Załącznik nr 3
do wniosku o wszczęcie postępowania habilitacyjnego

AUTOREFERAT
PRZEDSTAWIAJĄCY OPIS OSIĄGNIĘĆ NAUKOWYCH, DYDAKTYCZNYCH I ORGANIZACYJNYCH

dr Grzegorz Strupczewski

Spis treści

1. Posiadane dyplomy i stopnie naukowe
z podaniem nazwy, miejsca i roku ich uzyskania oraz tytułu rozprawy doktorskiej

2009 **Dyplom doktora nauk ekonomicznych w zakresie ekonomii**
Uniwersytet Ekonomiczny w Krakowie, Wydział Finansów (data nadania: 16 marca 2009 r.)

Tytuł rozprawy doktorskiej: *„Finansowe skutki ryzyka powodzi w Polsce"*
Promotor: Prof. zw. dr hab. Wanda Sułkowska

Rozprawa została nagrodzona w konkursie Rzecznika Ubezpieczonych na najlepszą pracę doktorską z dziedziny ubezpieczeń w 2010 r. (III miejsce). Otrzymała także nagrodę Izby Gospodarczej Ubezpieczeń i Obsługi Ryzyka za wybitne osiągnięcie na rzecz rozwoju ubezpieczeń w kategorii Debiut ubezpieczeniowy w 2010 r.

2003 **Dyplom ukończenia studium pedagogicznego dla nauczycieli akademickich**
Akademia Ekonomiczna w Krakowie, Studium Doskonalenia Dydaktyki Akademickiej
(d. Studium Pedagogiczne)

2002 **Dyplom magistra ekonomii**
Akademia Ekonomiczna w Krakowie, Wydział Ekonomii

Tytuł pracy magisterskiej: *„Analiza wskaźnikowa jako narzędzie badania kondycji finansowej zakładu ubezpieczeń"*
Promotor: dr Grażyna Sordyl

2. Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych

01.10.2009 r. – nadal
Adiunkt w Katedrze Zarządzania Ryzykiem i Ubezpieczeń
Kolegium Ekonomii, Finansów i Prawa, Instytut Finansów (d. Wydział Finansów)
Uniwersytet Ekonomiczny w Krakowie

01.10.2002 r. – 30.09.2009 r.
Asystent w Katedrze Ubezpieczeń
Wydział Finansów
Akademia Ekonomiczna w Krakowie

3. Omówienie osiągnięcia, o którym mowa w art. 219 ust. 1 pkt 2 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r. poz. 1668 ze zm.)

3.1. Tytuł osiągnięcia

Dziełem stanowiącym osiągnięcie jest monografia naukowa mojego autorstwa pt.:

„Rola państwa w rozwoju rynku ubezpieczeń cybernetycznych"

wydana w 2020 r. przez Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie
ISBN 978-83-7252-820-9, ss. 279

Recenzenci:

dr hab. Teresa H. Bednarczyk, prof. uczelni
Katedra Ubezpieczeń i Inwestycji
Wydział Ekonomiczny
Uniwersytet Marii Curie-Skłodowskiej w Lublinie

dr hab. Marietta Janowicz-Lomott, prof. uczelni
Instytut Ryzyka i Rynków Finansowych
Kolegium Zarządzania i Finansów
Szkoła Główna Handlowa w Warszawie

3.2. Uzasadnienie wyboru podjętego problemu

Ryzyko cybernetyczne (inaczej cyberryzyko) należy do najważniejszych wyzwań współczesnego świata, co znajduje potwierdzenie w wielu raportach gospodarczych i ubezpieczeniowych (m.in. *The Global Risks Report*... 2019; *Allianz Risk Barometer*... 2019). Czym zatem jest ryzyko cybernetyczne? Od początku XXI w. powstało wiele definicji tego pojęcia. Wywodzą się one z różnych dyscyplin nauki (informatyka, ekonomia, prawo, zarządzanie), więc w swej treści akcentują odmienne aspekty tego terminu, przez co są wycinkowe, brakuje im spójności i interdyscyplinarności. Ponadto w miarę upływu czasu ryzyko to ewoluuje, przejawiając się w nowych, wcześniej nieznanych formach, co rodzi potrzebę okresowej aktualizacji stosowanej terminologii. Prowadząc wszechstronne badania literaturowe na użytek niniejszej monografii, zauważyłem brak powszechnie uznanej, naukowej definicji ryzyka cybernetycznego, która stanowiłaby wspólny punkt odniesienia przy prowadzeniu szczegółowych badań. W wielu publikacjach naukowych wątek definicji cyberryzyka bywał pomijany lub przywoływano terminy występujące w zastosowaniach

praktycznych, którym brakuje jednak cech naukowości. Aby wypełnić tę lukę badawczą, zaproponowałem własne, ujednolicone i kompleksowe rozumienie pojęcia ryzyka cybernetycznego.

Samo uporządkowanie definicji ryzyka cybernetycznego nie jest jednak wystarczające. Wielość istniejących perspektyw badawczych w definiowaniu innych podstawowych pojęć z zakresu cyberbezpieczeństwa i technologii informacyjnych sprawia wrażenie chaosu. Gwałtowny wzrost liczby nowych pojęć z przedrostkiem „cyber" przybiera niespotykane wcześniej rozmiary. Chaos terminologiczny skłania badaczy do poszukiwania sposobów uporządkowania tej niezwykle dynamicznej materii, co wymaga bardziej kompleksowego spojrzenia. Moim zamiarem było włączenie się w ten nurt badawczy i uzupełnienie go o własną propozycję ontologicznego metamodelu definicji ryzyka cybernetycznego. Zadaniem tego metamodelu jest uszczegółowienie definicji cyberryzyka, ukazanie powiązań funkcjonalnych z innymi pojęciami, różnych współzależności, uwarunkowań i czynników, które tworzą szeroko pojęty koncept ryzyka cybernetycznego i determinują jego charakter.

Dynamiczny rozwój technologii informacyjnych i ich powszechne wykorzystanie niemal we wszystkich sferach życia prywatnego, gospodarczego i społecznego implikuje powstanie nowych czynników ryzyka lub nadanie całkowicie nowego sensu czynnikom istniejącym już wcześniej. Potrzeba zapewnienia cyberbezpieczeństwa stała się naturalną odpowiedzią na te wyzwania, jednak w celu skutecznej jej realizacji niezbędne jest odpowiednie instrumentarium. Główny nacisk w polityce budowania cyberbezpieczeństwa organizacji kładziony jest zwykle na rozwiązania techniczne i nietechniczne (m.in. regulacje, procedury, szkolenia), za które w większości odpowiadają działy IT. Należy jednak mieć świadomość, że podjęte działania zabezpieczające nie gwarantują nigdy pełnej skuteczności ze względu na obiektywne ograniczenia techniczne, organizacyjne i finansowe. Sytuacja ta stwarza przestrzeń do stosowania ubezpieczeń cybernetycznych.

Ubezpieczenia cybernetyczne (w skrócie cyberubezpieczenia) powstały pod koniec XX w. w odpowiedzi na wzrost świadomości zagrożeń cybernetycznych i uchwalenie w USA przepisów o ochronie danych osobowych przewidujących surowe sankcje za dopuszczenie przez administratora do ich wycieku. Współczesne cyberubezpieczenia to pakiet wyspecjalizowanych ubezpieczeń majątkowych, łączących elementy ubezpieczenia własnych szkód spowodowanych ryzykiem cybernetycznym (w tym przerwa w działalności wywołana incydentem cybernetycznym), ubezpieczenia odpowiedzialności cywilnej z tytułu szkód w mieniu lub strat finansowych wyrządzonych osobom trzecim (np. wskutek naruszenia poufności danych przetwarzanych cyfrowo), jak również ubezpieczenia *assistance* i ochrony

prawnej w postaci pokrycia różnych kategorii kosztów związanych z incydentem cybernetycznym. Ubezpieczenia cybernetyczne, podobnie jak cała problematyka cyberbezpieczeństwa, wzbudzają coraz większe zainteresowanie badaczy, co przekłada się na wzrost liczby publikacji naukowych, głównie zagranicznych. W Polsce wciąż nie ma zwartego opracowania monograficznego na temat ryzyka cybernetycznego i ubezpieczeń cybernetycznych. Stanowi to wartą zagospodarowania lukę i uzasadnia wybór obszaru badawczego w niniejszej pracy.

Coraz szybszy rozwój ubezpieczeń cybernetycznych na całym świecie uwydatnił – paradoksalnie – czynniki hamujące, których przezwyciężenie stanowi poważne wyzwanie dla branży ubezpieczeń i innych interesariuszy. Sprawne funkcjonowanie rynku ubezpieczeń cybernetycznych jest bowiem ściśle powiązane z polityką cyberbezpieczeństwa, a ta znajduje się w sferze istotnych interesów większości organizacji (poziom mikro), jak również władz państwowych i organizacji międzynarodowych (poziom makro). Warto zatem poszukać odpowiedzi na pytanie, na czym te bariery polegają. Zauważyłem, że rynek ubezpieczeń cybernetycznych nie nadąża za rozwojem technologii informacyjnych oraz dynamiką zmian intensywności i form ryzyka cybernetycznego. Cyberryzyko jest tak bardzo odmienne od konwencjonalnych rodzajów ryzyka, dla których tworzono produkty ubezpieczeniowe na przestrzeni ostatnich dekad, że towarzystwa ubezpieczeń muszą na nowo wypracować modele aktuarialne, zasady underwritingu, filozofię konstrukcji produktów ubezpieczeniowych czy metody likwidacji szkód.

Ponadto niedostatek danych o cyberryzyku, wysoka zmienność w obrębie tego ryzyka sprawiająca, że modele aktuarialne budowane z wykorzystaniem danych historycznych przestają mieć realną wartość prognostyczną, brak sprawdzonych metod pomiaru stanu cyberbezpieczeństwa w organizacji, wymagany wysoki stopień wiedzy specjalistycznej z zakresu IT podczas zawierania umowy ubezpieczenia i likwidacji szkody, trudności w identyfikacji i wycenie szkód cybernetycznych (ile kosztuje wyciek jednego rekordu danych osobowych?) – to tylko wybrane przesłanki sprawiające, że skala problemu asymetrii informacji jest większa niż w innych liniach ubezpieczeń. Kolejny zidentyfikowany przeze mnie problem to współzależność ryzyka cybernetycznego. Jej źródeł można się doszukiwać w takich czynnikach, jak: monokultura technologii IT, powszechne usieciowienie (coraz więcej urządzeń codziennego użytku i maszyn przemysłowych jest podłączone do sieci), architektura globalnej sieci internet ułatwiająca propagację cyberzagrożeń, skala uzależnienia gospodarki, społeczeństw i organizmów państwowych od technologii cyfrowych, wzrost znaczenia aktywów niematerialnych w majątku przedsiębiorstw. Współzależność ryzyka oznacza dla

towarzystw ubezpieczeń niebezpieczeństwo kumulacji szkód spowodowanych jedną przyczyną oraz niższą skuteczność dywersyfikacji ryzyka w portfelu ubezpieczeń.

Duże obawy ubezpieczycieli i reasekuratorów wzbudza ogromny potencjał zagrożeń cybernetycznych, które są zdolne do spowodowania szkód o rozmiarach katastrofy. Potencjalnie katastroficzne rozmiary ryzyka cybernetycznego mogą wynikać zarówno z kumulacji wielu mniejszych szkód spowodowanych tą samą przyczyną, jak również z zakłócenia w funkcjonowaniu jednej z usług krytycznych dla gospodarki (np. sieć energetyczna, telekomunikacyjna, transportowa, system płatniczy).

Przedstawione wyżej okoliczności, skupione wokół zagadnień asymetrii informacji i kumulacji ryzyka, budzą wątpliwości co do tego, czy ryzyko cybernetyczne spełnia znane w teorii ubezpieczeń warunki ubezpieczalności ryzyka. Obserwując, jak obecnie wygląda oferta ubezpieczeń cybernetycznych, doszedłem do wniosku, że ubezpieczyciele stosują strategię ekspansji rynkowej przy zachowaniu daleko idącej ostrożności w przyjmowaniu ryzyka. Przejawia się to przede wszystkim w oferowaniu niskich limitów odpowiedzialności w powiązaniu z relatywnie wysokimi franszyzami redukcyjnymi (lub udziałami własnymi). M. Eling i H. Wirfs trafnie zdiagnozowali tę sytuację pisząc, że rynek ubezpiecza wyłącznie „ryzyko dnia codziennego" (*everyday cyber risk*) (Eling i Wirfs 2019). Tu nasuwa się pytanie, czy branża ubezpieczeniowa jest gotowa przyjąć większą część ryzyka zgłaszanego do ubezpieczenia. Jeżeli nie, to podnoszone przez teoretyków i praktyków obawy o dalszy rozwój rynku ubezpieczeń cybernetycznych są w pełni uzasadnione. Biorąc pod uwagę znaczenie ubezpieczeń cybernetycznych w budowie ekosystemu cyberbezpieczeństwa, warto zastanowić się nad potencjalną rolą państwa we wsparciu funkcjonowania tego rynku, żeby mógł osiągnąć potencjał adekwatny do potrzeb nowoczesnej gospodarki cyfrowej. Jest to tym bardziej uzasadnione, że w razie katastrofy cybernetycznej, takiej jak na przykład paraliż sieci energetycznej lub telekomunikacyjnej kraju w wyniku ataku cyberprzestępców na elektroniczne systemy sterowania, większość negatywnych konsekwencji takiego incydentu musiałoby sfinansować państwo. Obciążenie finansowe budżetu państwa mogłoby być niższe, gdyby część kosztów odbudowy i naprawy szkód przejęła branża ubezpieczeń, wypłacając odszkodowania ubezpieczeniowe tym poszkodowanym, którzy posiadali ochronę ubezpieczeniową przed tego typu zdarzeniem.

Zaangażowanie państwa mogłoby polegać na aktywnej współpracy z sektorem ubezpieczeń w ramach partnerstwa publiczno-prywatnego lub na stworzeniu warunków inicjujących transfer ryzyka cybernetycznego na rynek kapitałowy, np. w drodze emisji obligacji katastroficznych. Materialnym wyrazem takiego partnerstwa są narodowe programy

ubezpieczeń różnych rodzajów ryzyka, które w myśl realizowanej polityki publicznej wymagają szczególnego podejścia. Są to najczęściej różnego rodzaju ryzyka naturalne, terroryzm, ryzyko katastrofy nuklearnej czy ryzyko ekologiczne. Do tej grupy należy również zaliczyć ryzyko cybernetyczne. Jestem zdania, iż w wielu aspektach ma ono cechy podobne do ryzyka terrorystycznego, w tym – co najistotniejsze – zasięg oddziaływania i potencjał zdolny do wyrządzenia szkód katastroficznych.

Interwencja państwa na rynku ubezpieczeń cybernetycznych, moim zdaniem, mogłaby ustabilizować warunki funkcjonowania ubezpieczycieli i reasekuratorów oraz wyeliminować niedoskonałości mechanizmu rynkowego. Ponadto aktywna postawa państwa w tym obszarze podniosłaby rangę kwestii cyberbezpieczeństwa, uświadomiła skalę zagrożenia i wzbudziła zainteresowanie zakupem ubezpieczenia cybernetycznego.

