych przez dynamicznie zmieniające się uwarunkowania. W kolejnych etapach pracy naukowo-badawczej szczególną uwagę poświęcałam badaniom nad zachowaniem użytkowników oraz zgłębiałam problematykę proliferacji zagrożeń w strukturze przepływów informacyjnych, co znalazło swoje odzwierciedlenie m.in. w monografii współautorskiej B.Wiśniewski, R. Kowalski, J. Kozioł, M.Szyłkowska, *Bezpieczeństwo procesów decyzyjnych*, WKA TUM, Wyd. Fundacja Obserwatorium Społeczne 2018. ISBN 978-83-7454-445-0, Wrocław 2018, jak i realizowanych samodzielnie projektach badawczych. W szczególności rezultaty badań empirycznych zawarte w przedstawionej monografii stanowiły część prac naukowo – badawczych w ramach badań podstawowych, których jestem kierownikiem. Należą do nich: *Niematerialne środki obrony narodowej* - kierownik pracy, Warszawa 2017-2018 [kod pracy: PBS 881/2018] oraz: *Proliferacja zagrożeń implikowanych przez użytkowników informacji newralgicznym czynnikiem ich bezpieczeństwa* - kierownik pracy, Warszawa 2019-2020 [kod pracy: PBS 904/2019].

W ciągu ostatnich pięciu lat pracy od momentu obrony rozprawy doktorskiej spośród badań, które zrealizowałam samodzielnie lub w zespołach badawczych, osiągnięcia stanowią między innymi opracowania naukowe w postaci zwartej, rozdziały w monografiach oraz artykuły naukowe w recenzowanych czasopismach naukowych wydawnictw krajowych i międzynarodowych (m.in. w Niemczech, Bułgarii, Słowacji, na Ukrainie), popularyzujących wiedzę z zakresu bezpieczeństwa. Dorobek ten stanowią zarówno opracowania samodzielne, jak i wypracowane wspólnie z innymi współautorami.

✓ Monografie i rozdziały w monografiach:

1. B.Wiśniewski, R. Kowalski, J. Kozioł, M.Szyłkowska, *Bezpieczeństwo procesów decyzyjnych*, WKA TUM, Wyd. Fundacja Obserwatorium Społeczne 2018. ISBN 978-83-7454-445-0 (udział własny: 25%). Ilość arkuszy wyd.: 9,77 (całość ss. 210), Wrocław 2018.

2. M.Marciniak (red.), B.Ćwik, J. Figurski, J.M. Niepsuj, M.Szyłkowska, S.Wojnarowska-Szpucha, K.E. Świerszcz, *Dylematy Współczesnej Obronności Polski - Pozamilitarne uwarunkowania obronności Państwa* (udział własny- rozdział 7, 72-82, ss. 270), Wydawnictwo Adam Marszałek, ISBN 978-83-8019-839-5. Toruń 2017.

3. L.S.Kościelecki, Z. Trejnis (red.), J.Bil, P. Bryczek-Wróbel, M. Cieślarczyk, M.Szyłkowska (i.in.), *Wyzwania i zagrożenia bezpieczeństwa i obronności RP w XXI wieku w wymiarze społecznym i technologiczno-środowiskowym*. Monografia stanowi sprawozdanie z realizacji zadania badawczego zatytułowanego „Wyzwania i zagrożenia bezpieczeństwa i obronności Rzeczypospolitej Polskiej w XXI wieku" realizowanego w ramach Grantu Badawczego nr 997/2018 pt. „System logistyczny determinantem zdolności obronnych Rzeczypospolitej Polskiej" przez Wydział Logistyki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie, finansowanego przez Ministerstwo Obrony Narodowej RP. Praca zbiorowa – uczestnik, udział (rozdział, s. 30, całość: ss. 381, ilość ark. wyd.: 22,9). Wyd. Oficyna Wydawnicza ASPRA-JR. ISBN 978-83-7545-913-5. Warszawa 2018.

✓ Rozdziały w monografiach:

4. B. Wiśniewski, M.Szyłkowska, *Bezpieczeństwo cyberprzestrzeni - wyzwania prawne i organizacyjne* [w:] Cyberprzestrzeń - uzależnienia, zahamowania, zagrożenia, Akademia Pomorska IBN, Wyd. Fundacja PRO POMERANIA Słupsk, s. 51-68, ISBN 978-83-63680-31-2 (mój udział w opracowaniu wynosi 50%), Słupsk 2016.

