SGH Kolegium Gospodarki Światowej

Warszawa, 15.12. 2024

Dr hab. Halina Brdulak, prof. SGH
Katedra Zarządzania Międzynarodowego
Kolegium Gospodarki Światowej
Szkoła Główna Handlowa w Warszawie

Recenzja rozprawy doktorskiej mgra Marca Wilczka "Decision-Making under Constraints: A Behavioral Economics Perspective on Cyber-Related Heuristics and Biases" przygotowanej pod kierunkiem naukowym dr hab. profesor UG Moniki Bąk

Ustalenia formalne

Podstawą opracowania recenzji jest pismo z dnia 17.10.2024 r. od Przewodniczącego Rady Dyscypliny Ekonomia i Finanse Uniwersytetu Gdańskiego, dr hab. Leszka Czerwonki, prof. UG, informujące o powołaniu mnie przez Radę Dyscypliny Ekonomia i Finanse Uniwersytetu Gdańskiego na recenzentkę rozprawy doktorskiej pana mgra Marca Wilczka pt. "Decision-Making under Constraints: A Behavioral Economics Perspective on Cyber-Related Heuristics and Biases" w dziedzinie nauk społecznych, dyscyplinie naukowej: ekonomia i finanse. Pismo otrzymałam w dniu 21.10.2024 r. drogą elektroniczną na adres e-mailowy. Funkcję promotorki niniejszej rozprawy pełni dr hab. prof. UG Monika Bąk.

Podstawą formalno-prawną oceny są wymagania określone w art. 187 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2022 r., poz. 574 z późn. zm.) w którym stwierdzono m.in., że

- rozprawa doktorska powinna reprezentować ogólną wiedzę teoretyczną kandydata w dyscyplinie oraz umiejętność samodzielnego prowadzenia pracy naukowej,

- przedmiotem rozprawy doktorskiej powinno być oryginalne rozwiązanie problemu naukowego, oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej lub społecznej,

- rozprawę doktorską może stanowić praca pisemna, w tym monografia naukowa, zbiór opublikowanych i powiązanych tematycznie artykułów naukowych, praca projektowa, a także samodzielna i wyodrębniona część pracy zbiorowej.

Mając na uwadze powyższe kwestie w oparciu o przeprowadzoną poniżej analizę, stwierdzam, że przedstawiona rozprawa doktorska mgra Marca Wilczka pt. "Decision-Making under Constraints: A Behavioral Economics Perspective on Cyber-Related Heuristics and Biases", przygotowana pod kierunkiem dr hab. prof. UG Moniki Bąk stanowi oryginalne rozwiązanie problemu naukowego w oparciu o przeprowadzone badania. Jednocześnie stwierdzam, iż doktorant posiada nie tylko ogólną wiedzą teoretyczną wymaganą w dyscyplinie ekonomia i finanse ale również potrafi dokonywać samodzielnie analiz i syntezy powyższej wiedzy. Tym samym potwierdzam, że recenzowana rozprawa spełnia kryteria ustawowe, wymagane dla prac doktorskich.

Uwagi ogólne

Praca składa się z 6 rozdziałów, 8 załączników i liczy 297 stron. Spis źródeł jest imponujący i zajmuje 52 strony. Są to przede wszystkim artykuły, w znaczącej liczbie z ostatnich lat. Dla ilustracji i zarazem syntetycznego ujęcia przekazywanych treści wykorzystano 16 tabel i 19 rysunków. W załącznikach znalazło się 8 kwestionariuszy, które autor wykorzystał w przeprowadzonych badaniach. Uzupełnieniem o dużym znaczeniu merytorycznym jest słownik wyrażeń i skrótów, użytych w pracy.

W rozdziale I, zatytułowanym jako Wprowadzenie autor przedstawia swoją motywację przy podjęciu się niniejszego tematu, w kontekście wzrastającego cyberzagrożenia. Jak wynika z analiz, przytoczonych przez autora mimo, że przedsiębiorstwa coraz więcej inwestują w ochronę przed atakami to poziom zagrożenia nadal rośnie. Głównym czynnikiem są nawyki i uprzedzenia osób, pracujących w organizacji. Zachowania właśnie

tych osób, nie zawsze uświadomione, stanowią niebezpieczeństwo dla środowiska IT, w którym funkcjonują. Liczba incydentów w tym zakresie, spowodowanych błędem człowieka rośnie dynamicznie i niekiedy już osiąga prawie 90 %. W oparciu o przegląd literatury autor zidentyfikował aż 17 czynników, wynikających z zachowań ludzi, które mogą mieć wpływ na bezpieczeństwo cyfrowe. Osoby młodsze, które od urodzenia są wychowane w środowisku cyfrowym, określane jako digital native, są w większym stopniu podatne na ataki cyfrowe, co wprost skorelowane jest z czasem, które spędzają w internecie. Po drugiej stronie są osoby starsze, w wieku 65 i więcej, które bardziej świadomie korzystają z Internetu.

Celem niniejszej dysertacji, jak wskazał autor w p.1.1 jest „ zbadanie skali zniekształceń poznawczych i ich roli w promowaniu błędnych osądów wśród specjalistów od cyberbezpieczeństwa." Tak sformułowany cel został doprecyzowany w dalszej części rozdziału: „ zbadanie wyzwań i ograniczeń w procesach podejmowania decyzji strategicznych związanych z cyberprzestrzenią, szczególnie w warunkach ograniczonej racjonalności". Autor dodał również, że analiza jest prowadzona w oparciu o założenia ekonomii behawioralnej, z uwzględnieniem błędów poznawczych i heurystyk. Został również sformułowany cel aplikacyjny dysertacji – wsparcie organizacji w zmniejszaniu ich narażenia na cyberzagrożenia i zwalczaniu rosnącego zagrożenia cyberprzestępczością. W związku z tak sformułowanym celem autor komunikuje, że jego dociekania badawcze są skoncentrowane na poszukiwaniu sposób ograniczenie lub przeciwdziałania wpływowi uprzedzeń poznawczych na strategiczne podejmowanie decyzji w zakresie cyberbezpieczeństwa. Sprowadza się to również do badania wpływu emocji i heurystyk na proces podejmowania decyzji.