Uwzględniając przedstawione argumenty, należy odpowiedzieć na podstawowe pytania badawcze:

1. Czy w obliczu eskalacji ryzyka cybernetycznego istnieją podstawy do interwencji państwa na rynku ubezpieczeń cybernetycznych?
2. Czy takie rozwiązania, jak stworzenie poolu ubezpieczeń lub reasekuracji ryzyka cybernetycznego, zaangażowanie państwa jako reasekuratora ostatniej instancji, emisja obligacji katastroficznych na ryzyko cybernetyczne, mogą wpłynąć pozytywnie na wzrost rynku cyberubezpieczeń?

Brak odpowiedzi na te pytania w formie kompleksowego opracowania naukowego stanowi kolejną lukę badawczą, której wypełnienie jest zadaniem mojej monografii.

3.3. Cele, hipotezy i metody badawcze

Z zamiarem wypełnienia wskazanej luki poznawczej podjąłem badania naukowe, których wyniki prezentuje monografia stanowiąca moje główne osiągnięcie naukowe. Za główny cel badań przyjąłem zbadanie zasadności bezpośredniego zaangażowania państwa w rynek ubezpieczeń cybernetycznych podejmowanego w celu ograniczenia negatywnego wpływu eskalacji ryzyka cybernetycznego na ten rynek. Cel główny zdekomponowałem na siedem celów szczegółowych:

1. Uporządkowanie zróżnicowanych podejść definicyjnych odnoszących się do ryzyka cybernetycznego i zaproponowanie własnej definicji tego pojęcia.
2. Diagnoza stanu rynku ubezpieczeń cybernetycznych.
3. Określenie barier rozwoju rynku ubezpieczeń cybernetycznych.

4. Określenie form bezpośredniego zaangażowania państwa w rynek ubezpieczeń komercyjnych i przesłanek je uzasadniających.
5. Zbadanie negatywnego wpływu eskalacji ryzyka cybernetycznego na rynek ubezpieczeń cybernetycznych.
6. Diagnoza istnienia luki pokrycia szkód cybernetycznych jako przesłanki uzasadniającej interwencję państwa na rynku ubezpieczeń cybernetycznych.
7. Ocena możliwości zastosowania obligacji katastroficznych w sekurytyzacji ryzyka cybernetycznego.

Powyższe cele pozwoliły mi na sformułowanie hipotez badawczych. Główna hipoteza badawcza pracy brzmi: w warunkach eskalacji ryzyka cybernetycznego występują uzasadnione przesłanki dla bezpośredniego zaangażowania się państwa na rynku ubezpieczeń cybernetycznych, aby stymulować jego zrównoważony rozwój i osiągnąć potencjał adekwatny do współczesnych potrzeb. Postawiłem również osiem hipotez szczegółowych:

H1. Pomimo mnogości podejść do definiowania ryzyka cybernetycznego nie została opracowana spójna i kompleksowa definicja tego pojęcia w szczególności z perspektywy naukowej.

H2. Rynek ubezpieczeń cybernetycznych nie nadąża za rozwojem technologii informacyjnych i ryzykiem, jakie ten rozwój niesie, a dotychczasowe modele aktuarialne, zasady underwritingu i konstrukcji produktów nie zapewniają efektywnego i zgodnego z oczekiwaniami klientów pokrycia ubezpieczeniowego.

H3. Rozwój rynku ubezpieczeń cybernetycznych jest hamowany przez realnie istniejące bariery o zróżnicowanym charakterze. Bariery te można sprowadzić do dwóch pierwotnych (fundamentalnych) problemów węzłowych: asymetrii informacji i kumulacji ryzyka.

H4. Eskalacja ryzyka cybernetycznego będzie miała negatywny wpływ na rynek cyberubezpieczeń w postaci obniżenia nasycenia rynku lub jego całkowitego zaniku.

H5. Istnieje znaczna luka pokrycia szkód cybernetycznych, a eskalacja cyberryzyka doprowadzi do jej dalszego zwiększenia.

H6. W warunkach współzależności ryzyka cybernetycznego stworzenie poolu ubezpieczeń cybernetycznych nie spowoduje poprawy dostępności ubezpieczeń cybernetycznych.

H7. Utworzenie poolu reasekuracyjnego z udziałem państwa jako reasekuratora ostatniej instancji jest najbardziej odpowiednim sposobem zahamowania regresu rynku ubezpieczeń cybernetycznych oraz stymulacji jego wzrostu w przyszłości.

H8. W warunkach eskalacji ryzyka cybernetycznego istnieje możliwość zastosowania obligacji katastroficznych do sfinansowania części negatywnych skutków tego ryzyka w ramach proponowanego poolu reasekuracji.

W celu weryfikacji postawionych hipotez przeprowadziłem analizę teoretyczną na podstawie dostępnej literatury, w szczególności dotyczącej teorii ryzyka cybernetycznego i ubezpieczeń cybernetycznych. Wykonałem także ilościowe badania empiryczne, które polegały na analizie symulacyjnej zachowania rynku ubezpieczeń cybernetycznych przy zmiennych warunkach otoczenia odnoszących się do wzrostu poziomu ryzyka cybernetycznego (eskalacja ryzyka cybernetycznego). Wzrost ten wyraziłem w trzech różnych aspektach, tj. jako wzrost prawdopodobieństwa realizacji ryzyka, wzrost wartości potencjalnych szkód oraz wzrost współzależności występowania ryzyka (modelowany z zastosowaniem kopuły *t*-Studenta). Symulacje przyszłych stanów rynku cyberubezpieczeń zostały wygenerowane przez samodzielnie zbudowany matematyczny model rynku cyberubezpieczeń oparty na dorobku teorii ryzyka i teorii ubezpieczeń, który został tak skalibrowany, by odwzorowywać aktualne realia rynkowe.

W monografii zastosowałem metody badawcze, które można uznać za typowe dla prac naukowych osadzonych w dyscyplinie ekonomia i finanse, takie jak:

- krytyczna analiza i synteza piśmiennictwa naukowego w zakresie teorii ryzyka ubezpieczeniowego, ryzyka cybernetycznego, ubezpieczeń, a w szczególności ubezpieczeń cybernetycznych. W analizie dorobku literatury przedmiotu skoncentrowałem się wyłącznie na zagadnieniach istotnych dla osiągnięcia założonych celów badawczych i weryfikacji postawionych hipotez,
- metoda obserwacyjna dotycząca funkcjonowania rynku ubezpieczeń cybernetycznych,
- analiza porównawcza,
- rozumowanie indukcyjne i dedukcyjne,
- analiza symulacyjna z elementami analizy scenariuszy.

Wyniki badań zawarte w rozdziale piątym uzyskałem metodą symulacji rynku ubezpieczeń cybernetycznych. Poszczególne warianty symulacji zostały wygenerowane na podstawie autorskiego modelu matematycznego odzwierciedlającego realia współczesnego rynku cyberubezpieczeń oraz rozbudowanej bazy danych zawierających przypadki realizacji

ryzyka cybernetycznego. Dzięki zastosowaniu modelu i różnych danych wejściowych odzwierciedlających zmiany poziomu ryzyka cybernetycznego możliwa stała się weryfikacja postawionych hipotez badawczych nie tylko w scenariuszu bazowym, odpowiadającym aktualnej ekspozycji na cyberryzyko, ale również w wielu innych scenariuszach symulujących różne kierunki zmian ryzyka cybernetycznego w przyszłości. Jako źródło wspomnianych danych wejściowych wykorzystałem bazę danych *Advisen Cyber Loss Data* (ACLD). ACLD jest relacyjną bazą danych o szkodach spowodowanych incydentami cybernetycznymi na całym świecie w latach 2000–2018, liczącą 82 300 przypadków. Szkody te są wyrażone w postaci pieniężnej i niepieniężnej. Do badań wybrałem tylko te, którym przypisano straty finansowe określone w jednostkach pieniężnych. Ostateczna próba badawcza liczyła zatem 5101 obserwacji reprezentujących straty wywołane realizacją ryzyka cybernetycznego o wartościach w zakresie od 1 USD do 150 mln USD. Kalibracja parametrów modelu w taki sposób, by odzwierciedlały aktualne realia rynku ubezpieczeń cybernetycznych i jego otoczenia, jak również zachowanie równowagi między precyzją modelu a jego relatywną prostotą pozwalającą na efektywne przeprowadzenie licznych symulacji – moim zdaniem – stanowi wartość dodaną prezentowanych wyników badań w porównaniu z dotychczasowymi publikacjami.

3.4. Struktura monografii

Struktura książki nawiązuje do teoretyczno-empirycznego charakteru prowadzonych badań. Książka ma pięć rozdziałów. Poszczególne rozdziały korespondują z celami i hipotezami badawczymi. Cztery pierwsze rozdziały monografii tworzą warstwę konceptualną badań, pokazując wyniki studiów teoriopoznawczych, które kilkakrotnie przekształcały się w studia teoriotwórcze. Wynikało to z potrzeby uporządkowania, uzupełnienia, bądź dookreślenia zastanego stanu wiedzy. Piąty rozdział monografii wprowadza empiryczną warstwę badań. Zaprezentowałem tam wyniki badań własnych odnoszących się do rynku ubezpieczeń cybernetycznych, luki pokrycia ubezpieczeniowego i różnych koncepcji finansowania negatywnych skutków ryzyka cybernetycznego.

Rozdział pierwszy zatytułowany *„Ryzyko cybernetyczne i jego systematyka"* stanowi wprowadzenie do problematyki ryzyka cybernetycznego. Na początek wyjaśniłem podstawowe pojęcia dla prowadzonych w pracy rozważań, takie jak cyberbezpieczeństwo, incydent cybernetyczny, cyberatak, zagrożenie cyberbezpieczeństwa, cyberprzestępczość. Szczególną uwagę skupiłem na wyjaśnieniu genezy i znaczenia terminu cyberprzestrzeń, pokazując go z różnych perspektyw poznawczych. Wskazałem też charakterystyczne cechy

zagrożeń pochodzących z cyberprzestrzeni, wśród których za najważniejszą uznałem asymetrię potencjałów atakującego i ofiary. Dalszą część rozdziału poświęciłem analizie porównawczej definicji ryzyka cybernetycznego, stosując autorskie podejście do ich klasyfikacji. Jako kryterium podziału przyjąłem perspektywę funkcjonalną, rozumianą jako operacjonalizacja badanej definicji poprzez wyodrębnienie w jej treści elementów składowych istotnych z punktu widzenia podjętego zamierzenia badawczego. Elementami tymi były trzy obszary problemowe, określane tu jako wymiary, odnoszące się odpowiednio do źródeł cyberryzyka, obiektów materialnych i niematerialnych, na których dochodzi do wystąpienia cyberryzyka oraz jego negatywnych konsekwencji. W analizowanych definicjach występowały jeden, dwa lub trzy wymiary. Na tej podstawie zaliczyłem rozpatrywane definicje do kategorii definicji jednowymiarowych, dwuwymiarowych lub definicji kompleksowych (trójwymiarowych). Definicje przyporządkowane do powyższych kategorii różnią się między sobą zawartością informacyjną. Na podstawie wniosków z przeprowadzonej analizy porównawczej zaproponowałem własną definicję ryzyka cybernetycznego. Rozwinięciem tej definicji jest autorska propozycja ontologicznego metamodelu definicji ryzyka cybernetycznego. Metamodel pozwala spojrzeć na ryzyko cybernetyczne w sposób bardziej kompleksowy, z uwzględnieniem innych związanych z nim pojęć i wzajemnych relacji przyczynowo - skutkowych. Następnie dokonałem przeglądu najważniejszych klasyfikacji ryzyka cybernetycznego. Ze względu na ich wielość przeprowadziłem wstępny podział analizowanych taksonomii na dwie grupy: taksonomie ogólne i taksonomie szczegółowe. Te pierwsze odnoszą się do generalnych cech wyróżniających rodzaje cyberryzyka. Taksonomie szczegółowe z kolei porządkują cyberryzyko według wyraźnie określonych, szczegółowych kryteriów, takich jak: źródło zagrożenia, motywy sprawcy, metoda cyberataku czy rodzaj szkód spowodowanych cyberincydentem. Sięgając do systematyki ryzyka znanej z teorii ubezpieczeń, podjąłem refleksję nad umiejscowieniem w niej ryzyka cybernetycznego. Ustaliłem, że cyberryzyko jest ryzykiem dynamicznym, ryzykiem czystym i ryzykiem majątkowym. Nie jest jednak możliwe jednoznaczne określenie cyberryzyka jako ryzyka finansowego bądź niefinansowego ze względu na zróżnicowanie skutków incydentu cybernetycznego. Analogiczna dwuznaczność klasyfikacyjna wystąpiła przy próbie rozróżnienia ryzyka partykularnego i ryzyka fundamentalnego.

W drugim rozdziale monografii zatytułowanym *„Rynek ubezpieczeń cybernetycznych i ocena jego funkcjonowania"* zawarłem charakterystykę i diagnozę rynku ubezpieczeń cybernetycznych. Na początek omówiłem genezę i główne determinanty ewolucji ubezpieczeń cybernetycznych. Wskazałem dostępne formy pokrycia tego ryzyka na rynku ubezpieczeń, zwracając uwagę na potencjalne luki pokrycia oraz nakładanie się zakresów ochrony różnych

produktów ubezpieczeniowych. Zdefiniowałem, czym jest ubezpieczenie ryzyka cybernetycznego i określiłem jego miejsce w systematyce ubezpieczeń gospodarczych zapisanej w załączniku do ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej. W dalszej części rozdziału scharakteryzowałem rynek ubezpieczeń cybernetycznych, poświęcając najwięcej uwagi USA, jako największemu rynkowi cyberubezpieczeń na świecie.

Na podstawie analizy porównawczej ogólnych warunków ubezpieczeń cybernetycznych dostępnych na polskim rynku i syntezy informacji w nich zawartych zdefiniowałem przedmiot i zakres ochrony ubezpieczeniowej standardowo oferowanej przez ubezpieczycieli. W analogiczny sposób określiłem rozumienie pojęcia incydent cybernetyczny, podstawowego terminu z punktu widzenia definicji wypadku ubezpieczeniowego. Jednocześnie wskazałem na problem braku jednolitości terminologii stosowanej przez ubezpieczycieli w ogólnych warunkach ubezpieczeń cybernetycznych. W kolejnej części rozdziału omówiłem specyfikę oceny ryzyka (*underwritingu*) w ubezpieczeniach cybernetycznych. Wskazałem na szczególną rolę oceny stanu cyberbezpieczeństwa klienta na etapie przedkontraktowym, co implikuje dużą złożoność ubezpieczeniowych kwestionariuszy oceny ryzyka cybernetycznego. Zdiagnozowałem czynniki hamujące rozwój *underwritingu* w dziedzinie ryzyka cybernetycznego. Przechodząc do kwestii składki ubezpieczeniowej, przedstawiłem różne podejścia do *pricingu* i budowy taryf w ubezpieczeniach cybernetycznych (na przykładzie rynku amerykańskiego). Wskazałem najważniejsze trudności w taryfikacji ryzyka cybernetycznego. Ponadto zwróciłem uwagę na relatywnie wysoki koszt ubezpieczenia cybernetycznego w porównaniu z innymi ubezpieczeniami dla klientów korporacyjnych, co można wyjaśnić m.in. niedostateczną znajomością cyberryzyka i ograniczonymi możliwościami indywidualizacji składki. Dalej przedstawiłem aktualny stan rozwoju rynku reasekuracji ryzyka cybernetycznego, jego najpoważniejsze problemy i perspektywy wzrostu. Opisałem kontrakty reasekuracyjne najczęściej wykorzystywane w reasekuracji cyberryzyka. Wspomniałem ponadto o pierwszych próbach zastosowania alternatywnego transferu ryzyka (*Alternative Risk Transfer* – ART) w postaci emisji ubezpieczeniowych instrumentów pochodnych (*Insurance-Linked Securities* – ILS) na ryzyko cybernetyczne i o potencjalnych przeszkodach do pokonania w tym segmencie rynku.