   W publikacji dokonana została analiza oraz diagnoza ówczesnego stanu organizacyjno-prawnego w obszarze bezpieczeństwa cyberprzestrzeni – z uwzględnieniem regulacji zawartych w szczególności w: Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Ustawie z dnia 29 sierpnia 2002 r. *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*, Ustawie z dnia 6 czerwca 1997 r. - *Kodeks karny,* Ustawie z dnia 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną,* Ustawie z dnia 12 września 2002 r. *o elektronicznych instrumentach płatniczych,* Ustawie z dnia 29 sierpnia 1997 r. - *Prawo bankowe* oraz Ustawie z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym.* Zasygnalizowany został również zakres regulacji zawarty w późniejszej Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.*

5. M.Szyłkowska, *Organy państwa wykonujące zadania policji administracyjnej* [w:] Administracja bezpieczeństwa. Wybrane problemy. Tom II. Wyższa Szkoła Administracji w Bielsku-Białej, s. 201-212; ISBN 978-83-935790-9-9, Bielsko-Biała 2016.

   W rozdziale dokonana została systematyzacja organów państwa wykonujących zadania policji administracyjnej. Organy tego rodzaju mają szczególny charakter - poza funkcjami kontrolnymi - posiadają również kompetencje typowe dla organów administracji państwowej - w szczególności kompetencje władcze (np. wydawanie decyzji) oraz funkcje policyjne. Formy funkcjonowania, jak i działania wykorzystywane

przy ich sprawowaniu realizowane są zarówno przez inspekcje, jak i wyspecjalizowane służby administracyjne wyposażone w funkcje nadzorczo-regulatywne oraz kontrolne (wydawanie pozwoleń, wymierzanie pieniężnych kar administracyjnych). Ponadto niektóre z nich posiadają kompetencje i prerogatywy inwestygatorskie (ścigania karnego przestępstw i przestępstw skarbowych oraz wykroczeń) oraz dochodźcze (np. Straż Graniczna, Służba Celna - a w zakresie postępowania uproszczonego m.in.: Inspekcja Handlowa, Prezes UKE, czy Straż Leśna).

6. M.Szyłkowska, *Prawne wyzwania dla cyfrowych zagrożeń* [w:] Współczesne wyzwania nauk społecznych i ekonomicznych, Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej, s.546-556. ISBN 9788362250370, Warszawa 2016.

   Kluczowym wynikiem dociekań zakreślonych tematem wskazanego rozdziału był postulat stworzenia oddzielnego aktu w postaci *Ustawy o ochronie cyberprzestrzeni*, zawierającego spójne definicje z obszaru cyberprzestrzeni; określającego kompetencje i zadania z uwzględnieniem struktury państwowej i podziału władz, jak również stworzenie nowych instytucji, posiadających wyodrębnione kompetencje oraz jednostki na płaszczyźnie cywilnej i wojskowej (np. Agencja Ochrony Cyberprzestrzeni, Wojskowa Służba Ochrony Cyberprzestrzeni). Z kolei utworzenie *Urzędu Ochrony Cyberprzestrzeni*, pozwoliłoby skoncentrować wysiłki, zadania i kompetencje w jednej instytucji.

7. M.Szyłkowska, *Współczesne problemy zwalczania cyberprzestępczości* [w:] *Bezpieczeństwo wewnętrzne a prawo i zarządzanie (wybrane problemy)*. Szkoła Główna Służby Pożarniczej, s. 35-52, ISBN 978-83-88446-62-7, Warszawa 2016.

   W rozdziale zostały przedstawione wyniki badań nad problematyką zwalczania cyberprzestępczości, wskazując na ich szeroki i heterogeniczny zakres - począwszy od nieścisłości zbiorów pojęciowych w regulacjach prawnych, po problemy dowodowe w zakresie przestępstw *stricte* internetowych. Dokonana została również analiza komparatystyczna przestępstw klasyfikowanych jako: *dokonanych z użyciem komputera* oraz *przeciwko systemom* - wraz z refleksją w zakresie trudności dowodowych w takich przypadkach.

8. M.Szyłkowska, W. Jakubczak, *Wyzwania i koncepcje ochrony cybeprzestrzeni w erze globalizacji* [w:] Cyberprzestrzeń - uzależnienia, zahamowania, zagrożenia, Akademia Pomorska IBN, Wyd. Fundacja PRO POMERANIA, s.69-98, ISBN 978-83-63680-31-2 (mój udział w opracowaniu wynosi 50%), Słupsk 2016.

   W materii publikacji znalazły się wyniki analizy, której zostały poddane istniejące koncepcje ochrony cyberprzestrzeni na poziomie międzynarodowym, jak i obowiązujące w tym zakresie dokumenty strategiczne oraz regulacje prawne. Przedstawione zostały także aktualne (wówczas) tendencje wraz z omówieniem założeń i celów budowy współpracy militarnej oraz potencjału obrony cyberprzestrzeni opartej o wspólne systemy ostrzegania i wymiany informacji, a także rozwijania zdolności do współdziałania we wszystkich stanach (pokoju, kryzysu i wojny).