W związku z tak określonym celem głównym zostały sformułowane przez autora następujące cele badawcze:

- zbadanie znaczenia uprzedzeń i heurystyk wpływających na strategiczne podejmowanie decyzji w zakresie cyberbezpieczeństwa przez specjalistów IT i ekspertów ds. cyberbezpieczeństwa w średnich i dużych przedsiębiorstwach w Niemczech, Austrii i Szwajcarii;

- ocena w jaki sposób uprzedzenia poznawcze, takie jak optymizm, nadmierna pewność siebie i heurystyka dostępności, prowadzą do zniekształceń w ocenie zagrożeń cybernetycznych, wdrażaniu zabezpieczeń i łagodzeniu cyberataków;

- zbadanie pojawiania się cyberprzestępczości, w tym elementów pomocniczych i podmiotów stanowiących zagrożenie, które zaostrzają sytuację i ostatecznie narażają organizacje na zagrożenia cybernetyczne;

- zbadanie i kontekstualizacja krajobrazu cyberzagrożeń oraz zilustrowanie ekonomicznych konsekwencji błędnego podejmowania decyzji;

- wypełnienie luki teoretycznej w istniejącej literaturze w odniesieniu do uprzedzeń związanych z cyberbezpieczeństwem;

- sformułowanie praktycznych porad dla przedsiębiorców dotyczących działań, które można podjąć w celu zmniejszenia narażenia organizacji na ryzyko cybernetyczne.

Cele badawcze posłużyły do sformułowania 3 pytań badawczych:

1. Jakie błędy poznawcze utrudniają podejmowanie decyzji ekspertom w danej dziedzinie i wpływają na skuteczność środków zaradczych w zakresie cyberbezpieczeństwa?

2. Jakie czynniki stoją za rozprzestrzenianiem się zagrożeń cybernetycznych i w jaki sposób błędy poznawcze kształtują skuteczność środków zaradczych w zmieniającym się krajobrazie cyberprzestępczości?

3. Dlaczego skutki ekonomiczne incydentów cyberbezpieczeństwa są niedoceniane z powodu błędów poznawczych i jakie są szersze implikacje dla przedsiębiorstw i odporności społeczeństwa?

W dysertacji wskazano również, w których rozdziałach znalazły się odpowiedzi na powyższe pytania. Do weryfikacji tak postawionych pytań wykorzystano ilościowe i jakościowe metody badawcze. Oprócz krytycznej analizy literatury, przeprowadzono wywiady z ekspertami, które pozwoliły autorowi na zawężenie problematyki do trzech głównych wzorców — heurystyki dostępności, optymizmu i nadmiernej pewności siebie. Faza ilościowa obejmowała opracowanie kwestionariusza, którego odpowiedzi poddano analizie przy użyciu modelowania równań strukturalnych (SEM) i oprogramowania SPSS.

Układ rozdziałów został w sposób przejrzysty przedstawiony w tabeli nr 2.

Konstrukcja pracy jest logiczna, cele badawcze zostały ujęte w 3 pytaniach badawczych. Temat, sformułowany przez doktoranta, jest aktualny i nabiera coraz większego znaczenia w kontekście postępującej cyfryzacji gospodarki i transformacji cyfrowej przedsiębiorstw. Podatność na zagrożenia wzrasta ponieważ cyberprzestępcy w coraz większym stopniu

wykorzystają wiedzę z zakresu socjologii i psychologii, podobnie jak to się dzieje w świecie realnym. Jednak w przypadku cyberświata możliwości działania rozciągają się na skalę globalną, ponieważ nie ograniczają je granice państw. Dodatkowo gospodarka oparta na nieustannym wzroście, prowadzi do wypaczeń i chciwości, o czym pisał również Sedlacek (T. Sedlacek, Ekonomia dobra i zła, 2012) czy Zuboff (S.Zuboff, Wiek kapitalizmu inwiligacji, 2020). Dlatego też podjęty przez doktoranta temat należy uznać za bardzo ważny, wpisujący się w nurt najnowszych badań.

Stylistyka oraz język rozprawy należy uznać za prawidłowe.

Uwagi szczegółowe

W rozdziale pierwszym autor przedstawia przegląd sytuacji w układzie dynamicznym w zakresie wykorzystania Internetu na świecie. Dokonuje także identyfikacji kluczowych ryzyk globalnych, wymienianych w raporcie WEF, wśród których zagrożenie cyberatakiem znalazło się na pozycji 8. Warte zauważenia są interesujące wnioski wynikające z przeglądu literatury, dokonanego przez doktoranta. To, że wzrost narażenia na cyberataki związany jest z rozpowszechnieniem się i dynamicznym rozwojem nowych technologii w wyniku pandemii nie jest zaskoczeniem. Jednak przestrzeń internetowa sprzyja również „rozdwojeniu" osobowości a działania w świecie realnym rządzą się innymi prawami niż w świecie wirtualnym. Osoby uczciwe nagle zmieniają swoje zachowania i stają się przestępcami w Internecie. Cyberprzestępczość stymulowana jest też przez zwiększoną dostępność Internetu i nie hamuje jej wyższe wykształcenie czy wysokość dochodów, a wręcz niekiedy przyspiesza.

Kolejne rozdziały mają na celu połączenie teorii i praktyki w celu dokonania diagnozy w zakresie oddziaływania uprzedzeń oraz nadmiernego optymizmu pracowników na poziom ryzyka odnośnie do bezpieczeństwa cyfrowego.