Następnie zbudowałem listę korzyści wynikających z posiadania ubezpieczenia cybernetycznego i – patrząc szerzej – sprawnie funkcjonującego rynku ubezpieczeń oferującego te produkty. Korzyści te wskazałem zarówno na poziomie indywidualnym (poziom mikro), jak i w skali całej gospodarki (poziom makro). Podkreśliłem, że ubezpieczenia

cybernetyczne, zapewniając ubezpieczonym dodatkowe korzyści na etapie przedszkodowym i poszkodowym, wykraczają poza klasyczny paradygmat funkcji pełnionych przez mechanizm ubezpieczeniowy na rzecz jednostki i gospodarki.

W trzecim rozdziale monografii zatytułowanym *„Bariery rozwoju rynku ubezpieczeń ryzyka cybernetycznego"* przeprowadziłem pogłębioną analizę barier rozwoju rynku ubezpieczeń cybernetycznych. Swoją diagnozę podzieliłem na trzy zasadnicze obszary problemowe, takie jak: asymetria informacji, kumulacja ryzyka i ubezpieczalność ryzyka. W analizie zastosowałem autorską metodologię badań, w której wyróżniłem pięć kroków badawczych. Są to: identyfikacja źródeł problemu, określenie problemu, wskazanie materialnych form manifestacji problemu, określenie konsekwencji istnienia problemu i propozycja jego rozwiązania. Zastosowanie takiej metodologii pozwoliło mi uporządkować rozproszone i zróżnicowane informacje w spójną i logiczną całość, uchwycić istotne relacje przyczynowo - skutkowe między omawianymi zagadnieniami, przeprowadzić poprawny proces wnioskowania i poszukiwania środków zaradczych.

Rozważania rozpocząłem od asymetrii informacji, określając źródła tego problemu. Zwróciłem uwagę na szczególną rolę niedoskonałości pomiaru ryzyka cybernetycznego, którą uznałem za główną przyczynę asymetrii informacji. Jednocześnie wyraziłem obawę, że usunięcie tych niedoskonałości w krótkim terminie będzie zadaniem niezwykle trudnym. Scharakteryzowałem hazard moralny i selekcję negatywną jako zjawiska będące pochodną asymetrii informacji, odnosząc się do ich aspektów teoretycznych i praktycznych. Przedstawiłem propozycje usunięcia niesprawności rynku cyberubezpieczeń wynikające z asymetrii informacji. Analogicznie zbadałem obszar kumulacji ryzyka, tzn. zidentyfikowałem źródła tego problemu i różne formy jego manifestacji. Omówiłem konsekwencje kumulacji cyberryzyka dla branży ubezpieczeń oraz zaproponowałem możliwe rozwiązania. Na koniec naświetliłem zagadnienie ubezpieczalności ryzyka cybernetycznego. W związku z tym przedstawiłem kryteria ubezpieczalności ryzyka sformułowane w pracach naukowych z teorii ubezpieczeń dokonując rozstrzygnięcia, które z kryteriów są spełnione przez ryzyko cybernetyczne, a które nie. Na koniec powiązałem kryteria ubezpieczalności ryzyka z barierami rozwoju rynku cyberubezpieczeń.

W czwartym rozdziale pracy pt. *„Przesłanki i możliwe formy zaangażowania państwa we wsparcie funkcjonowania rynku ubezpieczeń cybernetycznych"* przedstawiłem wyniki badań nad możliwym zaangażowaniem państwa w rynek ubezpieczeń cybernetycznych. Rozważania otwiera omówienie teoretycznych przesłanek partycypacji państwa w rynku ubezpieczeń, wśród których za najważniejszą uznałem istnienie zjawiska zawodności rynku (*market*

failures). Następnie zaprezentowałem różne formy bezpośredniego zaangażowania państwa w kompensację szkód katastroficznych, które zostały wyodrębnione, biorąc pod uwagę kryterium roli państwa w transferze ryzyka majątkowego. Przybliżyłem sposób, w jaki państwo może współuczestniczyć (obok branży ubezpieczeń) w finansowaniu ryzyka katastroficznego jako tzw. reasekurator ostatniej instancji, tj. podmiot, który odpowiada za pokrycie strat finansowych wynikających z wystąpienia szkód katastroficznych spowodowanych określonym ryzykiem. Wychodząc z założenia, że ryzyko cybernetyczne wykazuje podobieństwo do ryzyka terrorystycznego, dokonałem przeglądu wybranych programów ubezpieczeń (lub reasekuracji) ryzyka terrorystycznego w celu określenia cech, jakimi powinien charakteryzować się ewentualny program (*pool*) ubezpieczeń lub reasekuracji ryzyka cybernetycznego. Wskazałem potencjalne korzyści i wady wynikające z utworzenia poolu ubezpieczeń cybernetycznych. W nawiązaniu do głównego wątku rozważań, wzbogacając go o nową płaszczyznę badań, zasygnalizowałem możliwość zastosowania obligacji katastroficznych (*cat bonds*) do sekurytyzacji ryzyka cybernetycznego. Omówiłem ideę, mechanizm funkcjonowania i rynek obligacji katastroficznych, wskazując ich miejsce wśród technik alternatywnego transferu ryzyka ubezpieczeniowego. W konkluzji rozdziału zaprezentowałem wniosek, iż wartym rozważenia wariantem finansowania negatywnych skutków wystąpienia ryzyka cybernetycznego jest utworzenie poolu reasekuracyjnego z udziałem państwa w roli reasekuratora ostatniej instancji. Postulat ten poddałem szczegółowej analizie symulacyjnej w kolejnym rozdziale monografii.

Rozdział piąty zatytułowany *„Autorski model funkcjonowania rynku cyberubezpieczeń w warunkach eskalacji ryzyka cybernetycznego"* zawiera część empiryczną pracy. Przedstawiłem w nim i wykorzystałem do weryfikacji hipotez badawczych autorski model matematyczny rynku ubezpieczeń cybernetycznych. Na początek przywołałem pozycje literatury naukowej zawierające teoretyczne modele rynku ubezpieczeń cybernetycznych, poddając je ocenie i krytyce. W kolejnym punkcie sformułowałem założenia i ramową strukturę modelu, precyzyjnie definiując parametry i zasady modelowania decyzji trzech głównych typów podmiotów: ubezpieczonych, towarzystw ubezpieczeń i zakładów reasekuracji. Następnie naświetliłem metodykę symulacji, określając sześcioetapowy mechanizm generowania jej wyników. Poszczególne warianty stanów otoczenia zależą od zestawu danych wejściowych, jak również przyjętych parametrów rozkładu szkód cybernetycznych, takich jak prawdopodobieństwo wystąpienia i współczynnik korelacji *tau Goodmana-Kruskala*. Dalszą część rozdziału poświęciłem weryfikacji poszczególnych hipotez badawczych.

W zakończeniu monografii zebrałem najważniejsze wnioski oraz przedstawiłem, w jaki sposób zostały osiągnięte cele pracy i zweryfikowane hipotezy badawcze.

3.5. Osiągnięte wyniki wraz z omówieniem możliwości ich wykorzystania

W zderzeniu z nowym i powszechnym zagrożeniem, jakim jest ryzyko cybernetyczne, którego ubezpieczenie napotyka na fundamentalne problemy związane ze spełnieniem kryteriów ubezpieczalności, a potencjał możliwych szkód każe postrzegać je jako ryzyko katastroficzne, zrodziło się pytanie o rolę państwa w finansowaniu negatywnych jego skutków we współpracy z sektorem ubezpieczeń. Poszukiwanie odpowiedzi na to pytanie zainspirowało mnie do przeprowadzenia pogłębionych badań teoretyczno-empirycznych, których efektem jest niniejsza monografia. Syntezę osiągniętych wyników w odniesieniu do postawionych hipotez badawczych przedstawiam poniżej.

Wszechstronne badania literaturowe w pierwszym rozdziale pracy pokazały prawdziwość pierwszej hipotezy, że pomimo wielości podejść do definiowania ryzyka cybernetycznego, dotychczas – w szczególności na gruncie naukowym – nie powstała spójna, kompleksowa i powszechnie uznana definicja tego pojęcia. Istniejące definicje cyberryzyka odnoszą się do różnych, wycinkowych aspektów tego konstruktu, takich jak źródło ryzyka, obiekt materializacji cyberryzyka lub potencjalne negatywne skutki jego wystąpienia. Większość definicji powstała na gruncie praktyki na potrzeby regulacji prawnych w obszarze cyberbezpieczeństwa, raportów organizacji międzynarodowych, standardów technicznych i norm zarządzania bezpieczeństwem informacji. Można odnieść wrażenie, że nauka – niejako z konieczności – korzysta z dorobku praktyki. Na podstawie przeprowadzonych rozważań zaproponowałem własną definicję ryzyka cybernetycznego w brzmieniu: *„Ryzyko cybernetyczne to ryzyko operacyjne związane z prowadzeniem działalności w cyberprzestrzeni, dotyczące zasobów informacyjnych, teleinformatycznych i technologicznych, mogące powodować uszczerbek majątkowy w aktywach materialnych i niematerialnych organizacji, zakłócenie jej funkcjonowania lub obniżenie reputacji. W szczególnym przypadku źródłem ryzyka cybernetycznego mogą być zagrożenia fizyczne wobec wyżej wymienionych zasobów"*. Dodatkowo zbudowałem ontologiczny metamodel ukazujący kategorię cyberryzyka w szerszym kontekście. W modelu tym wskazałem tzw. czynniki wpływowe, które determinują zachowanie tzw. czynników efektowych (inaczej skutkowych). Czynnikami wpływowymi są m.in. źródła zagrożeń cybernetycznych, motywy działania sprawców cyberataków, wykorzystywane przez nich narzędzia i techniki czy umiejscowienie źródła zagrożenia. Po stronie czynników efektowych można wymienić częstość występowania incydentów

cybernetycznych, wielkość strat będących ich skutkiem, jak również poziom ryzyka cybernetycznego.

W wyniku diagnozy stanu rynku cyberubezpieczeń, zarówno na poziomie lokalnym (Polska), jak i globalnym, potwierdzono prawdziwość hipotezy H2. Branża ubezpieczeń nie nadąża za rozwojem technologii informacyjnych. Nie dysponując narzędziami techniczno-ubezpieczeniowymi adekwatnymi do nowych zagrożeń cybernetycznych, a jednocześnie dążąc do zwiększania przypisu składki w odpowiedzi na dynamicznie rosnący popyt, zakłady ubezpieczeń oferują produkty ochronne starając się utrzymać ekspozycję na ryzyko w bezpiecznych granicach. Świadomość współzależności występowania ryzyka cybernetycznego budzi uzasadnione obawy ubezpieczycieli, czy posiadane rezerwy okażą się wystarczające w razie wystąpienia wielkiego incydentu i kumulacji dużej liczby roszczeń. W rezultacie, na rynku oferowane są ubezpieczenia cybernetyczne z niskimi limitami odpowiedzialności, wysokimi udziałami własnymi, licznymi wyłączeniami odpowiedzialności, a same towarzystwa unikają przyjmowania do swoich portfeli ryzyk trudnych. Dla klientów strategia ta oznacza jednak niepełne zaspokojenie ich potrzeb ubezpieczeniowych.

Trzecia hipoteza badawcza brzmiała „Rozwój rynku ubezpieczeń cybernetycznych jest hamowany przez realnie istniejące bariery o zróżnicowanym charakterze. Bariery te można sprowadzić do dwóch pierwotnych (fundamentalnych) problemów węzłowych: asymetrii informacji i kumulacji ryzyka". Rozważania w rozdziale trzecim wyraźnie pokazały, z jak wieloma trudnościami zmagają się towarzystwa ubezpieczeń, które mają w swojej ofercie ubezpieczenia cybernetyczne. Niezwykła różnorodność problemów, źródeł ich pochodzenia oraz sposobów rozwiązań sprawiły, że konieczne było opracowanie autorskiej metodologii badawczej w celu ich uporządkowania i poprawnego wnioskowania. Na tej podstawie wyodrębniłem dwie grupy pierwotnych problemów węzłowych. Są nimi asymetria informacji i kumulacja ryzyka. Główną przyczyną asymetrii informacji jest niedostatek danych o ryzyku cybernetycznym, który implikuje kolejne trudności związane z pomiarem tego ryzyka. Asymetria informacji przejawia się w postaci hazardu moralnego i selekcji negatywnej, czego konsekwencją jest suboptymalny rozwój rynku cyberubezpieczeń. Aby temu przeciwdziałać, zaproponowałem m.in. nałożenie bądź rozszerzenie obowiązku raportowania incydentów cybernetycznych przez poszkodowane podmioty, certyfikację procedur cyberbezpieczeństwa w celu uproszczenia oceny ryzyka przez zakłady ubezpieczeń, częściową standaryzację warunków ubezpieczenia cybernetycznego. Jako źródło drugiego problemu, kumulacji ryzyka cybernetycznego, wskazałem proces transformacji ku gospodarce cyfrowej. Coraz większa skala cyfryzacji gospodarki sprawia, że współzależność występowania ryzyka, efekt zarażenia

i katastrofa cybernetyczna stały się realnymi zagrożeniami, w stosunku do których należy na nowo zdefiniować strategię zarządzania ryzykiem cybernetycznym. Analizując relacje przyczynowo-skutkowe między poszczególnymi składowymi powyższych problemów węzłowych, doszedłem do wniosku, że niespełnienie przez cyberryzyko niektórych warunków ubezpieczalności nie jest samoistnym, niezależnym od innych okoliczności zjawiskiem. Przeciwnie, jest konsekwencją asymetrii informacji i współzależności ryzyka, a więc uwarunkowań fundamentalnych. Spostrzeżenia te stały się podstawą potwierdzenia prawidłowości trzeciej hipotezy.

Hipoteza czwarta, w której stwierdzono, że eskalacja ryzyka cybernetycznego będzie miała negatywny wpływ na rynek cyberubezpieczeń w postaci obniżenia nasycenia rynku lub jego całkowitego zaniku, okazała się prawdziwa w części. O ile nasilenie poziomu cyberryzyka rozumiane jako wzrost wartości szkód oraz wzrost współzależności ryzyka rzeczywiście wywierały negatywny wpływ na wielkość rynku, o tyle zwiększenie prawdopodobieństwa incydentu cybernetycznego nie spowodowało dużych zakłóceń w mechanizmie rynkowym.

W toku weryfikacji hipotezy piątej doszedłem do interesujących konkluzji. Potwierdziłem istnienie luki pokrycia szkód cybernetycznych, co oznacza, że pierwsza część hipotezy jest prawdziwa. Jednak po przeprowadzeniu symulacji przyszłych stanów otoczenia ilustrujących różne aspekty eskalacji ryzyka cybernetycznego w przyszłości okazało się, że pierwotna luka pokrycia pozostaje bez zmian. Tym samym druga część hipotezy została zweryfikowana negatywnie.