9. M.Szyłkowska, R. Socha, *Organizational and Legal Conditions of Command in the Legal System in Poland* [w:] Schriften zu Mittel - und Osteuropa in der Europäischen Integration. Band 21 Management Contexts in Security Institutions, s. 97-108 (mój udział w opracowaniu wynosi 50%). ISBN 978-3-8300-9339-8, Hamburg 2017.

   W rozdziale dokonano analizy uwarunkowań prawno-organizacyjnych kierowania i dowodzenia w czasie pokoju oraz w czasie wojny na gruncie polskiego systemu prawa w świetle nowelizacji przepisów w tym zakresie wraz z analizą zmiany systemu kierowania i dowodzenia w ramach reformy Sił Zbrojnych zapoczątkowanej w roku 2011, stanowiącej ówcześnie jeden z *głównych kierunków rozwoju Sił Zbrojnych Rzeczypospolitej Polskiej oraz ich przygotowań do obrony państwa na lata 2013-2022.*

10. B.Wiśniewski, M. Szyłkowska, *Stany nadzwyczajne i zarządzanie kryzysowe w cyberprzestrzeni* [w:] Zarządzanie instytucjami publicznymi i prywatnymi w kontekście niepewności zagrożeń, kryzysów i ryzyka, s. 299-316. ISBN 978-83-7462-578-4 (mój udział w opracowaniu wynosi 50%), Wyd. WSPol, Szczytno 2017.

    W publikacji zaprezentowane zostały kluczowe rekomendacje związane z organizacją systemu bezpieczeństwa w osnowie normatywnej w kontekście stanów nadzwyczajnych oraz zarządzania kryzysowego, które mogą zostać wywołane przez *działania w cyberprzestrzeni.* Zwrócono uwagę na konieczność regulacji prawnych w szczególności dotyczących organów administracji – w kwestii określenia zasad ich działania oraz procedur podejmowania decyzji we wszystkich fazach zarządzania kryzysowego.

11. W. Kaczmarek, M.Szyłkowska, *Warunki prawne odpowiedzialności za oprogramowanie - zarys problemu* [w:] Administracja Bezpieczeństwa – wybrane problemy Tom IV, Wyższa Szkoła Administracji w Bielsku - Białej, 2017, s. 119-130. ISBN 978-83-935790-0-6 (mój udział w opracowaniu wynosi 50%), Bielsko-Biała 2017.

    W rozdziale przedstawiono (w zarysie) problematykę istniejących oraz brakujących regulacji prawnych dotyczących produktów cyfrowych i urządzeń elektronicznych oraz warunków odpowiedzialności za te produkty. Analizie poddano w szczególności: Dyrektywę Rady z dnia 14 maja 1991 r. *w sprawie ochrony prawnej programów komputerowych* (91/250/EWG), Dyrektywę Rady z dnia 25 lipca 1985 r. *w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe* (85/374/EWG), Ustawę z dnia 30 czerwca 2000 r. - *Prawo własności przemysłowej* oraz Ustawę z dnia 12 grudnia 2003 r. *o ogólnym bezpieczeństwie produktów.*

12. M.Szyłkowska, *Cyberterroryzm - zagrożenia dla bezpieczeństwa jednostki i państwa* [w:] *System logistyczny determinantem zdolności obronnych RP* – 1. Wyzwania i zagrożenia bezpieczeństwa i obronności RP w XXI wieku". Praca zbiorowa – uczestnik, udział własny: 30 s., całość: ss. 381; ISBN 978-83-7545-913-5. Warszawa 2018.

    W publikacji dokonana została analiza pojęciowa zjawiska *cyberterroryzmu* ocenianego obecnie jako jedno z najszybciej rosnących zagrożeń, wraz ze wskazaniem praktycznych przykładów – oraz propozycją teoretycznej typologii (cyberterroryzm właściwy (tylko w cyberprzestrzeni) i *quasi*-cyberterroryzm (wykorzystujący cyberprzestrzeń

jako element działań). Ponadto przedstawione zostały potencjalne rodzaje broni *cybeterroryzmu technicznego* i *elektromagnetycznego* (m.in. z użyciem IEMI, HPM i EMP).

13. M.Szyłkowska, *Postępowanie sprawdzające i poświadczenie bezpieczeństwa w kontekście globalnych form kontaktu* [w:] „Współczesne Problemy Zarządzania i Bezpieczeństwa", Wyd. UTH, ISBN 978-83-62250-42-4, Warszawa 2019.