I tak w rozdziale trzecim autor skoncentrował się na przeglądzie literatury i teoretycznym podejściu do cyberbezpieczeństwa, uwzględniając aspekty technologiczne. Istotnym elementem jest pokazanie zasad działania „czarnych rynków" i wyzwań, przed jakimi stoją organy ścigania. W kolejnym rozdziale scharakteryzowano środowisko hakerów i ich motywacje, bazując na analizach wynikających z ekonomii behawioralnej. W tej części wskazano również złożoność ekosystemu cyberprzestępczości i kluczowe czynniki, oddziałowujące na utrzymanie i rozwój tego systemu. Konsekwencją powyższych rozważań jest analiza podwójnej roli technologii cyfrowej w umożliwianiu

cyberprzestępczości jak też w zwiększaniu podatności. Spirala, która wiąże postęp technologiczny z rozwojem cyberprzestępczości, wydaje się nie mieć końca. Coraz większe uzależnienie gospodarki od wykorzystania nowych technologii, połączone z wzrastającą liczbą obszarów, objętych cyfryzacją, powoduje, że również poszerza się pojęcie infrastruktury krytycznej. Tak więc celem tej części jest pokazanie holistycznego rozumienia ekosystemu cyberbezpieczeństwa. W końcowej części autor analizuje skuteczność obecnych środków zaradczych, minimalizujących ryzyko cyberataku. Wskazuje również na niedocenianie błędów poznawczych, takich jak heurystyka dostępności, nadmierna pewność siebie i błąd optymizmu, które w istotnym sposób obniżają skuteczność zastosowanych strategii obrony przed cyberatakiem.

Poniżej chciałam się odnieść do poszczególnych rozdziałów, wskazując na istotne elementy, które uzasadniają mój ostateczny wniosek.

W rozdziale drugim autor skupia się na wyjaśnieniu swojego podejścia, bazującego na ekonomii behawioralnej. Omawia również założenia poszczególnych nurtów ekonomicznych, które w większym stopniu (jak ekonomia klasyczna) lub też już w nieco mniejszym (jak ekonomia neoklasyczna) bazowały na założeniach o racjonalności wyborów człowieka oraz użyteczności krańcowej. Omawia również założenia ekonomii instytucjonalnej i nowej ekonomii instytucjonalnej, wskazując na różnice między powyższymi podejściami. Rola szeroko rozumianych instytucji i oddziaływania ich na funkcjonowanie jednostki, przy uwzględnieniu kosztów transakcyjnych stanowi podstawę tej części pracy. Kolejnym etapem rozwoju podejścia ekonomicznego może być ekonomia neoinstytucjonalna. Dyskusje w rozwijających się nadal nurtach ekonomicznych w dużej mierze koncentrują się wokół pojęcia i znaczenia racjonalności w wyborach ludzi. Pytanie czy jednostki działają jako homo economicus, rozumiany jako racjonalny agent, kierujący się własnym interesem i dążący do maksymalizacji swoich preferencji, co oznacza „optymalizację" decyzji stanowi podstawę ekonomii neoistytucjonalnej. Ekonomia behawioralna i badania empiryczne zaprzeczyły powyższemu opisowi jednostki, wskazując, że właśnie m.in. uprzedzenia, nadmierny optymizm, emocje czy też niedobór informacji są istotnymi czynnikami, które wpływają na decyzje ekonomiczne. Dyskurs, którego istota została opisana przez doktoranta, ma głębsze korzenie i znajduje również odbicie w podejściu do edukacji. Coraz częściej negowana jest wąska specjalizacja w podejściu do badań czy też edukacji, a w większym stopniu doceniane jest podejście interdyscyplinarne. Dysertacja doktoranta stanowi właśnie przejaw powyższego podejścia i

stanowi istotny argument za włączeniem psychologii do analizy zachowań konsumentów w sferze gospodarki.

Częścią tego rozdziału jest również analiza poszczególnych rodzajów błędów poznawczych pod kątem ich wpływu na podejmowane decyzje i oddziaływania na cyberbezpieczeństwo. Być może zakres analiz jest zbyt szeroki i można było dokonać wyboru określonych błędów spośród omawianych przez autora, wskazując na ich szczególne znaczenie. Jednak doceniam również chęć doktoranta aby nie tylko omówić poszczególne błędy poznawcze, ale również wskazać w jaki sposób oddziaływały na decyzje podejmowane w realnej rzeczywistości. Doktorant, odwołując się również do wcześniejszych analiz, wskazuje, że awersja ludzi do ryzyka i ewentualnych strat powoduje, że działy IT często nie podejmują działań w zakresie zmiany oprogramowania czy też jego uzupełnienia przez nowsze wersje.

W kolejnym, trzecim rozdziale, doktorant analizuje czym jest cyberprzestrzeń i cyberpolityka. Dynamiczny rozwój nowych technologii powoduje również konieczność nieustannego dodefiniowania cyberprzestrzeni. Natomiast cyberizacja, traktowana jako zjawisko negatywne staje się już powszechna w gospodarce, nauce czy też polityce. Przykłady wykorzystania cyberprzestrzeni do wpływania na wyniki wyborów czy też budowania sojuszy lobbingowych, oddziaływania na percepcję społeczną zostały szczegółowo opisane przez doktoranta. Można dodać, że ostatnie wydarzenia w Rumunii, w której ostatecznie unieważniono wybory, świadczą o daleko rozwiniętym procesie cyberprzestępczości. Szczególne znaczenie ma wykorzystanie cyberataków do zakłócenia bezpieczeństwa międzynarodowego i staje się one też innym rodzajem walki w globalnym świecie. Jednym z istotnych ograniczeń w przeciwdziałaniu cyberatakom jest brak regulacji prawnych w tym zakresie. Wynika to również z trudności przypisania działań konkretnemu podmiotowi, ponieważ często to nieustannie kopiujące się boty są głównymi aktorami w tym scenariuszu. Trudno natomiast ustalić gdzie jest organizacja czy też zespół osób a czasem nawet osoba, która zapoczątkowała cały proces.