Wykazanie w badaniu symulacyjnym istnienia luki pokrycia szkód cybernetycznych, jak również zagrożenia stabilności rynku cyberubezpieczeń w warunkach eskalacji ryzyka cybernetycznego w przyszłości potraktowałem jako spełnienie warunków wstępnych uzasadniających dalsze badania różnych koncepcji organizacyjno-instytucjonalnego wsparcia rynku cyberubezpieczeń, takich jak pool ubezpieczeniowy, pool reasekuracji ryzyka cybernetycznego z aktywnym udziałem państwa, jak również możliwość zastosowania obligacji katastroficznych do sekurytyzacji części tego ryzyka. Kolejne trzy hipotezy odnosiły się do tej części badań. Na początek zbadałem reakcję rynku cyberubezpieczeń na stworzenie poolu ubezpieczeń. Moim zamiarem było sprawdzenie, czy uda się osiągnąć pozytywny efekt dywersyfikacji wynikający ze zwiększenia portfela ubezpieczonych ryzyk, biorąc pod uwagę, że ryzyko cybernetyczne cechuje się współzależnością występowania strat. Wyniki symulacji w pełni potwierdziły wstępne przypuszczenia wyrażone w hipotezie szóstej. W warunkach współzależności ryzyka cybernetycznego, stworzenie poolu ubezpieczeń cybernetycznych nie spowoduje poprawy dostępności ubezpieczeń cybernetycznych. W wielu przypadkach stopień

nasycenia rynku spadał poniżej 10%, a w scenariuszach zwiększenia stopnia korelacji ryzyka rynek całkowicie zanikał. Utworzenie poolu ubezpieczeń cybernetycznych nie może być więc uznane za rekomendowane rozwiązanie.

Następnie poddałem analizie utworzenie poolu reasekuracji (pod nazwą *Pool Cyber Re*, PCR) jako elementu szerszej koncepcji programu finansowania ryzyka cybernetycznego, w którym wyższe warstwy ryzyka, tj. szkody katastroficzne, byłyby finansowane przez państwo ze środków publicznych. Podobne rozwiązania funkcjonują w niektórych krajach świata (w szczególności w Wielkiej Brytanii) w odniesieniu do zagrożeń terrorystycznych. Analiza skuteczności przedstawionej koncepcji w stymulacji rozwoju rynku ubezpieczeń cybernetycznych lub zahamowaniu jego regresu wykazała, że rozwiązanie to sprawdza się w scenariuszach aprecjacji dotkliwości strat oraz wzrostu częstości wypadków. Natomiast ocena PCR w aspekcie zwiększenia skali współzależności występowania cyberryzyka nie jest w pełni jednoznaczna. Wiadomo, że korelacja cyberryzyka obniża skuteczność dywersyfikacji przy podnoszeniu liczebności ryzyk w portfelu, co niweluje podstawową korzyść wynikającą z łączenia wielu rodzajów ryzyka w pool. Jednak nie można zapominać o istotnej wartości dodanej poolu, jaką jest obecność państwa jako reasekuratora ostatniej instancji, który zapewnia pojemność reasekuracyjną w najwyższych warstwach szkód. To sprawia, że w ostatecznym rozrachunku można mówić o korzystnej roli PCR i pozytywnej weryfikacji hipotezy siódmej.

Dostrzegając coraz większą rolę innowacyjnych metod alternatywnego transferu ryzyka (ART) w finansowaniu ryzyka ekstremalnego, a w szczególności obligacji katastroficznych (*cat bonds*), sformułowałem hipotezę ósmą w następującym brzmieniu: „W warunkach eskalacji ryzyka cybernetycznego istnieje możliwość zastosowania obligacji katastroficznych do sfinansowania części negatywnych skutków tego ryzyka w ramach proponowanego poolu reasekuracji." W wyniku analizy strony popytowej (inwestorzy na rynku kapitałowym) i strony podażowej (towarzystwo reasekuracji jako sponsor emisji) potwierdziłem prawdziwość tej hipotezy. Uzyskałem efekt redukcji kosztu reasekuracji w ramach PCR we wszystkich rozpatrywanych scenariuszach. Tym samym uprawniony jest wniosek, że w przypadku dużych i wzajemnie skorelowanych rodzajów ryzyka cybernetycznego, ich sekurytyzacja w drodze emisji obligacji katastroficznych ma przewagę nad tradycyjną reasekuracją.

Reasumując i jednocześnie odnosząc się do hipotezy głównej, w toku badań empirycznych stwierdziłem, że istnieją uzasadnione przesłanki bezpośredniego zaangażowania państwa na rynku ubezpieczeń cybernetycznych. Prowadzi to bowiem nie

tylko do stabilizacji, ale także stymulacji rozwoju tego rynku, a przez to do osiągnięcia potencjału adekwatnego do współczesnych potrzeb w dobie gospodarki cyfrowej. Efekt ten jest obserwowalny zarówno przy założeniu aktualnej ekspozycji na ryzyko cybernetyczne, jak i przy różnych, hipotetycznych scenariuszach eskalacji tego ryzyka w niedalekiej przyszłości. Weryfikacja hipotezy głównej jest zwieńczeniem wykonanej pracy badawczej, stanowiąc tym samym dowód osiągnięcia celu głównego monografii.

Przedstawiona praca ma charakter poznawczo-aplikacyjny. Jej efektem jest dostarczenie wiedzy pozwalającej na lepsze zrozumienie uwarunkowań funkcjonowania rynku ubezpieczeń cybernetycznych w warunkach dynamicznych zmian ryzyka cybernetycznego. Wnioski z przeprowadzonych badań mogą być wykorzystane przez różne podmioty przy poszukiwaniu optymalnych narzędzi finansowania negatywnych skutków wystąpienia cyberryzyka. Ciekawym wątkiem badawczym jest poszukiwanie sposobów ograniczania luki pokrycia ubezpieczeniowego. Z przeprowadzonych badań wynika, że jej zmniejszenie nie należy do łatwych zadań. Niezwykle ważnym obszarem badawczym jest modelowanie ryzyka cybernetycznego. Na wyniki tych studiów w największym stopniu oczekuje branża ubezpieczeniowa, na co wielokrotnie zwracałem uwagę w monografii. Dla decydentów odpowiedzialnych za politykę cyberbezpieczeństwa na szczeblu krajowym lub międzynarodowym omawiana praca może stanowić wartościowe studium czynników determinujących tempo rozwoju rynku ubezpieczeń cybernetycznych wskazując te obszary, które wymagają działań stymulujących ze strony administracji rządowej. Budowa katalogu dobrych praktyk dla branży ubezpieczeń w zakresie ubezpieczeń cybernetycznych, inspirowanie wspólnych działań ubezpieczycieli dla dobra ogółu (np. budowa wspólnych baz danych o szkodach cybernetycznych), kreowanie merytorycznego dyskursu w przestrzeni publicznej na temat roli ubezpieczeń w zarządzaniu ryzykiem cybernetycznym – to kolejne potencjalne obszary wykorzystania treści zawartych w monografii.

3.6. Wkład do rozwoju dyscypliny ekonomii i finansów

Monografia stanowi oryginalne dzieło na tle krajowego i międzynarodowego piśmiennictwa ekonomicznego. Zgodnie z posiadaną przeze mnie wiedzą publikacja ta stanowi pionierskie, kompleksowe studium poświęcone ubezpieczeniom cybernetycznym i roli państwa na rynku ubezpieczeń cybernetycznych. Nieliczne teoretyczne i empiryczne rozważania odnoszące się do różnych form zaangażowania państwa w rynek ubezpieczeń cybernetycznych w literaturze światowej były publikowane w formie artykułów naukowych. Krajowy dorobek teoretyczny i empiryczny w tym zakresie jest znikomy.

Przedłożona w postępowaniu habilitacyjnym praca stanowi w mojej opinii wkład w rozwój nauki w dyscyplinie ekonomia i finanse zarówno w części teoretycznej, jak i empirycznej, a dodatkowo – poprzez wskazanie możliwych działań państwa mających na celu podtrzymanie rozwoju rynku ubezpieczeń cybernetycznych – ma też walor utylitarny.

Wkład teoretyczno-poznawczy w dyscyplinę ekonomii i finansów upatruję w szczególności w:

- usystematyzowaniu wiedzy na temat ryzyka cybernetycznego i jego rodzajów,
- opracowaniu autorskiego podejścia do systematyki definicji ryzyka cybernetycznego według kryterium zawartości informacyjnej i wyodrębnieniu trzech różnych aspektów w pojmowaniu istoty ryzyka cybernetycznego (źródło ryzyka, obiekt materializacji ryzyka, skutki realizacji ryzyka); idąc dalej typ tropem, pogrupowano istniejące definicje ryzyka cybernetycznego na definicje jednowymiarowe, dwuwymiarowe oraz kompleksowe (tj. odnoszące się w swej treści do wszystkich trzech wymienionych aspektów cyberryzyka),
- sformułowaniu własnej, kompleksowej definicji ryzyka cybernetycznego, uwzględniającej aktualny stan wiedzy w dziedzinie cyberbezpieczeństwa,
- autorskiej koncepcji ontologicznego metamodelu ryzyka cybernetycznego; wkład proponowanego metamodelu w rozwój dyscypliny można rozpatrywać w czterech aspektach:
    - identyfikacja czterech grup czynników charakteryzujących zagrożenia cybernetyczne (źródła zagrożeń, siła sprawcza, motywy działania sprawców, lokalizacja zagrożenia względem organizacji),
    - przedstawienie ryzyka cybernetycznego w kontekście misji, strategii, celów i polityk organizacji, w szczególności w kontekście polityki zarządzania ryzykiem,
    - pokazanie, że czynniki określające poziom ryzyka cybernetycznego, tj. prawdopodobieństwo wystąpienia i potencjalne negatywne skutki, mają charakter abstrakcyjny (tzn. wyznaczony przy pomocy narzędzi matematyczno-statystycznych), lecz są szacowane na podstawie danych historycznych o faktycznie zaistniałych incydentach i rozmiarach szkód. W warunkach dynamicznych i trudnych do przewidzenia zmian poziomu i charakteru ryzyka cybernetycznego rodzi to uzasadnione obawy o adekwatność modeli predykcyjnych,
    - ukazanie złożoności wzajemnych relacji między elementami składowymi konceptu ryzyka cybernetycznego,
- systematyzacji dotychczasowego dorobku naukowego i krytycznej analizie literatury przedmiotu z zakresu ubezpieczeń cybernetycznych (na polskim rynku jak dotąd nie ukazała się monografia poświęcona w całości ubezpieczeniom cybernetycznym),

- propozycji autorskiej metody badawczej do analizy barier rozwoju rynku ubezpieczeń cybernetycznych; przy pomocy tej metody zidentyfikowano i jednoznacznie zdefiniowano wspomniane bariery, opisano materialne formy ich manifestacji i konsekwencje dla rynku ubezpieczeń, na koniec proponując określone środki zaradcze.

W **części empirycznej** mój wkład do rozwoju nauki polega na:

- zbudowaniu autorskiego modelu matematycznego symulującego funkcjonowanie rynku ubezpieczeń cybernetycznych,

  W porównaniu z opublikowanymi dotychczas modelami odnoszącymi się do powyższego zagadnienia, przedstawiony model posiada unikalne cechy, stanowiące jego wkład w rozwój nauki. Kalibracja parametrów modelu w taki sposób, by odzwierciedlały aktualne realia rynku ubezpieczeń cybernetycznych i jego otoczenia, jak również zachowanie równowagi między precyzją modelu a jego relatywną prostotą, pozwalającą na efektywne przeprowadzenie licznych symulacji – zdaniem autora stanowią wartość dodaną prezentowanych wyników badań w porównaniu z wcześniejszymi publikacjami. Modelując decyzje poszczególnych uczestników rynku cyberubezpieczeń połączono teorię użyteczności (zasada maksymalizacji oczekiwanej użyteczności majątku jako kryterium podejmowania decyzji w warunkach niepewności) z teorią ubezpieczeń (aktuarialne zasady kalkulacji składki ubezpieczeniowej, kryterium wypłacalności wynikające z teorii ruiny przy podejmowaniu decyzji o podaży ubezpieczeń).

- analizie wpływu eskalacji ryzyka cybernetycznego na rynek ubezpieczeń cybernetycznych,

- identyfikacji i empirycznym potwierdzeniu istnienia problemu luki pokrycia ubezpieczeniowego w zakresie ryzyka cybernetycznego oraz analizie rozmiarów luki pokrycia w różnych scenariuszach eskalacji cyberryzyka,

- dostarczeniu dowodów empirycznych sugerujących zasadność utworzenia poolu ryzyk cybernetycznych oraz zaangażowanie państwa w finansowanie części ryzyka cybernetycznego jako reasekurator ostatniej instancji.

Przeprowadzone badania wnoszą również wkład **w wymiarze utylitarnym**:

- całość rozważań dotyczących ryzyka cybernetycznego (jego definicji, źródeł, rodzajów, form materializacji) oraz ubezpieczeń cybernetycznych, może przyczynić się do budowania świadomości ubezpieczeniowej właścicieli i kadry zarządczej podmiotów gospodarczych, pełniejszego zrozumienia istoty i roli tych ubezpieczeń w zarządzaniu ryzykiem cybernetycznym, co w konsekwencji może doprowadzić do rozpowszechnienia ubezpieczeń cybernetycznych,

- prezentacja możliwych form bezpośredniego udziału państwa w rynku ubezpieczeń cybernetycznych wraz ze wskazaniem zasadności ich wykorzystania, może mieć walor opiniotwórczy w kształtowaniu relacji między podmiotami rynku ubezpieczeń a organami państwa w zakresie polityki cyberbezpieczeństwa oraz roli ubezpieczeń cybernetycznych w gospodarce narodowej.

4. Informacja o istotnej aktywności naukowej realizowanej w więcej niż jednej uczelni lub instytucji naukowej, w szczególności zagranicznej

4.1. Syntetyczna charakterystyka dorobku naukowego

Mój dotychczasowy dorobek naukowy obejmuje 63 recenzowane prace naukowe, na które składają się 2 monografie naukowe (w tym rozprawa habilitacyjna), 26 artykułów w czasopismach naukowych (w tym 2 z Impact Factorem), 29 rozdziałów w monografiach oraz 6 redakcji monografii naukowych (tabela 1). 51 prac przygotowałem samodzielnie, a 12 powstało we współautorstwie. Z łącznej liczby publikacji, po doktoracie opublikowałem 52 prace, w tym 12 prac w języku angielskim (5 to artykuły naukowe, a 7 to rozdziały w monografiach).

Tabela 1. Syntetyczne zestawienie dorobku naukowego

Wyszczególnienie	Przed uzyskaniem stopnia doktora	Po uzyskaniu stopnia doktora	Razem
Monografie	-	2	2
Rozdziały w monografiach	9	20	29
Artykuły w czasopismach naukowych	2	24	26
Redakcja naukowa monografii	-	6	6
Razem	11	52	63

Źródło: na podstawie bazy Dorobek Uniwersytetu Ekonomicznego w Krakowie.