    We wskazanej publikacji analizie poddano kwestie istniejącej procedury postępowania sprawdzającego na gruncie prawa polskiego oraz poświadczenia bezpieczeństwa w kontekście globalnych - cyfrowych form kontaktu. Głównym celem rozważań było wskazanie konieczności aktualizacji regulacji dotyczących omawianej materii - w szczególności - *Ankiety bezpieczeństwa osobowego* - stanowiącego załącznik do ustawy, w odniesieniu do form kontaktu z obywatelami obcych państw, które obecnie odbywają się najczęściej za pośrednictwem komunikatorów cyfrowych.

✓ Wybrane artykuły naukowe:

14. M.Szyłkowska, *Cyberzagrożenia nowoczesnych rozwiązań informatycznych wspierających logistykę* [w:] Gospodarka Materiałowa & Logistyka, Nr 5/2015, Polskie Wydawnictwo Ekonomiczne S.A., s. 719-730, ID: 620240, ISSN 1231-2037, Warszawa 2015.

15. M. Szyłkowska, J. Murasicki, *Cyfrowa globalizacja determinantem współczesnego bezpieczeństwa* [w:] Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy Nr 16(3)/2015, s. 73 - 83, ISSN 1896-8333, eISSN 2449-9013 (mój udział w opracowaniu wynosi 70%), Legnica 2015.

16. M. Szyłkowska, *IT threats to national security: description, classification and problems* [w:] Bulletin of the Lviv State University of Life Safety/ Вісник Львівського державного університету безпеки життєдіяльності /Bulletin of Lviv State University of Life Safety, Nr 12/2015, s. 18 – 22, ISSN 2078-4643, Lwów 2015.

17. M.Szyłkowska, M. Kulczycki, *The Armed Forces as the guarantee of the safety and peace on the country's territory and beyond the border`s- legal regulations* [w:] Вісник Львівського державного університету безпеки життєдіяльності / Bulletin of the Lviv State University of Life Safety, s. 6-11, No. 12/2015, ISSN 2078-4643 (mój udział w opracowaniu wynosi 50%), Lwów 2015.

18. M.Szyłkowska, *Regulation on State of Exception in Polish Legislation* [w:] Schriften zu Mittel- und Osteuropa in der Europäischen Integration/Legal Context in the Chosen Order and Security Area, Verlag Dr. Kovač, s. 135-148, ISBN 978-3-8300-9140-0, Hamburg 2016.

19. M.Szyłkowska, *Cyfrowe wyłudzenia i fałszerstwa jako kluczowe zagrożenia dla przedsiębiorstw-ogniw łańcucha dostaw* [w:] Polskie Wydawnictwo Ekonomiczne, Gospodarka Materiałowa & Logistyka, Nr 5/2016 (CD), s. 716-727, ISSN 1231-2037, Warszawa 2016.

20. M.Szyłkowska, R. Polak, *Cyfrowe wyzwania logistyki* [w:] Polskie Wydawnictwo Ekonomiczne, Gospodarka Materiałowa & Logistyka, Nr 9/2016, s. 719-729, ISSN 1231-2037 (mój udział w opracowaniu wynosi 60%). Warszawa, 2016.
21. M.Szyłkowska, *Cyfrowe zagrożenia i wyzwania dla bezpieczeństwa państwa - przegląd, klasyfikacje, definicje,* Sociálno-psychologické aspekty utvárania osobnosti príslušníkov ozbrojených síl, bezpečnostných a záchranných zborov: zborník vedeckých a odborných prác z medzinárodnej vedecko-odbornej konferencie v Liptovskom Mikuláši, Akadémia Ozbrojených Síl gen. M. R. Štefánika, ISBN 978-80-8040-519-9 Słowacja 2016.
22. M.Szyłkowska, *Cyber threats in logistics - an outline of the problem* [w:] „Vasil Levski" National Military University/ "Scientific Works", s.130-139, ISBN 978-954-9681-82-6, *Cybersecurity in the information society*, Shumen 2017.
23. M.Szyłkowska, *Human factor in the proliferation of threats* [w:] The Intentional Scientific Journal: "Security & Future" Issue 2/2018, s. 55- 58, ISSN (Print) 2535-0668, ISSN (Online) 2535-082X. Red. Prof. Nikolay Radulov, Sofia 2018.
24. M.Szyłkowska, *Security challenges for cyber identity-outline of the problem* [w:] International Scientific Journal "Industry 4.0." ISSUE 2, P.P. 102-105 (2019), ISSN 2535-0005 (Print), ISSN 2535-0013. Sofia 2019.