Zdefiniowano również cyberprzestępstwo, zarówno w wąskim jak też szerokim znaczeniu. Istotne jest rozróżnienie – czy przedmiotem ataku jest komputer czy też komputer służy jako narzędzie do przestępstwa. Jednocześnie wskazano na rozróżnienie między pojęciami cyberprzestępczości i cyberwojny, która ma wyraźny aspekt polityczny. W przypadku cyberwojny chodzi przede wszystkim o zakłócenie działań krytycznej infrastruktury komunalnej, tak jak to miało miejsce przykładowo w przypadku Ukrainy. Dlatego też

wszelkie centralne systemy (serwery, bazy danych) zostały przeniesione poza terytorium, na którym toczą się działania wojenne. Wykorzystanie dronów, sterowanych z bezpiecznych miejsc, powoduje, że cyberwojna staje się zupełnie nową doktryną wojskową, co również definiuje w swojej pracy doktorant. Celem jest realizacja agendy 5D, czyli dezinformacji, oszustwa, destabilizacji, dezorganizacji i dostosowanego zniszczenia.

Pojawienie się cyberprzestępczości jako usługi (CaaS) tworzy nowe pole działania dla hakerów i cyberprzestępców. Bariery wejścia stały się znacznie mniejsze niż dotychczas, a łatwość pozyskania znacznych dochodów spowodowało masowe zainteresowanie kryminalnymi działaniami w cyberprzestrzeni. Wyciąg z cennika „Dark Web" z 2023 r. , który został zaprezentowany przez doktoranta, pokazuje jak rozwinęła się cyberprzestępczość. Jednocześnie dostępność sfałszowanych dokumentów stała się coraz łatwiejsza (s. 97). Przeszkodą w sprawnym pozyskiwaniu statystyk, które pozwalają na efektywniejsze zarządzanie przestrzenią cybernetyczną jest brak jasnego wyodrębnienia poszczególnych kategorii przestępstw, co również jest konsekwencją braku jednolitych definicji. W związku z powyższym wyliczenie kosztów cyberataków w podziale na poszczególne kategorie jest jednak bardzo trudne. Dodatkowo koszt ten wymaga również uwzględnienia różnych kategorii strat – poczynając od sprzętu poprzez przerwanie łańcuchów dostaw (koszty ekonomiczne) do kosztów społecznych i środowiskowych. Jak wynika z przeglądu literatury znaczna część cyberprzestępstw nie została zidentyfikowana. Brak ujawnień i zgłoszeń powoduje, że trudno określić skalę zjawiska. Problemem jest brak znajomości procedur zgłaszania cyberprzestępstw, ale też brak wiary w skuteczne działania organów ścigania w przypadku zgłoszenia. Według analiz FBI z 2019 r. szacuje się, że około 90 % wszystkich cyberprzestępstw pozostaje niezgłoszonych. Oznacza to, że istnieje ogromna czarna sfera w tym obszarze. Sugerowane rozwiązanie, polegające na standaryzacji i jednolitej kategoryzacji cyberprzestępczości napotyka na problem, który znany jest również w innych obszarach transformacji cyfrowej – brak wiarygodnych danych i trudność w ich pozyskiwaniu.

W kolejnym rozdziale autor podejmuje wątek rodzajów cyberzagrożeń, dzieląc je na międzynarodowe, wewnętrzne, zagrożenia w łańcuchu dostaw towarów i usług oraz zagrożenia wynikające z lokalnej zdolności operacyjnej. Zwraca uwagę na rozróżnienie między bezpieczeństwem a ochroną a także na zagrożenia związane z bezpieczeństwem fizycznym (zagrożenie życia) i bezpieczeństwem danych czy infrastruktury. Ponieważ

cyberkrajobraz jest dynamiczny cyberzagrożenia dzieli się na trzy różne kategorie: mające na celu integralność danego systemu informatycznego lub sieci, mające na celu dostępność i te, których celem jest naruszenie poufności. Powyższy podział został przez doktoranta przedstawiony w tabeli nr 5. W dalszych częściach doktorant omawia poszczególne typy zagrożeń: randsomware, WannaCry, Not Petya, wskazując również na konkretne przykłady ich użycia. Istotnym czynnikiem, który utrudnia przeciwdziałanie cyberatakom jest asymetria charakterystyczna dla cyberprzestrzeni, o której szerzej pisze autor. Powoduje ona, że cyberprzestępcy mają do dyspozycji szeroką gamę różnego rodzaju taktyk, gdy natomiast ofiary narażone są na ciągłe poszukiwanie właściwych narzędzi i analizowanie ataków, aby im przeciwdziałać w przyszłości. Ze względu na niejednolite metody identyfikacji i kategoryzacji działań przestępczych (gospodarczych, takich jak: kradzieże, oszustwa, pranie pieniędzy i przestępstwa przeciw własności intelektualnej) , występujące w poszczególnych krajach, zwalczanie ich napotyka na duże trudności. W związku z powyższym doktorant proponuję przyjęcie określonej typologii, przedstawionej w tabeli nr 10 (s. 125). W dalszej części dokonano charakterystyki poszczególnych grup oraz wskazano ich motywację i skalę oddziaływania. Tak szczegółowy podział, choć niewątpliwie pozwalający na lepsze zrozumienie zasad działania poszczególnych grup może jednak sprawiać pewne trudności przy zbieraniu danych dotyczących zagrożeń czy też incydentów w krajach. Dodatkowym utrudnieniem są również rozmyte granice między powyższymi grupami, o czym również autor wspomina w pracy.