Wydawcy publikacji obejmują renomowane międzynarodowe wydawnictwa z obszaru nauk ekonomicznych (Springer), krajowe renomowane wydawnictwa naukowe (C.H. Beck, Wolters Kluwer, Poltext, Difin, CeDeWu) czy wydawnictwa uniwersyteckie (Masaryk University in Brno (Czechy), Szkoła Główna Handlowa w Warszawie, Uniwersytet Ekonomiczny w Katowicach, Uniwersytet Ekonomiczny w Krakowie, Uniwersytet Warmińsko-Mazurski w Olsztynie). Poza nimi są to wiodące czasopisma naukowe, takie jak *Geneva Papers on Risk and Insurance - Issues and Practice, Safety Science, Economics and Business Review, Ekonomista, Finanse. Czasopismo Komitetu Nauk o Finansach PAN, Rozprawy Ubezpieczeniowe, Wiadomości Ubezpieczeniowe.*

Łączna liczba punktów za prace opublikowane w okresie przed uzyskaniem stopnia doktora wynosi 34 (tabela 2). Tyle samo wynosi łączna liczba punktów ważonych

procentowym wkładem w powstanie publikacji. Z kolei łączna liczba punktów za prace opublikowane w okresie po uzyskaniu stopnia doktora wynosi 699. Natomiast łączna liczba punktów ważonych procentowym wkładem w powstanie publikacji to 628,8. Sumaryczny Impact Factor moich publikacji wynosi 4,408 (z roku publikacji), a 5-letni Impact Factor to 4,931.

Tabela 2. Zestawienie liczby punktów MNiSW

Wyszczególnienie	Okres przed doktoratem	Okres po doktoracie
Monografie naukowe	-	**125** (102,5)*
Rozdziały w monografiach	**28** (28)	**213** (203,5)
Redakcja naukowa monografii	-	**30** (11,8)
Artykuły w czasopismach naukowych	**6** (6)	**331** (311)
Razem	**34** (34)	**699** (628,8)

* W nawiasach podano liczbę punktów ważoną udziałem w powstaniu publikacji.
Źródło: na podstawie bazy Dorobek Uniwersytetu Ekonomicznego w Krakowie.

Cytowania prac bez autocytowań, zgodnie z raportem przygotowanym przez Bibliotekę Główną Uniwersytetu Ekonomicznego w Krakowie, pokazuje tabela 3. Łączna liczba cytowań moich prac wynosi 101 i odnosi się do 35 publikacji, a współczynnik Hirscha przyjął wartość 6.

Tabela 3. Statystyka dotycząca cytowań (bez autocytowań)

Wyszczególnienie	Liczba cytowanych prac	Liczba cytowań bez autocytowań	Indeks Hirscha bez autocytowań
Web of Science	**1**	**1**	**1**
Web of Science B	**8**	**5**	**-**
Scopus	**1**	**1**	**1**
Scopus B	**6**	**12**	**-**
BazEkon	**16**	**25**	**3**
Inne źródła	**28**	**63**	**4**
Razem (bez powtórzeń)	**35**	**101**	**6**

Źródło: raport Biblioteki Głównej Uniwersytetu Ekonomicznego w Krakowie (stan na 1.02.2021 r.)

4.2. Obszary prowadzonych badań naukowych

Moje zainteresowania naukowe po uzyskaniu stopnia doktora nauk ekonomicznych koncentrowały się wokół czterech powiązanych ze sobą obszarów badawczych, które doprowadziły mnie do wyboru tematu rozprawy habilitacyjnej. Były to:

- Instrumenty finansowania negatywnych skutków katastrof naturalnych
- Popyt przedsiębiorstw na ubezpieczenia majątkowe a retencja ryzyka
- Motywy zakupu dotowanego ubezpieczenia upraw rolnych i zwierząt gospodarskich
- Ryzyko cybernetyczne i ubezpieczenia cybernetyczne

Główną osią, wokół której koncentruje się mój dorobek naukowy w dyscyplinie ekonomia i finanse jest problematyka ubezpieczeń gospodarczych. Jest to pochodną obszaru badawczego Katedry Zarządzania Ryzykiem i Ubezpieczeń, w której jestem zatrudniony od samego początku. Moje zainteresowania badawcze zostały ukształtowane przez samodzielne studia literaturowe, realizowane projekty badawcze, współpracę naukowo-badawczą z innymi ośrodkami oraz współpracę z otoczeniem gospodarczym (głównie w charakterze brokera ubezpieczeniowego).

4.2.1. Instrumenty finansowania negatywnych skutków katastrof naturalnych

Do pierwszego obszaru tematycznego zaliczyłem:

1. **Strupczewski G.** (2009), Obligacje katastroficzne wobec kryzysu na rynkach finansowych, [w:] Szanse i zagrożenia dla rynków ubezpieczeń w krajach Europy Środkowej i Wschodniej, red. W. Sułkowska, Wyd. Uniwersytetu Ekonomicznego w Krakowie, Kraków, s. 85-93, ISBN: 978-83-7252-462-1
2. **Strupczewski G.** (2011), Ubezpieczenie od skutków trzęsień ziemi w Japonii jako przykład udziału państwa w reasekuracji ryzyka katastroficznego, "Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego", ISSN: 1644-8979, Nr 11(2011), s. 437-446
3. **Strupczewski G.** (2011), Wybór triggera w obligacjach katastroficznych, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Poznaniu", Tytuł numeru: "Studia Ubezpieczeniowe. Społeczno-gospodarcze aspekty funkcjonowania rynku ubezpieczeniowego", ISSN: 1689-7374, Nr 181(2011), s. 160-168
4. **Strupczewski G.** (2011), Zastosowanie ubezpieczeniowych instrumentów pochodnych jako sposób alternatywnego transferu ryzyka katastroficznego, "Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie", ISSN: 1898-6447, Nr 875(2011), s. 29-46
5. **Strupczewski G.** (2012), Program ubezpieczeń katastroficznych w Rumunii, "Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego", ISSN: 1644-8979, Nr 13(2012), s. 277-288

6. **Strupczewski G.** (2013), Narodowy program ubezpieczeń powodziowych w USA – sugerowane kierunki zmian, [w:] Wyzwania dla rynków ubezpieczeń w świetle sytuacji na globalnych rynkach finansowych, red. T. Michalski, Oficyna Wydawnicza SGH w Warszawie, Warszawa, s. 191-210, ISBN: 978-83-7378-799-5

Badania naukowe w tym obszarze są kontynuacją i rozwinięciem zainteresowań badawczych wokół problematyki zarządzania ryzykiem katastrof naturalnych i roli ubezpieczeń w tym procesie, zawartej w dysertacji doktorskiej. Warto jednak podkreślić, że pewne wątki badawcze znalazły zastosowanie w książce habilitacyjnej, wskazując na ciągłość procesu ewolucji moich zainteresowań badawczych.

Publikacje [1], [3] i [4] są wynikiem zainteresowania wykorzystaniem ubezpieczeniowych instrumentów pochodnych i obligacji katastroficznych (*cat bonds*) w finansowaniu negatywnych skutków katastrof naturalnych i ich rolą w dostarczeniu na rynek ubezpieczeń dodatkowej pojemności. Wnioski z tych badań wykorzystałem później w monografii habilitacyjnej w odniesieniu do ryzyka cybernetycznego.

Celem pracy [1] była analiza wpływu kryzysu finansowego zapoczątkowanego we wrześniu 2008 r. w USA na rynek obligacji katastroficznych, które stanowią ważny instrument finansowania ryzyka klęsk żywiołowych, alternatywny wobec klasycznej reasekuracji. Pomijając kilka serii obligacji bezpośrednio związanych z upadłym bankiem Lehmann Brothers, cat bonds wykazały się odpornością na światowy kryzys finansowy, potwierdzając teorię o braku korelacji ze stopami zwrotu na rynkach kapitałowych. W odpowiedzi na spadek zaufania inwestorów do złożonych instrumentów pochodnych, w obligacjach katastroficznych wprowadzono szereg zmian w ich konstrukcji mających na celu poprawę transparentności i wiarygodności kredytowej.

W artykule [3] skupiłem uwagę na jednym z podstawowych parametrów obligacji katastroficznej, jakim jest tzw. trigger. Spełnienie warunków określonych w triggerze warunkuje wykorzystanie przez sponsora/cedenta kapitału zgromadzonego w wyniku jej emisji. Wybór rodzaju triggera wynika z wielu uwarunkowań, przede wszystkim związanych ze specyfiką sekurytyzowanego ryzyka, a także wiąże się z pewnymi konsekwencjami dla sponsora i inwestorów, takimi jak wymagana premia za ryzyko, poziom ryzyka bazowego, hazard moralny i poziom transparentności obligacji. Przedmiotem badań była analiza rynku cat-bonds pod kątem tendencji w wykorzystaniu różnych rodzajów triggerów. Rezultaty badań ukazały złożoność uwarunkowań wyboru określonego rodzaju triggera i wagę tej decyzji dla sukcesu emisji.

W artykule [4] przedstawiłem istotę, rodzaje i zasady działania ubezpieczeniowych instrumentów pochodnych, zwracając szczególną uwagę na możliwości ich zastosowania w finansowaniu ryzyka katastroficznego.

Analiza wybranych narodowych programów ubezpieczeń katastrof naturalnych w celu identyfikacji ich wad i korzyści oraz wskazania dobrych praktyk wartych rozważenia w kontekście implementacji w warunkach polskich, stanowi wątek badawczy łączący teksty [2], [5] i [6]. Rezultaty tych rozważań stanowiły bazę do dyskusji nad potencjalną rolą państwa w rynku ubezpieczeń cybernetycznych, zawartą w monografii habilitacyjnej.

W tekście [6] zawarłem obszerne studium Narodowego Programu Ubezpieczeń Powodziowych w USA (NFIP). Scharakteryzowałem warunki ubezpieczenia i zasady

finansowania NFIP, zidentyfikowałem i poddałem dyskusji bariery rozwoju NFIP, dokonałem krytycznej oceny projektu nowelizacji ustawy o NFIP (z 2011 r.), jak również innych koncepcji reformy NFIP zgłaszanych przez świat nauki i praktyków. W konkluzji podkreśliłem, iż poszukując optymalnego modelu finansowania negatywnych skutków ryzyka powodzi warto dążyć do równowagi między zaangażowaniem państwa a udziałem prywatnych ubezpieczycieli, zapewniając jednocześnie odpowiednią infrastrukturę organizacyjną, prawną i techniczną.

Do napisania artykułu [5] skłoniła mnie chęć zbadania doświadczeń z procesu wdrażania i pierwszych lat funkcjonowania programu ubezpieczeń katastroficznych uruchomionego w Rumunii w lipcu 2010 r. Płynące stąd wnioski mogły okazać się ważne dla krajów, które rozważają wprowadzenie własnych rozwiązań ubezpieczeniowych w odniesieniu do katastrof naturalnych. Doświadczenia rumuńskie potwierdziły, że najefektywniejszym rozwiązaniem jest skorzystanie z potencjału, jaki oferuje partnerstwo publiczno-prywatne między władzą publiczną a branżą ubezpieczeniową i reasekuracyjną.

Program ubezpieczeń budynków mieszkalnych od skutków trzęsień ziemi w Japonii – przedstawiony w artykule [2] – jest interesującym przykładem rozwiązania systemowego, w którym państwo angażuje się w reasekurację części ryzyka. Wyniki moich badań doprowadziły do wniosku, że udział państwa pozwala przesunąć granicę ubezpieczalności ryzyka, a przez to otworzyć szansę akceptacji tego ryzyka przez sektor prywatnych ubezpieczycieli i zwiększyć powszechność ubezpieczenia.

4.2.2. Popyt przedsiębiorstw na ubezpieczenia majątkowe a retencja ryzyka

Do drugiego obszaru tematycznego zaliczyłem:

1. **Strupczewski G.,** Thlon M. (2014), Wykorzystanie techniki zatrzymania ryzyka przez średnie i duże przedsiębiorstwa w Polsce w świetle badań ankietowych, "Wiadomości Ubezpieczeniowe", ISSN: 0137-7264, Nr 3/2014, s. 31-55
2. **Strupczewski G.** (2014), Why enterprises buy insurance? Theoretical aspects of corporate demand for property insurance, [w:] Managing disruption and destabilization, red. T. Baaken, J. Teczke, Wyd. International Management Foundation oraz Uniwersytet Ekonomiczny w Krakowie, Kraków-Muenster, s. 69-80, ISBN: 978-83-937642-3-5
3. **Strupczewski G.** (2014), Corporate Non-life Insurance Claims: Empirical Evidence from the Polish Market, [w:] European Financial Systems 2014. Proceedings of the 11th International Scientific Conference, Wyd. Masaryk University, Brno, s. 596-604, ISBN: 978-80-210-7153-7
4. **Strupczewski G.,** Thlon M. (2015), Retencja ryzyka a ubezpieczenie: analiza zachowań polskich przedsiębiorstw, " Ekonomista", ISSN: 0013-3205, Nr 6, s. 804-829
5. **Strupczewski G.,** Thlon M., Fijorek K. (2016), Corporate Insurance Versus Risk Retention: an Empirical Analysis of Medium and Large Companies in Poland, "The Geneva Papers on Risk and Insurance - Issues and Practice", ISSN: 1018-5895, Vol. 41(4), s. 626-649, DOI: 10.1057/s41288-016-0005-4

Problematyka badawcza drugiego obszaru tematycznego koncentruje się wokół determinant popytu przedsiębiorstw na ubezpieczenia majątkowe oraz roli retencji ryzyka jako

alternatywy wobec zakupu ubezpieczenia. Badania w obrębie tego obszaru zainteresowań otwiera tekst [2] o charakterze teoriopoznawczym, w którym dokonałem syntezy dorobku literatury światowej w zakresie czynników wyjaśniających popyt przedsiębiorstw na ubezpieczenia majątkowe. Krytyczna analiza najważniejszych publikacji doprowadziła do konkluzji, że teoria ubezpieczeń nie dostarcza jednoznacznego wyjaśnienia przesłanek zakupu ubezpieczeń majątkowych przez przedsiębiorstwa.

Tekst [3] stanowi uzupełnienie rozważań poświęconych roli ubezpieczeń w finansowaniu strat w majątku przedsiębiorstw. Dzięki pozyskaniu obszernej bazy danych zawierającej rejestr 5.000 szkód ubezpieczeniowych zgłoszonych do zakładów ubezpieczeń przez 480 polskich firm w okresie 7 lat, przeprowadziłem wielowymiarową analizę zgłoszonych roszczeń w przekroju rodzajów działalności gospodarczej i różnych linii ubezpieczeń. Wykazałem istotne zróżnicowanie częstości, dotkliwości i rodzaju szkód w zależności od przedmiotu działalności gospodarczej. Dodatkowo poddałem badaniu skalę retencji ryzyka stosowaną przez poszkodowane przedsiębiorstwa zanotowane w bazie, ponownie uzyskując wyniki wskazujące na znaczne zróżnicowanie. Firmy z branży energetycznej i rozrywkowej zatrzymywały na udziale własnym niższy odsetek strat niż firmy z branży nieruchomości, instytucje finansowe, firmy usługowe i administracja publiczna. Przytoczone wyniki skłoniły mnie do podjęcia pogłębionych badań nad retencją ryzyka w kontekście ubezpieczeń. Rezultatem tych dociekań są artykuły [1] i [4] napisane na bazie wyników badania ankietowego na ogólnopolskiej próbie 386 średnich i dużych przedsiębiorstw, oraz artykuł [5], który można traktować jako zwieńczenie niniejszego obszaru badań.