Prezentowaną powyżej aktywność badawczą przedstawiałam na krajowych i międzynarodowych konferencjach oraz seminariach naukowych, gdzie w formie referatów lub wystąpień zaprezentowałam zagadnienia problemowe oraz wyniki prowadzonych w tym zakresie dociekań, m.in.:

- ✓ II Konferencja Koordynacyjna udziału Polski w Projekcie MCDC 2015-2016 - spotkanie robocze: "Koncepcja działań militarnych w cyberprzestrzeni", Warszawa 2015;
- ✓ Międzynarodowa Konferencja naukowo – techniczna: *Medzinárodná vedecko - odborná konferencia Sociálno - psychologické aspekty utvárania osobnosti príslušníkov ozbrojených síl, bezpečnostných a záchranných zborov*, Liptovský Mikuláš, Słowacja 2015.
- ✓ I Międzynarodowa Konferencja Naukowa: *Współczesne problemy zarządzania i bezpieczeństwa*, UTH, Zakopane 2016;
- ✓ VIII Ogólnopolska Konferencja Naukowa: *Udział nowoczesnych rozwiązań w zapewnieniu bezpieczeństwa Polski w świetle aktualnych zagrożeń,* WSGE, Józefów 2016;
- ✓ VIII Konferencja Naukowa Logistyki Stosowanej: *Technologie podwójnego zastosowania w logistyce cywilnej i wojskowej. Teoria i praktyka*, ILOG WLO WAT, Rynia 2016;

- ✓ III Międzynarodowa Konferencja Naukowa: Współczesne Problemy Zarządzania i Bezpieczeństwa, UTH, Zakopane 2017 r.;
- ✓ International Scientific conference: Cybersecurity in the information society, "VASIL LEVSKI" National Military University, Shumen, Bułgaria 2017;
- ✓ II International Scientific Conference on Security „CONFSEC 2018", Scientific-Technical Union of Mechanical Engineering, Bułgaria 2018.

Ponadto byłam zaangażowana w organizację konferencji naukowych, których zakres tematyczny odnosił się do obszarów badawczych będących w centrum moich naukowych zainteresowań – również tych o charakterze interdyscyplinarnym, m.in.:

- ✓ I Edycja Konferencji: *Bezpieczeństwo Granic Europy XXI w. „Ochrona granic Unii Europejskiej w kontekście procesów migracyjnych*, WLO WAT, Warszawa 2015.
- ✓ I Ogólnopolska Konferencja Naukowo – Szkoleniowa: *Pozamilitarne przygotowania obronne, zarządzanie kryzysowe i obrona cywilna w systemie bezpieczeństwa i obronności Rzeczypospolitej Polskiej*, ISBiO WAT, Warszawa 2016.
- ✓ I Ogólnopolska Konferencja Naukowa: *Dylematy współczesnej obronności RP*, ISBiO WLO, Warszawa 2017.
- ✓ II Ogólnopolska Konferencja Kół Naukowych, Warszawa 2017.
- ✓ II Międzynarodowa Konferencja Naukowa: *Dylematy współczesnej obronności i bezpieczeństwa RP*, ISBiO WLO WAT, Warszawa 2018.
- ✓ Konferencja Naukowa: *ANIMUS BELLI 2017*, Akademia Sztuki Wojennej, Warszawa 2017.
- ✓ I Ogólnopolska Konferencja Naukowa *GlobState*, 2018: *Wyzwania dla bezpieczeństwa państwa w aspekcie zmieniającego się środowiska geopolitycznego*, CDiS SZ, Bydgoszcz 2018.
- ✓ III Ogólnopolska Konferencja Kół Naukowych Wydziału Logistyki WAT „Nowe wyzwania i kierunki przemian w logistyce", ILOG ISBiO WLO WAT, Warszawa 2018.

W tym miejscu warto również wskazać, że jestem autorką następujących recenzji:

- ✓ monografii Gula P.; Prońko J.; Wiśniewski B.: *Zarządzanie informacją w sytuacjach kryzysowych (wydanie II uzupełnione)*, ISBN: 978-83-60430-08-X, WSA Bielsko-Biała 2015;
- ✓ artykułu naukowego: *National critical infrastructure as the target of cyberattacks* [w:] „Zeszyty Studenckie PRO PUBLICO BONO", Rocznik Szkoły Głównej Służby Pożarniczej w Warszawie, Warszawa 2017;

- ✓ artykułu naukowego: *Wyzwanie XXI wieku – wojna w cyberprzestrzeni* - II Ogólnopolska Konferencja Kół Naukowych „Logistyka i obronność w świetle nowych technologii", WLO WAT 2017;
- ✓ artykułu naukowego: *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, Przegląd Teleinformatyczny / Teleinformatics Review ISSN 2300-5149, Warszawa 2018.