Autor w swojej rozprawie zajmuje się przede wszystkim grupami, które działają złośliwie, naruszając zasady etyczne, w celu osiągnięcia osobistych satysfakcji i/lub korzyści finansowych. Kolejne pokolenia, już po pokoleniu Generacji Z, wychowane w świecie mocno zdigitalizowanym podejmują trochę dla zabawy próby łamania zabezpieczeń. W przedstawionym przez doktoranta cyberświecie przestępczość wydaje się na wczesnym etapie rozwoju, podobnie jak to miało miejsce w tworzących się dopiero zasadach funkcjonowania organizacji na wczesnym etapie rozwoju cywilizacji. Próby udaremnienia cyberprzestępstw przez organizacje, które zostały stworzone w świecie realnym, z natury rzeczy charakteryzują się niską skutecznością. Być może stworzenie takich organizacji, zwalczających cyberprzestępczość w metaversum pomogłoby lepiej zrozumieć i wykorzystać narzędzia. *W związku z powyższym proszę doktoranta o przeanalizowanie takiego wariantu w czasie obrony, wskazując zarówno na pozytywne, jak też negatywne aspekty powyższego rozwiązania.* Warto też zauważyć, że kilka państw (wśród nich Rosja,

Północna Kora, Chiny, Iran, Nigeria i Wietnam) specjalizuje się w sponsorowaniu grup przestępczych, których działania prowadzą w ostateczności do destabilizacji sytuacji politycznej i gospodarczej krajów, w stronę których są wymierzone.

W kolejnym rozdziale autor skupił się na analizie zakresu cyberryzyka i zasadach zarządzania w tym obszarze. Przyjęta za Wrede i in. definicja, iż jest to „jakiekolwiek ryzyko wynikające z wykorzystania technologii informacyjno-komunikacyjnych (ICT), które narusza poufność, integralność lub dostępność danych lub usług" powoduje konieczność rozpatrywania ryzyka w całej jego złożoności. Wymaga to wskazanie na powiązania występujące między czynnikami technicznymi, ekonomicznymi i społecznymi, czego próby podjął się w swojej dysertacji doktorant. Istotnym elementem tej części opracowania jest rozróżnienie między zarządzanie ryzykiem, co wiążę się z tworzeniem systemów identyfikujących, a następnie łagodzącym zagrożenia a odpornością na ryzyko. Odporność rozumiana jest w tym przypadku jako zdolność organizacji do szybkiego przywrócenia operacji biznesowych po udanym ataku ale też przewidywania, wytrzymywania, odzyskiwania i dostosowania się do niekorzystnych warunków w systemach, które są obsługiwane przez zasoby cybernetyczne. Zważywszy na to, że obecnie coraz większa liczba organizacji przeszła lub jest w fazie transformacji cyfrowej, odporność cybernetyczna stanowi podstawę funkcjonowania tych organizacji. Plan ciągłości procesów biznesowych, niedoceniany w fazie przedpandemicznej, okazał się zasobem strategicznym również w momencie innych działań, prowadzących do nagłych i niespodziewanych zaburzeń łańcuchów dostaw. Autor, bazując na analizie literatury, opisuje trzy możliwe stany po zaistniałym ataku: przywrócenie usług, poprawa będąca analizą zaistniałej sytuacji oraz pogorszenie, jeśli działanie negatywnego zdarzenia będzie trwałe, a organizacja nie będzie w stanie wystarczająco szybko zareagować. Z analiz recenzentki (szerszy opis powyższego zagadnienia znajdzie się w monografii red. H. Brdulak, Zarządzanie międzynarodowe w warunkach niepewności- zrównoważony rozwój i cyfryzacja, OW SGH, 2025) wynika, że organizacje uznają czas 24 godziny za pożądany, w przypadku niespodziewanego zdarzenia. Jednak w przypadku cyberataku może to prowadzić do uruchomienia systemów i zablokowania procesów w dużo krótszym czasie, o czym pisze również doktorant. Przeprowadzanie systematycznych ćwiczeń symulacji ataków prowadzi do wzmocnienia świadomości pracowników w organizacji, gdy tymczasem nadmierny optymizm i zaufanie do siebie jest silnym elementem zagrożenia. Dodatkowo wzrasta również zagrożenie wynikające z dużej liczby urządzeń

elektronicznych, z których korzystają użytkownicy, przy czym część z nich jest prywatna a część należy do organizacji, w której pracują. Często nie istnieje rozróżnienie między zakresem dostępności prywatnym i służbowym, co pozwala na komunikowanie się w organizacji z dowolnego urządzenia, które jest w posiadaniu użytkownika. To również ma wpływ na zacieranie się granic między czasem pracy i czasem prywatnym. Dodatkowe zagrożenia tworzą również systemy pośrednie (API), które wykorzystywane są dość powszechnie w organizacjach, Internet Rzeczy czy też Chmura komputerowa. Skala zagrożeń według badań jest wysoka. Szczegółowe dane zostały podane przez doktoranta. Często również bezpośredni atak przenika do całej organizacji i może powodować negatywne skutki nie tylko w danej organizacji ale w całym łańcuchu wartości, w którym uczestniczy atakowany. Spillover effect i jego skutki nie są jeszcze do końca zidentyfikowane, ale są znaczącym elementem ryzyka i procesów polegających na budowaniu odporności. Szczególnie istotne jest określenie infrastruktury krytycznej, która powinna mieć zabezpieczenia, które mogą stawiać czoła wszelkim niespodziewanym zdarzeniom i atakom cybernetycznym. Zwraca na to uwagę doktorant, wskazując przykłady skutków ataków na elementy tej infrastruktury, zarówno w organizacjach, jak też w poszczególnych krajach.