W artykule [1] szczególną uwagę poświęciłem opisowi motywów wyboru między ubezpieczeniem a retencją ryzyka. Najważniejszą przesłanką zatrzymania ryzyka jest brak oferty ubezpieczenia adekwatnej do potrzeb firmy. Drugim istotnym powodem rezygnacji z ubezpieczenia i wyboru samofinansowania ryzyka jest wysoki koszt związany z realizacją zaleceń audytu ubezpieczeniowego. Kolejnymi motywami wyboru retencji są: skrócenie czasu likwidacji szkody i oczekiwania na wypłatę odszkodowania oraz niższy koszt w stosunku do składki ubezpieczeniowej. Badaniu poddano również zróżnicowanie elastyczności popytu na ubezpieczenie, tj. deklarowaną reakcję przedsiębiorstwa na wzrost składki ubezpieczeniowej. Z badań wynika, że czynnikiem różnicującym elastyczność popytu jest rodzaj prowadzonej działalności gospodarczej. Największą tolerancją wobec podwyżki składki wykazały się przedsiębiorstwa usługowe, a najniższą – firmy handlowe.

W rezultacie przeprowadzonych badań w artykule [4] zidentyfikowałem najważniejsze czynniki warunkujące poziom retencji ryzyka w analizowanych przedsiębiorstwach. Ustaliłem, że większa liczba szkód w przedsiębiorstwie, wyższe zatrudnienie (a więc pośrednio wielkość firmy) oraz większa kwota płaconej aktualnie składki ubezpieczeniowej miały związek z wyższym stopniem zatrzymania ryzyka na udziale własnym. Na poziom samoubezpieczenia nie mają istotnego wpływu motywy związane ze stabilizacją cash-flow i bezpieczeństwem finansowym przedsiębiorstwa. Skala stosowanej retencji ryzyka różni się pomiędzy firmami z różnych branż gospodarki (wg PKD), jak i pomiędzy podmiotami wykonującymi działalność usługową, produkcyjną lub handlową. Wiek firmy nie miał natomiast istotnego znaczenia w kontekście zatrzymania ryzyka.

W pracy [5], posługując się modelem regresji wielorakiej zidentyfikowałem zmienne, które mają istotny statystycznie związek z poziomem retencji w przedsiębiorstwie. Zgodnie z przewidywaniami opartymi na przeglądzie literatury wykazałem, iż racjonalny konsument liczy się z ryzykiem odrzucenia jego roszczenia przez towarzystwo ubezpieczeń oraz ryzykiem zbyt długiego oczekiwania na decyzję o uznaniu roszczenia, a przez to decyduje się na zatrzymanie części ryzyka. Ponadto, analogicznie do wcześniejszych prac, branża w której firma prowadzi działalność jest powiązana z rozmiarami retencji, a wysoki koszt ubezpieczenia i niski poziom akceptacji ewentualnych podwyżek składki dodatnio korelują z wielkością ryzyka zatrzymanego.

4.2.3. Motywy zakupu dotowanego ubezpieczenia upraw rolnych i zwierząt gospodarskich

Do trzeciego obszaru tematycznego zaliczyłem:

1. **Strupczewski G.** (2015), Zastosowanie regresji porządkowej do identyfikacji determinant skłonności do płacenia składki za ubezpieczenie upraw rolnych, [w:] Dylematy teorii i praktyki ubezpieczeń, red. W. Sułkowska, G. Strupczewski, Wyd. Poltext, Warszawa, s. 263-279, ISBN: 978-83-7561-595-1
2. **Strupczewski G.** (2015), Cluster analysis of natural disaster losses in Polish agriculture, "Scientific Papers Series Management, Economic Engineering in Agriculture and Rural Development", ISSN: 2284-7995, Vol. 15, Issue 1, s. 513-526
3. **Strupczewski G.** (2016), Identyfikacja kluczowych determinant zakupu dotowanego ubezpieczenia upraw rolnych i zwierząt gospodarskich, "Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", ISSN: 1899-3192, Nr 415, s. 225-240, DOI: 10.15611/pn.2016.415.21
4. **Strupczewski G.** (2019), What characterizes farmers who purchase crop insurance in Poland?, "Problems of Agricultural Economics", ISSN: 2392-3458, Nr 1(358), s. 106-119, DOI: 10.30858/zer/103596

Prezentowane prace są efektem badań statutowych pt. „Ryzyko i ubezpieczenia w obszarze rolnictwa" prowadzonych w Katedrze Zarządzania Ryzykiem i Ubezpieczeń UEK w latach 2014-2015. Pozostając w nurcie badań nad czynnikami popytu na ubezpieczenia majątkowe, skupiłem swoje zainteresowania na grupie zawodowej rolników. Publikacje [1], [3] i [4] zostały oparte na wynikach badań ankietowych na ogólnopolskiej próbie 150 rolników prowadzących gospodarstwa rolne o powierzchni użytków rolnych minimum 5 ha.

W artykule [3] podjąłem rozważania nad przyczynami relatywnie niskiego popytu producentów rolnych na dotowane ubezpieczenie upraw rolnych i zwierząt gospodarskich. Celem artykułu było wskazanie zmiennych istotnie wpływających na zakup tego ubezpieczenia oraz zbudowanie modelu decyzyjnego (ekonometrycznego) określającego prawdopodobieństwo zakupu ubezpieczenia upraw. Wykazałem, iż decyzja o zakupie ubezpieczenia upraw warunkowana jest dodatnio dwoma czynnikami: powierzchnią posiadanych gruntów rolnych oraz skłonnością do zapłaty składki ubezpieczeniowej. Szansa zakupu ubezpieczenia jest 2,07 razy wyższa, jeśli gospodarstwo rolne dysponuje większym areałem gruntów rolnych. Z kolei, im wyższa składka ubezpieczeniowa, którą skłonny jest zaakceptować ankietowany, tym większe prawdopodobieństwo zakupu ubezpieczenia upraw.

Wzrost deklarowanej skłonności do płacenia składki WTP o jeden punkt procentowy wiąże się z 1,73 razy większą szansą na zakup ubezpieczenia.

Ten drugi czynnik, skłonność do płacenia składki (WTP, *Willingness To Pay*), stał się przedmiotem pogłębionych analiz w pracy [1]. Starałem się w niej wskazać czynniki wpływające na maksymalną akceptowalną składkę za dotowane ubezpieczenie upraw, którą rolnicy byliby gotowi ponieść. Do analizy danych użyłem modelu wieloczynnikowej regresji porządkowej. Badania pokazały, że mężczyźni są skłonni zaakceptować wyższą składkę ubezpieczeniową w porównaniu z kobietami. Po drugie, posiadacze mniejszych obszarowo gospodarstw są gotowi zaakceptować wyższą cenę ubezpieczenia niż farmerzy dysponujący dużym areałem upraw. Po trzecie, zaobserwowałem że wiek i związane z nim doświadczenie życiowe kształtują świadomość ubezpieczeniową rolnika, prowadząc do zwiększenia motywacji zakupu ubezpieczenia, nawet za cenę wyższej składki.

Celem artykułu [4] było porównanie populacji rolników, którzy wykupili dotowane ubezpieczenie upraw z populacją rolników nieubezpieczonych. Na tej podstawie zidentyfikowałem cechy charakteryzujące rolników, którzy zdecydowali się na zakup ubezpieczenia upraw. Obserwacje te zostały wykorzystane do wyciągnięcia bardziej ogólnych wniosków dotyczących czynników wpływających na skłonność do zakupu ubezpieczenia. W tym celu uwzględniłem czynniki demograficzne, społeczne i ekonomiczne, indywidualne postrzeganie ryzyka, liczbę szkód w uprawach doświadczonych przez rolnika w ostatnich 15 latach oraz skłonność do płacenia składki ubezpieczeniowej. Uzyskane rezultaty potwierdziły wcześniejsze wyniki badań. Dodatkowo wykazałem wpływ poziomu dochodów z produkcji rolnej oraz doświadczenia strat materialnych w przeszłości na gotowość do zakupu ubezpieczenia. Co zaskakujące, czynniki takie jak poziom wykształcenia czy percepcja ryzyka nie determinują decyzji o ubezpieczeniu upraw.

Artykuł [2] jest wynikiem zainteresowania problematyką zróżnicowania przestrzennego szkód w rolnictwie spowodowanych ryzykami naturalnymi, co jest zagadnieniem istotnym przy budowie taryf ubezpieczeniowych. Wyniki analizy skupień województw ze względu na kryteria wartości szkód w uprawach i powierzchni zniszczonych upraw wykazały, że 11 województw tworzy jednorodną grupę, natomiast pozostałe 5 województw cechuje się odrębnymi profilami szkodowości. Rezultaty te stanowią przesłankę do wprowadzenia zróżnicowania składki ubezpieczeniowej ze względu na położenie geograficzne gospodarstwa rolnego.

4.2.4. Ryzyko cybernetyczne i ubezpieczenia cybernetyczne

Czwarty obszar tematyczny, który zawiera najwięcej publikacji (14), podzieliłem na 4 nurty badawcze:

1. Zagrożenia cybernetyczne w wybranych obszarach gospodarki
2. Pojęcie i analiza ryzyka cybernetycznego
3. Ubezpieczenia cybernetyczne
4. Rola państwa w rynku ubezpieczeń cybernetycznych

Jest on komplementarny wobec badań prowadzonych w monografii habilitacyjnej. Rozważania prowadzone w poszczególnych nurtach i uzyskane wyniki badań kształtowały stopniowo moje

spojrzenie na tematykę ryzyka cybernetycznego i ubezpieczeń cybernetycznych, co doprowadziło do wskazania istotnych w moim mniemaniu problemów badawczych, sformułowania hipotez i celów badawczych w monografii habilitacyjnej.

Nurt 1 – Zagrożenia cybernetyczne w wybranych obszarach gospodarki

1. **Strupczewski G.** (2017), Zagrożenia cybernetyczne instytucji finansowych, "Rozprawy Ubezpieczeniowe. Konsument na rynku usług finansowych", ISSN: 1896-3641, Vol. 2, Nr 24, s. 65-83
2. **Strupczewski G.** (2019), Pracownicze plany kapitałowe jako e-usługa – między funkcjonalnością a cyberbezpieczeństwem, [w:] Ubezpieczenia: Wyzwania rynku, red. I. Kwiecień, P. Kowalczyk-Rólczyńska, Wyd. C.H. Beck, Warszawa, s. 63-74, ISBN: 978-83-8198-041-8
3. **Strupczewski G.** (2019), Nowoczesne rolnictwo wobec zagrożeń cybernetycznych, "Ubezpieczenia w rolnictwie", ISSN: 1507-4757, Nr 70/2019, s. 9-31

Tematem przewodnim tego nurtu badań są rozważania nad skalą zagrożeń cybernetycznych w wybranych obszarach gospodarki. W artykule [1] skoncentrowałem uwagę na instytucjach finansowych, wskazując możliwości zastosowania ubezpieczeń cybernetycznych jako narzędzia minimalizującego negatywny wpływ incydentów cybernetycznych.

W tekście [2] kontynuowałem badania nad branżą usług finansowych. Wychodząc od potwierdzenia hipotezy, iż pracownicze plany kapitałowe (PPK) będą funkcjonować w modelu e-usługi, wskazałem źródła podatności systemu PPK na zagrożenia cybernetyczne. Są nimi: znaczna skala operacji uruchomienia PPK, zróżnicowanie podmiotowe uczestników systemu, ryzyko niedostatecznych kompetencji cyfrowych oszczędzających, intensyfikacja zjawiska cyberprzestępczości, zwłaszcza w obszarze usług finansowych.

Nawiązując do moich wcześniejszych zainteresowań sektorem rolnictwa, w pracy [3] podjąłem się wskazania zagrożeń cybernetycznych wobec nowoczesnego rolnictwa, wynikających z wykorzystania najnowszych technologii cyfrowych, takich jak internet rzeczy i rolnictwo precyzyjne. Na koniec sformułowałem kierunki działań zmierzające do poprawy stanu cyberbezpieczeństwa agrobiznesu.

Nurt 2 – Pojęcie i analiza ryzyka cybernetycznego

1. **Strupczewski G.** (2019), What is the worst scenario? Modeling extreme cyber losses, [w:] Multiple Perspectives in Risk and Risk Management, red. P. Linsley, P. Shrives, M. Wieczorek-Kosmala, Wyd. Springer, Cham, s. 211-230, ISBN: 978-3-030-16044-9
2. **Strupczewski G.** (2020), What Do We Know About Data Breaches? Empirical Evidence from the United States, [w:] Eurasian Economic Perspectives. Eurasian Studies in Business and Economics, red. M. Bilgin, H. Danis, G. Karabulut, G. Gözgor, Wyd. Springer, Cham, s. 281-299, ISBN: 978-3-030-40374-4
3. **Strupczewski G.** (2021), Defining Cyber Risk, "Safety Science", ISSN: 0925-7535, Vol. 135, March 2021 (105143), s. 1-10, DOI: 10.1016/j.ssci.2020.105143

Praca [1] jest wynikiem zainteresowania statystycznymi właściwościami rozkładu ryzyka cybernetycznego w części odnoszącej się do dużych strat występujących z niskim prawdopodobieństwem, a więc w obszarze tzw. ryzyka ekstremalnego. Modelowanie ryzyka ekstremalnego jest szczególnie istotne w tych rodzajach ryzyka, które cechują się prawoskośnym rozkładem strat, a do takich należy – w świetle danych empirycznych – ryzyko

cybernetyczne. W artykule porównałem różne rozkłady ryzyka ekstremalnego, zarówno klasyczne (uogólniony rozkład Pareto GPD), jak i mieszane (m.in. rozkład Erlanga), celem znalezienia odpowiedzi na pytanie, który z nich jest najlepiej dopasowany do danych empirycznych. Ustaliłem, że rozkładem teoretycznym, który najlepiej odzwierciedla warunki rzeczywiste (w świetle przyjętych kryteriów oceny) jest rozkład GPD.

Świadomość znaczenia, jakie w nowoczesnej gospodarce cyfrowej ma ochrona danych osobowych przed różnymi zagrożeniami pochodzącymi z cyberprzestrzeni, skłoniła mnie do podjęcia pogłębionych badań (tekst [2]) nad ryzykiem wycieku danych osobowych (ang. *data breach*). Naruszenie bezpieczeństwa danych osobowych to jeden z ważniejszych aspektów ryzyka cybernetycznego. Swoją uwagę skupiłem na USA, które dzięki obowiązywaniu od wielu lat rygorystycznych przepisów federalnych i stanowych o ochronie danych osobowych i obowiązku notyfikacji w razie incydentu *data breach*, zgromadziły największą na świecie bazę danych o tego typu zdarzeniach. Na jej podstawie przeprowadziłem wielowymiarową i wielowątkową analizę statystyczną, której wyniki dostarczyły istotnej wiedzy empirycznej na temat specyfiki tego ryzyka. Syntetycznie ujmując uzyskane wyniki można powiedzieć, że przyczyny, formy materializacji, jak i skutki ryzyka *data breach* różnią się w zależności od typu organizacji (w której dochodzi do wycieku), branży gospodarki, w której prowadzi działalność oraz lokalizacji geograficznej na terenie USA.