W ramach popularyzacji nauki byłam autorką artykułów pt.: *Cyberprzestrzeń – nowe pole działań podczas nowoczesnej wojny*, Informator Obrony Cywilnej i Zarządzania Kryzysowego, Marzec 1/2016. ISSN 1733-8417 oraz *Cztery strony informacji*, Informator Obrony Cywilnej i Zarządzania Kryzysowego. ISSN 1733-8417.

W kategoriach stanowiących istotny wkład w działalność naukową należy postrzegać także osiągniecia o charakterze dydaktycznym, w ramach których prowadziłam i prowadzę następujące zajęcia (obejmujące wszystkie formy: wykłady, ćwiczenia, konwersatoria, laboratoria i seminaria):

- ✓ *Ochrona cyberprzestrzeni w systemie obronnym.*
- ✓ *Społeczeństwo informacyjne.*
- ✓ *Krajowe i międzynarodowe standardy bezpieczeństwa w cyberprzestrzeni.*
- ✓ *Bezpieczeństwo w cyberprzestrzeni.*
- ✓ *Nauka o państwie i prawie.*
- ✓ *Logistyka międzynarodowa.*
- ✓ *Podstawy logistyki międzynarodowej.*
- ✓ *Cyberspace protection as a part of defence system* – w ramach program ERASMUS+.

Zagadnienia we wskazanych obszarach badawczych stanowiły teoretyczną podstawę do opracowania przeze mnie modułów w ramach programów kształcenia:

- ✓ *Społeczeństwo informacyjne* – program studiów magisterskich, kierunek: *Obronność państwa* [2017/2018].
- ✓ Opracowanie koncepcji zajęć z wykorzystaniem multimedialnego laboratorium – Trenażer Laserowy *Wisła* – przedmiotów: *Teoria i praktyka strzelań* – program studiów magisterskich, kierunek: *obronność państwa* [2019/2020].
- ✓ *Logistyka międzynarodowa* – program studiów magisterskich, kierunek: logistyka [2016/2017; 2017/2018].
- ✓ *Krajowe i międzynarodowe standardy ochrony cyberprzestrzeni* program studiów magisterskich [2016/2017],
- ✓ *Cyberprzestępczość* [2017],

- ✓ *Cyberprzestrzeń i jej zagrożenia* [2017],
- ✓ Opracowanie modułu zajęć z wykorzystaniem multimedialnego laboratorium – Trenażer Laserowy *Wisła* – przedmiotów: *Podstawy strzelania* – program studiów licencjackich, wdrożony w roku akademickim [2018/2019].
- ✓ *Ochrona cyberprzestrzeni w systemie obronnym państwa* – program studiów licencjackich, kierunek: o*bronność państwa* [2015/2016].
- ✓ *Bezpieczeństwo cyberprzestrzeni* - program studiów licencjackich [2015/2016].
- ✓ *Podstawy logistyki międzynarodowej* – program studiów licencjackich, kierunek: logistyka [2016/2017; 2017/2018].
- ✓ *Cyberspace protection as a part of defense system* – program ERASMUS+ [2018/2019].
- ✓ *Cyberbezpieczeństwo – podstawy* - opracowanie programu szkolenia w obszarze cyberbezpieczeństwa – uzyskanie zgody Rektora na prowadzenie szkoleń adresowanych w szczególności do pracowników administracji publicznej wszystkich szczebli. Program został opracowany zgodnie z założeniami przyjętymi w *Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej:* Rozdział 4. *Koncepcja zadań preparacyjnych* (...) - 4.3. *Publiczne i prywatne ogniwa wsparcia* – pkt. 54.

W ramach wskazanej działalności kierowałam także 43. pracami dyplomowymi (jako promotor prac dyplomowych: I. stopnia, II. stopnia oraz kierownik prac końcowych studiów podyplomowych) oraz byłam recenzentką 7 prac. Spośród tematów prac wskazać można m.in.: *Znaczenie bezpieczeństwa systemów przetwarzania informacji dla funkcjonowania przedsiębiorstw logistycznych. Cyberzagrożenia w logistycznym łańcuchu dostaw produktów cyfrowych. Analizowanie i kreowanie zachowań konsumentów z wykorzystaniem danych cyfrowych. Możliwości osiągania przewagi konkurencyjnej na rynku nierywalizacyjnych produktów cyfrowych w procesie dystrybucji. Cyfrowa inwigilacja jako narzędzie kształtowania środowiska bezpieczeństwa. Elektroniczne nieposłuszeństwo obywatelskie jako nowe zjawisko społeczne. Znaczenie ochrony danych osobowych dla kształtowania środowiska bezpieczeństwa. Możliwości wykorzystania cyfrowych mediów w walce informacyjnej. Potencjał wykorzystania Internetu Rzeczy w kształtowaniu środowiska bezpieczeństwa państwa.* Obecnie jestem promotorem i kierownikiem prac końcowych 10. dyplomantów.