Po tak szczegółowym omówieniu zagadnień dotyczących zarówno definicji cyberzagrożeń, cyberekosystemu wraz z jego głównymi aktorami, jak też ryzyka i budowania odporności doktorant w rozdziale szóstym zmierzył się z lukami badawczymi, pokazując wyniki swoich badań empirycznych. W zakresie podejmowania decyzji doktorant zidentyfikował lukę w postaci braku kompleksowego badania (badania szczegółowe były przytaczane w dysertacji) znaczenia uprzedzenia w decyzjach związanych z cyberbezpieczeństwem. W szczególności problem ten dotyczy specjalistów IT i specjalistów do spraw cyberbezpieczeństwa. Kolejną, zidentyfikowaną przez doktoranta luką jest brak uwzględnienia przy analizach nieporozumień i barier psychicznych. W szczególności należy tu wymienić zbytnie przywiązanie do standardów branżowych czy też oczekiwanie na większą ilość informacji w celu podjęcia działań zapobiegawczych. Nadal połowa dyrektorów generalnych uważa, że koszt wdrożenia systemów cyberodporności przekracza koszty cyberataku. Mimo wzrostu natężenia cyberataków i coraz szerszych ich skutków, nadal nie doceniane są straty wynikające z przerwania łańcuchów dostaw. Nadmierna pewność siebie i przekonania stanowią kolejną lukę, zidentyfikowaną przez doktoranta. Błędne przekonania dotyczące podatności na

cyberatak połączone z nieuzasadnionym przekonaniem na temat własnego bezpieczeństwa stanowią istotną przyczyną zaniedbań w sferze zabezpieczenia przed zagrożeniami cyberataku. Mimo nagłośnienia przez media informacji w tym zakresie – widoczne jest skupianie się decydentów na fragmencie przekazu, który wspiera ich przekonania, a nie uwrażliwia na nowe zagrożenia. Dodatkowo złożoność problemów dotyczących ekosystemu cyberprzestępstw, która nieustannie rośnie, utrudnia ich zrozumienie. W niewielkim stopniu zanotowano postęp w tym obszarze w ciągu ostatnich 10 lat. Zagrożenia wynikające z cyberprzestępstw powinny być uświadamiane na każdym szczeblu organizacji, co jak wynika z badań CISCO, nie zawsze ma miejsce. Świadomość powyższych ryzyk na szczeblu zarządu i właścicieli jest kluczowym elementem zarządzania ryzykiem w tym obszarze, jednak nie wystarczającym. Szkolenia i procedury, które powinny być systematycznie sprawdzone pod kątem aktualności ale także świadomość błędów poznawczych będzie miała wpływ na budowanie cyberodporności organizacji.

Pomimo badań, dotyczących błędów poznawczych, prowadzonych przez naukowców w ostatnich latach, brakuje całościowego podejścia w obszarze cyberbezpieczeństwa oraz praktycznych wskazówek dla menedżerów. Lukę tę stara się wypełnić doktorant, koncentrując się na analizie zachowań menedżerów z regionu DACH, najmniej eksplorowanego z punktu widzenia badaczy.

Doktorant w sposób jednoznaczny i klarowny pokazuje na ile jego dysertacja zapełnia lukę badawczą w zakresie cyberbepieczeństwa w powiązaniu z błędami poznawczymi. Dodatkowo również wskazuje kierunki dalszych badań, które wiążę się również z pewnymi ograniczeniami jego opracowania, które doktorant jasno definiuje. Badania, które zostały przeprowadzone przez doktoranta z wysoką starannością jeśli chodzi o metodologię, łączą podejście jakościowe i ilościowe. Mimo niewystarczającej liczby wypowiedzi oraz niejednoznaczności wyników analiz statystycznych niezbędnych do generalizacji wniosków, doktorant zmierzył się z pytaniami badawczymi, postawionymi w części wstępnej dysertacji.

W celu właściwej konstrukcji kwestionariusza zostały przeprowadzone 4 wywiady z ekspertami, które miały na celu zdiagnozowanie problemu. Staranny dobór ekspertów, który został szczegółowo wyjaśniony w dysertacji, miał również duży wpływ na ostateczny kształt pytań w kwestionariuszu. *Jedno z kryterium doboru – 20-letnie doświadczenie w obszarze cyberbepieczeństwa, może jednak oddziaływać na uaktywnienie*

się między innymi jednego z błędów poznawczych – nadmiernej pewności siebie. Czy autor dysertacji mógłby odnieść się w czasie obrony do powyższego ryzyka? Jakie jest Jego zdaniem prawdopodobieństwo, że mogłoby ono wystąpić?. W czasie wywiadów zidentyfikowano brak strategicznego podejścia do kwestii cyberbezpieczeństwa w przeciwieństwie do procesu transformacji cyfrowej. Obszar cyberbezpieczeństwa traktowany jest jako techniczny a nie strategiczny. W efekcie wprowadzanie nowych technologii często nie jest związane z dogłębną analizą ryzyka, a szybkość wdrażania nowych technologii nie sprzyja również powyższemu działaniu. Głosy ekspertów w danej organizacji nie są doceniane i w wystarczający sposób uwzględniane, ponieważ nie sprzyja temu również silosowa struktura organizacji.