Artykuł [3] wypełnia lukę badawczą w zakresie definiowania ryzyka cybernetycznego i wskazania jego powiązań z innymi terminami składającymi się na szeroko pojęty konstrukt cyberryzyka. Po wykonaniu analizy porównawczej istniejących definicji ryzyka cybernetycznego i ich systematyki według autorskiej metodyki, zaproponowałem własne brzmienie kompleksowej definicji tego pojęcia. Praca ta bazuje na badaniach zawartych w monografii habilitacyjnej, dodając pewne dodatkowe elementy. Poza rozbudowaniem warstwy analitycznej, cyberryzyko zostało ukazane na tle dwóch innych pojęć, które są rozróżniane w terminologii angielskiej (*security, safety*), jednak w języku polskim mają tylko jedno brzmienie „niebezpieczeństwo". Kontekst rozważań poszerzyłem dodatkowo o bezpieczeństwo miejsca pracy w warunkach różnych zagrożeń cybernetycznych, takich jak choćby praca zdalna.

Nurt 3 – Ubezpieczenia cybernetyczne

1. **Strupczewski G.** (2017), Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie, "Finanse. Czasopismo Komitetu Nauk o Finansach PAN", ISSN: 1899-4822, Nr 1(10), s. 251-271
2. **Strupczewski G.** (2017), The cyber-insurance market in Poland and determinants of its development from the insurance brokers' perspective, "Economics and Business Review", ISSN: 2392-1641, Vol. 3(17), Nr 2, s. 33-50, DOI: 10.18559/ebr.2017.2.3
3. **Strupczewski G.** (2017), Wymogi informacyjne towarzystw ubezpieczeń w zakresie prewencji i bezpieczeństwa IT jako metoda redukcji asymetrii informacji w ubezpieczeniach cybernetycznych, [w:] Kierunki rozwoju ubezpieczeń prywatnych i publicznych, red. W. Sułkowska, M. Cycoń, Wyd. Poltext, Warszawa, s. 215-227, ISBN: 978-83-7561-808-2
4. **Strupczewski G.** (2018), Current State of the Cyber Insurance Market, [w:] Proceedings of the 10th Economics & Finance Conference, Rome, 10-13 September 2018, s. 491-501, International Institute of Social and Economic Sciences (IISES), Prague, ISBN: 978-80-87927-77-9, ISSN: 2336-6044 (indeksowane w Web of Science)

5. **Strupczewski G.** (2019), Ubezpieczenie wycieku danych osobowych a odpowiedzialność administratora danych wynikająca z RODO, [w:] O dobre prawo dla ubezpieczeń, red. E. Bagińska, W.W. Mogilski, M. Wałachowska, M.P. Ziemiak, Wyd. TNOiK w Toruniu, Toruń, s. 701-718, ISBN: 978-83-7285-841-2

Artykuł [1] stanowił pomost pomiędzy badaniami nad ryzykiem cybernetycznym a eksploracją roli ubezpieczeń w finansowaniu negatywnych jego skutków. Zaczynając od przybliżenia istoty, klasyfikacji i rozmiarów ryzyka cybernetycznego, przeszedłem do dyskusji szans i barier rozwoju rynku ubezpieczeń cybernetycznych, dzieląc je na czynniki popytowe i podażowe. Konkludując podkreśliłem istotną rolę cyberubezpieczeń nie tylko na poziomie mikro (pojedynczego przedsiębiorstwa), ale także w skali makro dla całej gospodarki narodowej.

Publikacja [2] była rezultatem własnych badań ankietowych przeprowadzonych wśród brokerów ubezpieczeniowych działających w Polsce. Dzięki pozyskanym danym, przeprowadziłem pionierską (według mojej najlepszej wiedzy) analizę polskiego rynku ubezpieczeń cybernetycznych. Skupiłem się na takich wątkach, jak percepcja cyberryzyka jako jedna z głównych determinant zakupu ubezpieczenia, indykacja najważniejszych problemów w asekuracji ryzyka cybernetycznego w ocenie brokerów ubezpieczeniowych, określenie barier popytowych i podażowych w rozwoju rynku cyberubezpieczeń w Polsce. Wyniki badań dla rynku polskiego skonfrontowałem z analogicznymi danymi dla rynku globalnego.

Rozszerzając perspektywę badawczą z lokalnej do globalnej, napisałem tekst [4] zawierający diagnozę aktualnego stanu rynku ubezpieczeń cybernetycznych, prognozę kierunków jego rozwoju oraz identyfikację wyzwań, przed którymi stoją towarzystwa ubezpieczeń funkcjonujące na tym rynku. Przedmiotem rozważań był także rynek reasekuracji ryzyka cybernetycznego oraz luka ubezpieczeniowa w zakresie cyberryzyka.

Artykuł [3] jest owocem mojego zainteresowania problemem asymetrii informacji w ubezpieczeniach cybernetycznych. Choć jest to problem znany i powszechnie występujący w ubezpieczeniach, to jednak w tej konkretnej kategorii ubezpieczeń jest on szczególnym wyzwaniem z uwagi na złożoność oceny ryzyka, jakie wnosi do portfela ubezpieczeń dany podmiot zamierzający zawrzeć umowę ubezpieczenia. Oszacowanie ekspozycji na cyberryzyko potencjalnego klienta oraz pomiar jakości wdrożonych przez niego działań prewencyjnych w zakresie cyberbezpieczeństwa nie są zadaniami trywialnymi. Przedmiotem badań były kwestionariusze oceny ryzyka stosowane przez towarzystwa ubezpieczeń w celu redukcji asymetrii informacji w ubezpieczeniach cybernetycznych. Efektem poznawczym podjętych badań była identyfikacja czynników oceny ryzyka branych pod uwagę przez ubezpieczycieli przy underwritingu ryzyka cybernetycznego, a ponadto wskazanie różnic pomiędzy kwestionariuszami oceny ryzyka stosowanymi przez zakłady ubezpieczeń oferujące cyberubezpieczenia w Polsce.

Tekst [5] wynika ze szczególnego zainteresowania ryzykiem wycieku danych osobowych i poszukiwaniem odpowiedzi na pytanie, w jaki sposób oferta ubezpieczycieli działających w Polsce zapewnia ochronę przed tego typu zdarzeniami. Pogłębiona analiza porównawcza ogólnych warunków ubezpieczeń cybernetycznych oferujących ochronę w zakresie odpowiedzialności za naruszenie bezpieczeństwa danych osobowych pozwoliła mi wychwycić podobieństwa i różnice w dostępnej ofercie rynkowej, a także ocenić adekwatność oferowanego pokrycia ubezpieczeniowego do przepisów RODO.

Nurt 4 – Rola państwa w rynku ubezpieczeń cybernetycznych

1. **Strupczewski G.** (2016), Wpływ ustawodawstwa amerykańskiego na rozwój rynku ubezpieczeń cybernetycznych w USA, "Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie", ISSN: 1898-6447, Nr 10(958), s. 81-99, DOI: 10.15678/ZNUEK.2016.0958.1006
2. **Strupczewski G.** (2019), Źródła cyberprzestępczości w systemie pracowniczych planów kapitałowych i rozwiązania minimalizujące jej negatywny wpływ, [w:] Rynek ubezpieczeniowy : zapobieganie przyczynom przestępczości, red. M. Płonka, B. Oręziak, M. Wielec, Wyd. Instytut Wymiaru Sprawiedliwości, Warszawa, s. 75-107, ISBN: 978-83-6634-407-5
3. **Strupczewski G.** (2020), Cyberterroryzm jako nowe wyzwanie dla branży ubezpieczeń w Polsce: Koncepcja finansowania ryzyka cyberterroryzmu w formie partnerstwa publiczno-prywatnego państwa i sektora ubezpieczeń, [w:] Możliwe przyczyny i rodzaje przestępczości w przyszłości oraz przygotowania prewencyjne, red. R. Koszewski, B. Oręziak, M. Wielec, Wyd. Instytut Wymiaru Sprawiedliwości, Warszawa, s. 195-219, ISBN: 978-83-66344-10-5

Rozważania prowadzone w trzecim nurcie badawczym uświadomiły mi, jak istotny wpływ na tempo rozwoju rynku ubezpieczeń cybernetycznych może mieć państwo, a zwłaszcza tworzone przez nie regulacje. Wzmożone zainteresowanie cyberubezpieczeniami w Europie po wejściu w życie RODO w 2018 r. jest tego znamiennym przykładem. Jednak podobne w swym charakterze regulacje prawne zostały wprowadzone w USA już kilkanaście lat wcześniej. To skłoniło mnie do podjęcia badań nad rolą regulacji prawnych w stymulowaniu popytu na cyberubezpieczenia na przykładzie doświadczeń USA. Artykuł [1] prezentuje pogłębioną analizę komparatywną prawodawstwa amerykańskiego (w szczególności prawa stanowego) w zakresie odpowiedzialności za naruszenie bezpieczeństwa danych osobowych. W rezultacie przeprowadzonych badań wykazałem wyraźny wpływ regulacji stanowych i federalnych wprowadzających obowiązek notyfikacji o wycieku danych osobowych na tempo wzrostu rynku ubezpieczeń cybernetycznych w USA.

Masowość pracowniczych planów kapitałowych (PPK), wysoka wartość zarządzanych środków, cyfryzacja obsługi PPK sprawiają, że są one w znacznym stopniu narażone na problem cyberprzestępczości. Warto zatem zbudować wokół PPK skuteczny ekosystem cyberbezpieczeństwa, w który zaangażowane będą instytucje finansowe zarządzające PPK, oszczędzający i inni interesariusze. W pracy [2] przedstawiłem własne propozycje rozwiązań mających na celu minimalizację ryzyka cyberprzestępczości w PPK. Zarekomendowałem włączenie instytucji finansowych zarządzających PPK do krajowego systemu cyberbezpieczeństwa, ustanowienie certyfikowanej polityki zarządzania bezpieczeństwem informacji przez pracodawców, budowanie świadomości cyberzagrożeń przez edukację, stosowanie biometrii behawioralnej do uwierzytelniania użytkowników PPK.

Rozwijając wątek możliwej roli państwa w rynku ubezpieczeń cybernetycznych, skupiłem swoją uwagę na ryzyku cyberterroryzmu, postrzegając je jako poważne wyzwanie dla branży ubezpieczeń, a jednocześnie pole możliwego zaangażowania państwa w formie partnerstwa publiczno-prywatnego (PPP). W pracy [3] zaprezentowałem autorską koncepcję finansowania ryzyka cyberterroryzmu w formie PPP pomiędzy państwem a branżą ubezpieczeń w Polsce. Koncepcja ta została później rozwinięta i doprecyzowana w monografii habilitacyjnej. W omawianej publikacji poruszyłem też istotne dla cyberbezpieczeństwa

narodowego zagadnienia istoty, przyczyn i skali problemu cyberterroryzmu. Następnie podjąłem dyskurs nad problematyczną ubezpieczalnością tego ryzyka i omówiłem różne formy zaangażowania państwa w rynek ubezpieczeń.

Rozproszona tematyka prac opublikowanych przed uzyskaniem stopnia doktora świadczy o poszukiwaniu obszaru badawczego[1]. W obszarze moich zainteresowań była teoria ryzyka ubezpieczeniowego i zarządzanie ryzykiem. W szczególności przedmiotem moich badań było zarządzanie ryzykiem katastrof naturalnych i rola ubezpieczeń w tym procesie. Jeden z artykułów poświęciłem kapitałom własnym zakładów ubezpieczeń. W badaniach prowadzonych przed doktoratem analizowałem też i poddałem ocenie rynek gwarancji ubezpieczeniowych w Polsce. Ostatecznie swoje zainteresowania skierowałem w stronę zarządzania ryzykiem powodzi jako najpoważniejszego ryzyka katastrofy naturalnej w Polsce, czego efektem była rozprawa doktorska.

4.3. Synteza aktywności naukowej realizowanej we współpracy z krajowymi i zagranicznymi uczelniami

Za swoje **najistotniejsze osiągnięcie na polu współpracy międzynarodowej** uznaję zaangażowanie w działalność sieci naukowo-badawczej European Risk Research Network (ERRN)[2], do której dołączyłem w 2016 r. Dotychczasowe zaangażowanie w działalność sieci przyniosło mi wiele satysfakcji, wynikającej głównie z możliwości współpracy oraz konsultacji zamierzeń badawczych z uznanymi naukowcami zajmującymi się szeroko pojętą problematyką ryzyka i zarządzaniem ryzykiem. W uznaniu dotychczasowego zaangażowania w prace ERRN, w połowie 2020 r. Koordynator sieci powierzył mi zadanie zbudowania międzynarodowego zespołu badawczego i przygotowanie wstępnej koncepcji badań pod roboczym tytułem *„Valuation of the personal data of Internet users and demand for identity theft insurance"*. Do współpracy w ramach projektu pozyskałem partnerów m.in. z: Glasgow Caledonian University London (Wlk. Brytania), Federico II University of Naples (Włochy), ISCTE Business School in Lisbon (Portugalia), Moorhouse Risk Management Consulting (Kanada). Dodatkowo zgłosiłem propozycję zorganizowania kolejnej, cyklicznej konferencji naukowej sieci ERRN na terenie Uniwersytetu Ekonomicznego w Krakowie, jednocześnie deklarując chęć podjęcia się funkcji przewodniczącego komitetu organizacyjnego konferencji. Oferta ta spotkała się z pozytywną reakcją Komitetu Sterującego ERRN, który decyzją z dnia 22 stycznia 2021 r. powierzył mi funkcję organizatora konferencji (*ERRN local organizer*) we wrześniu 2022 roku.

[1] Wykaz prac opublikowanych przed uzyskaniem stopnia doktora znajduje się w punktach II.2.2 i II.4.2 Załącznika nr 5.
[2] Szersza informacja na temat sieci ERRN została zawarta w pkt. 10 załącznika nr 5.

Po obronie pracy doktorskiej uczestniczyłem w dwóch stażach realizowanych poza macierzystą uczelnią, w tym jednym zagranicznym:

- 6 miesięczny staż naukowy w Katedrze Systemu Finansowego Kolegium Zarządzania i Finansów Szkoły Głównej Handlowej w Warszawie. Celem stażu było wzmocnienie kontaktów naukowych, doskonalenie warsztatu badawczego, wymiana doświadczeń naukowych i transfer wiedzy, a także gromadzenie materiałów do monografii habilitacyjnej. Podczas stażu prowadziłem badania naukowe pt. „Zarządzanie ryzykiem cybernetycznym ze szczególnym uwzględnieniem ubezpieczeń".
- tygodniowy zagraniczny staż w Lizbonie na ICSTE-Business School Instituto Universitario de Lisboa. Oprócz celu dydaktycznego związanego z prowadzeniem zajęć w ramach programu Erasmus+ KA103, wyjazd miał również charakter naukowy. Uczelnia goszcząca zorganizowała w tym czasie „Exchange Week for Foreign Visiting Professors", w którym wzięło udział ponad 20 pracowników naukowych z uczelni europejskich. Uczestnictwo w tym wydarzeniu umożliwiło mi: nawiązanie kontaktów naukowych, zapoznanie się z tematyką badań uczestników stażu, udział w seminariach naukowych, prezentację własnych kierunków badawczych i dyskusję nad nimi.