W kategoriach stanowiących istotny wkład w działalność naukową należy postrzegać także moje inne osiągniecia o charakterze dydaktycznym i organizacyjnym. Wśród nich na podkreślenie zasługują podjęte przeze mnie działania w zakresie wdrożenia nowoczesnych rozwiązań wspierających procesy dydaktyczne w obszarze bezpieczeństwa i obronności państwa oraz logistyki. Wartością dodaną jest również możliwość prowadzenia za ich pomocą badań naukowych, których wyniki przekładają się na wykorzystanie w procesie dydaktycznym. Należą do nich:

- ✓ Opracowanie, przygotowanie i wdrożenie stanowiska laboratoryjnego - *Multimedialny System Treningu Strzeleckiego TL WISŁA*. Kierunek studiów: *Obronność państwa* [przedmioty: *Podstawy strzelania* oraz *Teoria i praktyka strzelań*]. System pozwala na prowadzanie ćwiczeń: statycznych, sytuacyjnych oraz interaktywnych z wykorzystaniem replik broni wyposażonych w emiter laserowy. Generowane scenariusze pozwalają rzeczywiste odwzorowanie symulowanych warunków m.in. w zakresie balistyki pocisku – wagi, średnicy, prędkości wylotowej oraz warunków atmosferycznych. Dodatkowym, nowatorskim rozwiązaniem są kamizelki taktyczne symulujące postrzał z wykorzystaniem silników wibracyjnych [2017/2018].
- ✓ Opracowanie, przygotowanie i wdrożenie: *Laboratorium badań nad cyberbezpieczeństwem* i *bezpieczeństwem informacji*. Nazwa przedmiotu wiodącego: *Ochrona cyberprzestrzeni w systemie obronnym* [2018/2019]. Laboratorium posiada separowane stanowiska komputerowe, przygotowane do badań rodzajów *złośliwego oprogramowania* w aspekcie ich wpływu na systemy operacyjne oraz stanowiska do przeprowadzenia badań behawioralnych użytkowników w ramach aktywności w sieci Internet oraz skutków poszczególnych działań wykonywanych na urządzeniach wyposażonych w komercyjne systemy operacyjne.
- ✓ Opracowanie, przygotowanie i wdrożenie: *Laboratorium ochrony infrastruktury krytycznej* [2019/2020]. Obecnie wyposażenie laboratorium – poza infrastrukturą stanowiskową - stanowi dedykowane oprogramowanie, tj.: a.) symulacyjne gry decyzyjne oparte o techniki umożliwiające odwzorowanie rzeczywistego przebiegu wybranej sytuacji krytycznej z uwzględnieniem niezbędnych ról, decyzji, zjawisk i infrastruktury, co pozwala na efektywne doskonalenie umiejętności m.in.: selekcji i analizy informacji, poprawnej oceny sytuacji, podejmowania trudnych decyzji, wykorzystywaniu dostępnych sił i środków w optymalny sposób, postępowania w granicach uprawnień wyznaczonych pełnioną funkcją, komunikowania się i współpracy w zespole; b.) oprogramowanie do zarządzania ryzykiem w znormalizowanych systemach zarządzania, m.in. wsparcie

zarządzania ryzykiem strategicznym i operacyjnym, w tym w ramach standardów: ISO 31000 i COSO I; zarządzanie ryzykiem w ramach kontroli zarządczej, czy identyfikacji i oceny zagrożeń dla ciągłości procesów.

Ponadto:

- ✓ Wdrożenie oprogramowania obejmującego zestaw zaawansowanych procedur analitycznych [2016/2017].
- ✓ Wdrożenie oprogramowania dedykowanego analizie ryzyka i analizie zagrożeń ochrony informacji niejawnych, opartego o metodykę zgodną z zaleceniami Departamentu Bezpieczeństwa Teleinformatycznego ABW oraz z Rozporządzeniem Prezesa Rady Ministrów *w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego* [2017/2018].
- ✓ Wdrożenie oprogramowania dedykowanego analizie ryzyka i analizie zagrożeń dla bezpieczeństwa danych osobowych [2018/2019].
- ✓ Wdrożenie oprogramowania w obszarze logistyki międzynarodowej wraz z możliwością certyfikacji - wersja edukacyjna profesjonalnej aplikacji wykorzystywanej w branży TSL (moduł pomaga kształcić praktyczne umiejętności studentów w zakresie szeroko rozumianej organizacji transportu) [2016/2017].
- ✓ Wdrożenie oprogramowania w obszarze logistyki - wersja edukacyjna specjalistycznego oprogramowania, pozwalającego na zdobycie praktycznych umiejętności w szerokim zakresie m.in.: planowania struktury i sieci, optymalizacji dystrybucji i automatyzacji pracy, podnoszenie wydajności procesów (w tym analiza jakości KPI) oraz podejmowania decyzji [2017/2018].