Badania przeprowadzono na platformie internetowej w terminach od 9 kwietnia do 26 lipca 2024 r. . Korzystano z dwóch wersji językowych: angielskiej i niemieckiej. W tym czasie mogło dojść do różnych incydentów w zakresie cyberbezpieczeństwa, co również mogłoby mieć wpływ na udzielane odpowiedzi. Autor skupił się na badaniu różnic między czasem odpowiedzi gdy być może warto było podjąć się badania czy i na ile odpowiedzi powiązane były z określonymi wydarzeniami, które miały miejsce w organizacji. Do konstrukcji kwestionariusza wykorzystano wielopoziomową analizę czynnikową, opierając się na badaniach Rhee in. (2012). Przytoczone badania uwzględniały optymistyczne skrzywienie i iluzję kontroli w podejmowanych decyzjach dotyczących cyberbezpieczeństwa. Uwzględniono również praktyczne doświadczenie respondentów, cechy organizacji oraz istnienie określonych procedur (plan komunikacji kryzysowej, coroczne praktyki audytowe, regularne ćwiczenia przeciwpożarowe). Badania przeprowadzono na terenie Niemiec, Austrii i Szwajcarii – obszaru, który wcześniej w niewielkim stopniu został przebadany. W ten sposób uzupełniono lukę badawczą. Zadbano również o aspekt etyczny badania. Respondentami była wyższa i średnia kadra kierownicza, reprezentująca zarówno przedsiębiorstwa duże jak też średnie. Ostatecznie uzyskano 144 odpowiedzi (ponad 5 proc. zwrot), które można było zakwalifikować do analizy. Interesująca jest przedstawiona przez autora analiza demograficzna respondentów. Ponad 55 proc. stanowią osoby w wieku ponad 50 lat, głównie mężczyźni (ponad 88 proc.), o ponad 15 letnim doświadczeniu (prawie 48 proc.). Ich obszar działania to IT, cyberbezpieczeństwo, zarządzanie ryzykiem i zgodnością z prawem, dbanie o bezpieczeństwo danych. Głównie reprezentują branże IT, produkcję, profesjonalny serwis oraz handel. Zabrakło informacji, dotyczącej kraju pochodzenia danego respondenta. Z

badań recenzentki kultura danego kraju ma również wpływ na zachowania respondentów. W efekcie zidentyfikowano kilka korelacji, które pozwalają na interesujący ogląd powyższych zjawisk a także rzucają nowe światło na kwestie cyberbezpieczeństwa. I tak systematycznie przeprowadzone audyty prowadziły do nadmiernej pewności siebie w zakresie bezpieczeństwa. Miało to również związek z nadmiernym optymizmem. Doktorant zauważył również (choć nie zostało to w pełni statystycznie potwierdzone), że przebieg raportowania może mieć wpływ na powstawanie uprzedzeń poznawczych. W przypadku raportowania menedżera do osoby, które nie jest z pionu IT, konieczne jest głębsze zrozumienie problemu (włączenie tzw. wolnego myślenia) tak, aby można było wytłumaczyć dane zagadnienie osobie spoza branży technologicznej. Doświadczenia ataku bez istotnych negatywnych skutków i podwyższona świadomość nie zmniejsza błędów poznawczych, które doktorant wcześniej zdefiniował, a nawet może je wzmacniać. Wprawdzie taki wniosek wymaga jeszcze dodatkowych potwierdzeń, ale jest cenną wskazówką badawczą. Tak więc trudno uznać, wobec niejasności uzyskanych wyników statystycznych, o potwierdzeniu lub odrzuceniu hipotez(pytań badawczych), które zostały wcześniej sformułowane przez doktoranta. Również analiza wyników innych badaczy, nie prowadzi do jednoznacznych konkluzji. Jednak powiązanie podejmowanych działań w zakresie cyberbezpieczeństwa z analizą błędów poznawczych wskazuje istotny obszar badawczy, którego eksploracja została już częściowo rozwinięta przez doktoranta.

Godna podkreślenia jest również analiza ograniczeń, którą dokonał doktorant w ostatnim rozdziale dysertacji, których część została już wskazana w niniejszej recenzji.

W podsumowaniu doktorant zmierzył się z odpowiedziami na postawione pytania badawcze, zestawiając jeszcze raz wyniki badań, które są już dostępne w literaturze z badaniami własnymi.

Całość dysertacji stanowi pasjonujący materiał dla czytelnika. Staranne podejście do analiz, przeglądu literatury, sposób uzasadnienia i w końcu również badań świadczą o bardzo wysokich kompetencjach doktoranta w analizowanym obszarze. W przeciwieństwie do oceny kompetencji dyrektorów przez menedżerów (przytaczane w opisie wyników badań przez doktoranta, tzw. efekt „aureoli") moja ocena oparta jest na mocnych argumentach, które znalazłam w niniejszej dysertacji.

Tym niemniej chciałabym również wskazać kilka obszarów, które mogą podlegać doskonaleniu. Jednym z nich jest nadmierne moim zdaniem nasycenie i nieustanne

odwoływanie się do publikacji innych autorów. Świadczy o tym 52 strony spisu samych pozycji literatury, które zostały uwzględnione w pracy. Z jednej strony jest to wymóg oczekiwany od doktorantów, z drugiej strony może jednak prowadzić do wniosku, że doktorant obawia się prowadzić samodzielny wywód a każdą konkluzję odnosi do określonej pozycji w literaturze. Znalezienie punktu przegięcia między tymi dwoma obszarami to również duże wyzwanie stawiane przed naukowcem. Kolejny obszar dotyczy wielokrotnego powtarzania treści, które już wcześniej zostały przedstawione. I znowu – dzięki temu można swobodnie śledzić wywód doktoranta, ale można tez spróbować dokonać takiej zmiany struktury narracji w ramach dysertacji, aby zmniejszyć liczbę powtarzalnych wniosków, bez uszczerbku dla meritum.

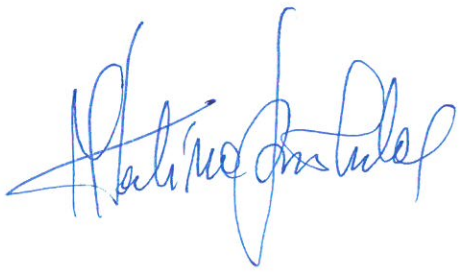
Na koniec chciałabym zainteresować doktoranta podjęciem badań w pokoleniu Z i/lub Alpha. Ponieważ w prezentowanych badaniach te grupy są w niewielkim stopniu reprezentowane to może właśnie skupienie się na młodych osobach mogłoby prowadzić do ciekawych wniosków, zważywszy też na to, że zmienia się obecnie model zarządzania. Nowe pokolenie także przejmuje coraz więcej stanowisk kierowniczych.