Na forum międzynarodowym aktywnie popularyzuję wyniki prowadzonych badań naukowych, co potwierdza udział w licznych konferencjach krajowych i zagranicznych:

- Przed uzyskaniem stopnia doktora czynnie uczestniczyłem w 7 konferencjach naukowych - 2 krajowych i 5 międzynarodowych, przy czym 1 konferencja międzynarodowa odbyła się poza granicami kraju. Na każdej z tych konferencji wygłosiłem referat.
- Po uzyskaniu stopnia doktora czynnie uczestniczyłem w 29 konferencjach naukowych, w tym 7 krajowych i 22 międzynarodowych, przy czym 5 konferencji międzynarodowych odbywało się poza granicami kraju. Na konferencjach tych wygłosiłem łącznie 26 referatów.
- Dwukrotnie przewodniczyłem sesji tematycznej konferencji, a raz miałem przyjemność wygłosić referat jako gość honorowy na sesji plenarnej konferencji.

Duży wpływ na mój rozwój naukowy i doskonalenie warsztatu badacza miał udział w pracach zespołów badawczych realizujących różne projekty naukowe:

- W okresie po uzyskaniu stopnia doktora brałem udział w 12 projektach realizowanych w ramach utrzymania potencjału badawczego uczelni, zaś przed doktoratem - w 6 projektach badawczych tego typu.
- Trzy projekty, w których obecnie biorę udział, realizowane są w ramach współpracy między naukowcami z różnych uczelni krajowych, z czego dwa pod moim kierunkiem. Ponadto w trakcie przygotowań jest jeden projekt w ramach współpracy międzynarodowej, który będzie realizowany pod moim kierownictwem.

- Aktualnie uczestniczę w realizacji dwóch projektów naukowych finansowanych przez MEiN (dawne MNiSW) w trybie konkursowym: w projekcie pt. „Zintegrowane narzędzie wspomagania zarządzania ryzykiem cybernetycznym w przedsiębiorstwie" pełnię funkcję kierownika zespołu badaczy z różnych uczelni krajowych, zaś w projekcie pt. „Społeczno-gospodarcze konsekwencje czwartej rewolucji przemysłowej" jestem wykonawcą.
- W 2019 r. brałem udział (jako wykonawca) w pracach zespołu badawczego w 2 odrębnych modułach projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości". Projekt realizowany był przez Instytut Wymiaru Sprawiedliwości przy współpracy z Harvard Business School, SRI International i Massachusetts Institute of Technology, finansowany ze środków Funduszu Sprawiedliwości w Ministerstwie Sprawiedliwości RP. Efektem projektu jest seria publikacji monograficznych, w których jestem autorem dwóch rozdziałów.

Ponadto chciałbym zwrócić uwagę na inne osiągnięcia naukowo-badawcze:

- **Otrzymane nagrody i wyróżnienia**: otrzymałem łącznie 8 nagród za działalność naukowo-badawczą: 6 Nagród Rektora UEK (z czego 5 to nagrody indywidualne) oraz 2-krotnie byłem laureatem nagród przyznawanych przez instytucje związane z rynkiem ubezpieczeń (Rzecznik Finansowy, Izba Gospodarcza Ubezpieczeń i Obsługi Ryzyka).
- **Członkostwo w międzynarodowych organizacjach i towarzystwach naukowych**: jestem członkiem 6 takich organizacji; udział w tych organizacjach traktuję jako ważny element własnego rozwoju naukowego oraz wkład w aktywizowanie środowiska i podtrzymanie struktur dynamizujących wymianę myśli naukowej i współpracę badawczą.
- **Organizacja międzynarodowych konferencji naukowych:** przed doktoratem trzykrotnie przewodniczyłem komitetowi organizacyjnemu międzynarodowych konferencji naukowych, zaś po uzyskaniu stopnia doktora – ośmiokrotnie uczestniczyłem w organizacji międzynarodowych konferencji naukowych, w tym 5 razy moja rola polegała na koordynacji i prowadzeniu prac zmierzających do przygotowania publikacji konferencyjnej, co traktuję jako wyróżnienie i jednocześnie szczególnie odpowiedzialne zadanie.

Szczegółowy wykaz moich osiągnięć naukowo-badawczych zaprezentowałem w załączniku 5 do niniejszego wniosku.

5. Informacja o osiągnięciach dydaktycznych i sprawowanej opiece naukowej, działalności organizacyjnej oraz popularyzującej naukę

Moje **osiągnięcia dydaktyczne** po uzyskaniu stopnia doktora nauk ekonomicznych obejmują następujące obszary:

- Prowadzę zajęcia dydaktyczne w formie wykładów i ćwiczeń (w większości autorskich) na studiach stacjonarnych i niestacjonarnych, w tym przedmiot anglojęzyczny *Insurance* w wymiarze 15 godz. Tematyka moich zajęć obejmuje cyberbezpieczeństwo, ubezpieczenia, teorię ryzyka i zarządzanie ryzykiem. Opierając się na wynikach ankiet studentów mogę stwierdzić, że prowadzone przeze mnie zajęcia są oceniane wysoko (w najnowszym badaniu ogólnouczelnianym wykonanym w czerwcu 2020 r. uzyskałem ogólną ocenę zajęć dydaktycznych 5,25, gdzie 5,0 oznacza ocenę bardzo dobrą, a 5,5 ocenę celującą). Traktuję to jako źródło satysfakcji zawodowej i motywację do ciągłego podnoszenia jakości moich zajęć.
- Jestem promotorem 40 prac dyplomowych i 19 magisterskich. Wykonałem recenzje 23 prac dyplomowych i 10 prac magisterskich. Za szczególne osiągnięcie uważam promotorstwo pracy licencjackiej pt. „Ubezpieczenia cybernetyczne", która zajęła 2. miejsce w I edycji Konkursu o Nagrodę Rzecznika Finansowego za najlepszą pracę doktorską, magisterską, licencjacką i podyplomową z zakresu ochrony klienta na rynku finansowym w 2018 r.
- Pełniłem funkcję promotora pomocniczego w jednym przewodzie doktorskim. Rozprawa doktorska autorstwa Pana Tomasza Jedynaka pt. "Efektywność i ryzyko funduszy inwestycji społecznie odpowiedzialnych", przygotowana w Katedrze Zarządzania Ryzykiem i Ubezpieczeń na Wydziale Finansów Uniwersytetu Ekonomicznego w Krakowie, została obroniona z wyróżnieniem w czerwcu 2015 r. Jej promotorem była Pani Prof. ucz. dr hab. Teresa Tatiana Czerwińska (Uniwersytet Warszawski). Praca ta zdobyła pierwsze miejsce w konkursie o Nagrodę Prezesa Zarządu GPW SA.
- Angażuję się w programy międzynarodowe w obszarze dydaktyki:
    - Zakwalifikowanie się do programu Erasmus+ KA107 dającego możliwość wyjazdu do Tashkent Institute of Finance (Uzbekistan) w celu wygłoszenia wykładu gościnnego nt *„Cyber risk management"* (2020). Z powodu pandemii Covid-19 realizacja zajęć została przełożona na termin późniejszy.
    - Koordynacja przyjazdu i opieka nad Panią dr Silvia Panfilo, PhD (Ca' Foscari University of Venice) goszczącą na UEK w ramach programu Erasmus +/KA1 Staff Mobility for Teaching Assignment (2019).

- Przeprowadzenie zajęć dydaktycznych po angielsku nt *„Non-life insurance for corporations – practical applications"* na ICSTE-Business School w Lizbonie w ramach programu Erasmus+ KA103 dla nauczycieli akademickich (2017).
- Przeprowadzenie zajęć dydaktycznych po angielsku nt *„Natural disaster insurance"* na EAE Business School w Barcelonie w ramach programu Erasmus+ dla nauczycieli akademickich (2012).
- Regularne prowadzenie zajęć po angielsku z przedmiotu "*Insurance*" na specjalności Corporate Finance (Instytut Finansów UEK) dla studentów przebywających na UEK w ramach programu Erasmus (2012-nadal).

- Jestem współautorem 4 ogólnopolskich podręczników z zakresu ubezpieczeń:
  - *Ubezpieczenia*, red. W. Ronka-Chmielowiec, Wyd. C.H. Beck, Warszawa 2016, ISBN: 978-83-255-6078-2,
  - *System ubezpieczeń społecznych*, red. W. Sułkowska, Wyd. Uniwersytetu Ekonomicznego w Krakowie, Kraków 2014, ISBN: 978-83-7252-674-8,
  - *Współczesne ubezpieczenia gospodarcze*, red. W. Sułkowska, Wyd. Uniwersytetu Ekonomicznego w Krakowie, Kraków 2013, ISBN: 978-83-7252-631-1,
  - *Ubezpieczenia*, red. W. Sułkowska, Wyd. Akademii Ekonomicznej w Krakowie, Kraków 2007, ISBN: 978-83-7252-334-1.
- W latach 2015-2020 czterokrotnie brałem czynny udział w krajowych projektach dydaktycznych angażujących studentów z Koła Naukowego Ubezpieczeń „Risk Management" w prowadzenie własnych badań naukowych, wygłoszenie wystąpień na konferencji naukowej oraz wydanie wspólnej monografii naukowej. W projektach tych moja rola polegała na opiece naukowej nad studentami oraz redakcji naukowej monografii studenckiej.
- Na studiach podyplomowych z obszaru bankowości prowadziłem wykłady o tematyce cyberbezpieczeństwa instytucji finansowych oraz ubezpieczeń.
- Dążę do podnoszenia jakości prowadzonych zajęć i wprowadzania nowych metod nauczania poprzez udział w ogólnopolskich konferencjach dydaktycznych. W okresie 2011-2020 uczestniczyłem w 7 takich konferencjach (m.in. w Kongresach Rozwoju Edukacji).

Aktywnie angażuję się w **działalność organizacyjną** na Uniwersytecie Ekonomicznym w Krakowie. Do najważniejszych dokonań w tym obszarze zaliczam:

- Praca w zespołach roboczych i organach kolegialnych UEK. W kadencji 2020-2024 zostałem powołany do: Rady Centrum Językowego UEK, Rady Instytutu Finansów, Zespołu programowo-dydaktycznego ds. kierunku Bankowość i Zarządzanie Ryzykiem w Instytucie Finansów, Zespołu programowo-dydaktycznego ds. kierunku Finanse i Rachunkowość w Instytucie Finansów, Zespołu ds. Ewaluacji Dyscypliny Ekonomia i Finanse powołanego przez Dziekana Kolegium Ekonomii, Finansów i Prawa UEK. W

latach wcześniejszych byłem członkiem m.in. Rady Wydziału Finansów i Prawa oraz Uczelnianego Kolegium Elektorów w wyborach Rektora (dwukrotnie).

- Pełnienie funkcji Sekretarza Komitetu Redakcyjnego Zeszytów Naukowych Uniwersytetu Ekonomicznego w Krakowie (ISSN: 1898-6447) w latach 2009-2018. Do moich zadań należała organizacja pracy Komitetu Redakcyjnego ZN UEK oraz koordynacja procesu wydawniczego od strony administracyjnej i merytorycznej.
- W okresie przed doktoratem trzykrotnie przewodniczyłem organizacji międzynarodowych konferencji naukowych, zaś w okresie po doktoracie – ośmiokrotnie uczestniczyłem w organizacji międzynarodowych konferencji naukowych (szczegóły można znaleźć w pkt . 8 Wykazu osiągnięć naukowych).

W ramach działalności **popularyzującej naukę** chciałbym wymienić następujące aktywności:

- Realizacja autorskiego pomysłu napisania, wspólnie z moimi studentami uczestniczącymi w zajęciach z cyberbezpieczeństwa, „Leksykonu zagrożeń cybernetycznych" – publikacji popularno-naukowej o charakterze encyklopedycznym, która będzie dostępna na niżej wymienionym blogu, a w dalszej perspektywie – wydana jako e-book.
- Prowadzenie (od grudnia 2019 r.) autorskiego bloga pt. „Ryzyko cybernetyczne. Merytorycznie o cyberbezpieczeństwie" poświęconego tematyce cyberbezpieczeństwa, zagrożeniom cybernetycznym i ubezpieczeniom cybernetycznym (http://cyber.uek.krakow.pl).
- Wywiad ekspercki dla tygodnika Gazeta Finansowa (ISSN 1734-8900) Nr 16 z 15-21 kwietnia 2016 r. na temat ubezpieczenia środków obrotowych firmy.

6. Współpraca z otoczeniem gospodarczym

Moje doświadczenia w zakresie współpracy z otoczeniem gospodarczym związane są z wykonywaniem zadań brokera ubezpieczeniowego. W 2011 r. zdałem egzamin brokerski przed Komisją Egzaminacyjną dla Brokerów Ubezpieczeniowych i Reasekuracyjnych w Warszawie. Uzyskanie uprawnień zawodowych pozwoliło mi na nawiązanie współpracy z polskim oddziałem międzynarodowej firmy brokerskiej Marsh Polska Sp. z o.o. Współpraca ta polegała na wykonywaniu zadań brokera ubezpieczeniowego, w okresach lipiec-październik 2012 oraz kwiecień-wrzesień 2013. To doświadczenie pozwoliło mi poznać praktyczne aspekty rynku ubezpieczeń gospodarczych i funkcjonowanie różnych rodzajów ubezpieczeń

korporacyjnych, co przełożyło się na dostarczenie inspiracji do badań naukowych i podniesienie jakości dydaktyki.

W 2016 r. nawiązałem współpracę ze Stowarzyszeniem Brokerów Ubezpieczeniowych i Reasekuracyjnych "Polbrokers", której celem była realizacja badań rynku ubezpieczeń cybernetycznych w Polsce poprzez badania ankietowe wśród brokerów ubezpieczeniowych zrzeszonych w tej organizacji. Uzyskane wyniki badań zostały zaprezentowane na międzynarodowej konferencji w Yorku (7th ERRN European Risk Conference Multiple Perspectives on Risk Management, 15-16.09.2016 r.) oraz opublikowane w czasopiśmie naukowym (Strupczewski G. (2017), *The cyber-insurance market in Poland and determinants of its development from the insurance brokers' perspective*, "Economics and Business Review", ISSN: 2392-1641, Vol. 3(17), Nr 2, s. 33-50).

Ostatecznie w roku 2017 r. podjąłem decyzję o rezygnacji z dalszej aktywności zawodowej na rzecz realizowania wyłącznie działalności naukowo-badawczej.

7. Literatura przywołana w autoreferacie

Allianz Risk Barometer. Top Business Risks for 2019 (2019), Allianz Global Corporate & Specialty (AGCS), styczeń, Monachium, https://www.agcs.allianz.com/assets/PDFs/Reports/ /Allianz_Risk_Barometer_2019.pdf (dostęp: 4.02.2019).

Eling M., Wirfs J.H. (2019), *What are the Actual Costs of Cyber Risk Events?*, „European Journal of Operational Research", vol. 272(3), s. 1109–1119, DOI: 10.1016/j.ejor.2018.07.021.

The Global Risks Report 2019 (2019), 14. ed, World Economic Forum (WEF), https://www.weforum.org/reports/the-global-risks-report-2019 (dostęp: 2.02.2019).

Grzegorz Strupczewski

(podpis wnioskodawcy)