Dodatkowo w ramach działalności dydaktycznej i popularyzatorskiej:

- ✓ zorganizowałam zajęcia studyjne dla studentów na kierunku: *Obronność państwa* - w Centralnym Ośrodku Analizy Skażeń [2016/2017],
- ✓ przeprowadziłam szkolenie pt.: *Cyberbezpieczństwo – podstawy* - na Uniwersytecie Szczecińskim [2017],
- ✓ przeprowadziłam wykłady zewnętrzne i otwarte w obszarze *cyberbezpieczeństwa*:

- w Akademii Obrony Narodowej [*Zarządzanie systemami bezpieczeństwa wewnętrznego*] [2014/2015],
- na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie: *Podstawy prawne cyberbezpieczeństwa* [2016],
- w ramach sympozjum zorganizowanego przez Centrum Certyfikacji i Jakości [2019],
- w ramach Dnia Otwartego WAT [2017,2018 i 2019],

- dla pracowników Wydziału Logistyki [2019] oraz przeprowadziłam zajęcia szkoleniowe: *Cyberbezpieczeństwo* - w ramach programu Ministerstwa Obrony Narodowej *Legia Akademicka* realizowanego w Wojskowej Akademii Technicznej w Warszawie [2019].

W kategoriach stanowiących istotny wkład w działalność naukową należy postrzegać także inne moje osiągniecia o charakterze organizacyjnym. Wśród nich na podkreślenie zasługują działania w zakresie propagowania wiedzy o bezpieczeństwie - w ramach udziału w komitetach redakcyjnych i radach naukowych czasopism, wśród których należy wymienić m.in.:

- ✓ *Przegląd nauk o obronności/Defence science review* – członek redakcji, Wyd. WAT, Warszawa 2017, ISSN 2450-6869.
- ✓ *Zeszyty Studenckie PRO PUBLICO BONO* Nr 1(1) 2017, Szkoła Główna Służby Pożarniczej, Wydział Inżynierii Bezpieczeństwa Cywilnego - Członek kolegium redakcyjnego - redaktor tematyczny działu: *Cyberbezpieczeństwo*. Warszawa 2017 ISSN 2544-2481.
- ✓ *Logistyka i obronność w świetle nowych technologii – KNS WAT,* Red. Wyd. WAT, Warszawa 2017 – członek komitetu redakcyjnego.

Ponadto jestem członkiem międzynarodowych i krajowych organizacji: *Information Systems Security Association* – Międzynarodowe Stowarzyszenie Bezpieczeństwa Systemów Informacyjnych [2018 – obecnie] oraz Fundacji „Bezpieczne dzieci" [2015-obecnie].

Powyższa aktywność, w szczególności propagowanie dorobku nauk o bezpieczeństwie, znalazło uznanie przez przyznane wyróżnienia od:

- ✓ Dyrektora Wydziału Bezpieczeństwa i Zarządzania Kryzysowego - Dyplom uznania *za popularyzowanie z zakresu bezpieczeństwa na łamach Informatora obrony cywilnej i zarządzania kryzysowego służącej zwiększeniu efektywności działania terenowej administracji rządowej* (2015).
- ✓ Komendanta Szkoły Aspirantów Państwowej Straży Pożarnej w Krakowie - *za naukowe wsparcie inicjatyw edukacyjnych na rzecz bezpieczeństwa powszechnego* (2016).

Ponadto otrzymałam Brązowy medal *Siły Zbrojne w Służbie Ojczyzny* (2018) oraz wielokrotnie otrzymywałam wyróżnienia i nagrody uznaniowe od przełożonych. Wartym odnotowania jest również posiadanie międzynarodowego Certyfikatu PRINCE2® Foundation – poświadczającego znajomość opartego na procesach zarządzania projektami.

Reasumując prezentację mojego dotychczasowego dorobku, działalności oraz osiągnięć pragnę podkreślić, że mieszczą się one w obszarze nauk społecznych i są z nią ściśle związane – przede wszystkim w sferze nauk o bezpieczeństwie. Moja działalność naukowa odnosi się przede wszystkim do fenomenu deterministycznej złożoności cyberprzestrzeni w kontekście bezpieczeństwa oraz prawnych aspektów i podstaw bezpieczeństwa w szerokim znaczeniu.

Warszawa 11 kwietnia 2019 r. Monika Antkowska

(miejscowość) *(data)* *(podpis habilitanta)*