Nieco anegdotycznie – ale mimo wszystko chciałabym dopytać, który z analizowanych przez doktoranta błędów poznawczych, wymienionych na wstępie pracy, został zidentyfikowany przez doktoranta jako cecha, która jemu również towarzyszyła w czasie pisania pracy. Byłoby interesujące gdyby doktorant chciałby się zmierzyć z tym pytaniem w czasie obrony, przytaczając również argumenty.

Konkluzja końcowa

Przedstawiona rozprawa doktorska mgra Marca Wilczka pt. "Decision-Making under Constraints: A Behavioral Economics Perspective on Cyber-Related Heuristics and Biases", przygotowana pod kierunkiem dr hab. prof. UG Moniki Bąk stanowi oryginalne rozwiązanie problemu naukowego w oparciu o przeprowadzone badania. Jednocześnie stwierdzam, iż doktorant posiada ogólną wiedzą teoretyczną wymaganą w dyscyplinie ekonomia i finanse, potrafi dokonywać samodzielnie analiz i syntezy powyższej wiedzy. Stosowane metody badawcze wskazują na dobrą znajomość narzędzi, które pozwalają na mierzenie się z odpowiedziami na pytania badawcze. Warto podkreślić, że doktorant łączy również umiejętność prowadzenia wywodu w oparciu o literaturę z pragmatycznym podejściem do rzeczywistości. Tym

samym potwierdzam, że recenzowana rozprawa spełnia kryteria ustawowe, wymagane dla prac doktorskich. Jednocześnie wnioskuję o dopuszczenie doktoranta do publicznej obrony, a także - wyróżnienie pracy i publikację w formie zwartej po dokonaniu niezbędnych skrótów.



SGH Collegium of World Economy

Warsaw, 15.12.2024

Dr hab. Halina Brdulak, professor SGH

Department of International Management

Collegium of International Economics

SGH - Warsaw School of Economics

Review of the PhD dissertation of Mr. Marc Wilczek, MA "Decision-Making under Constraints: A Behavioral Economics Perspective on Cyber-Related Heuristics and Biases" prepared under the scientific supervision of dr. hab. professor UG Monika Bąk

Formal arrangements

The basis for the review is a letter dated 17.10.2024 from the Chairman of the Discipline Council of Economics and Finance of the University of Gdańsk, dr. habil. Leszek Czerwonka, prof. UG, informing me that the Discipline Council of Economics and Finance of the University of Gdańsk appointed me as a reviewer of the PhD dissertation of Mr. Marc Wilczek, MA entitled "Decision-Making under Constraints: A Behavioral Economics Perspective on Cyber-Related Heuristics and Biases" in the field of social sciences, scientific discipline: economics and finance. I received the letter on 21.10.2024 electronically to the e-mail address. The supervisor of this dissertation is dr. hab. prof. UG Monika Bąk. The formal and legal basis for the assessment are the requirements specified in art. 187 of the Act of 20 July 2018 - The Law on Higher Education and Science (Dz. U. 2022, item 574, as amended), which states, among other things, that

- the doctoral dissertation should represent the candidate's general theoretical knowledge in the discipline and the ability to independently conduct scientific work,

- the subject of the doctoral dissertation should be an original solution to a scientific problem, an original solution in the scope of applying the results of one's own scientific research in the economic or social sphere,

- a doctoral dissertation may be a written work, including a scientific monograph, a collection of published and thematically related scientific articles, project work, as well as an independent and separate part of a collective work.

Taking into account the above issues based on the analysis conducted below, I state that the presented PhD dissertation of M.A. Marc Wilczek entitled "Decision-Making under Constraints: A Behavioral Economics Perspective on Cyber-Related Heuristics and Biases", prepared under the supervision of dr hab. prof. UG Monika Bąk, is an original solution to a scientific problem based on the conducted research. At the same time, I state that the doctoral student not only has the general theoretical knowledge required in the discipline of economics and finance but is also able to independently analyze and synthesize the above knowledge. I thereby confirm that the reviewed dissertation meets the statutory criteria required for doctoral theses.

General remarks

The Phd dissartation consists of 6 chapters, 8 appendices and 297 pages. The list of sources is impressive and takes up 52 pages. These are primarily articles, a significant number from recent years. For illustration and at the same time a synthetic presentation of the content provided, 16 tables and 19 drawings were used. The appendices include 8 questionnaires that the author used in the conducted research. A supplement of great substantive importance is a glossary of expressions and abbreviations used in the work.

In Chapter I, entitled Introduction, the author in the first part presents his motivation for taking up this topic, in the context of the increasing threat due to cyberattacks. As it results from the analyses cited by the author, despite the fact that companies are investing more and more in protection against attacks, the level of threat is still growing. The main factor is the habits and prejudices of people working in the organization. The behavior of these people, not always consciously aware, poses a threat to the IT environment in which they function. The number of incidents in this area caused by human error is growing dynamically and sometimes reaches almost 90%. Based on a review of the literature, the author identified as many as 17 factors resulting from human behavior that may affect digital security. Younger people who have been raised in a digital environment since birth, referred to as digital natives, are more susceptible to digital attacks, which is directly correlated with the time they spend on the Internet. On the other side are older people, aged 65 and over, who use the Internet more consciously.

The aim of this dissertation, as indicated by the author in p. 1.1, is to " explore the magnitude of cognitive distortions and their role in fostering erroneous judgments among cyber professionals". The aim formulated in this way was clarified later in the chapter "explore the challenges and limitations in cyber-related strategic decision-making processes, particularly under conditions of bounded rationality.."

The author also added that the analysis is conducted based on the assumptions of behavioral economics, taking into account cognitive biases and heuristics. The application aim of the dissertation was also formulated - to support organizations in reducing their exposure to cyber threats and combating the growing threat of cybercrime. In connection with the aim formulated in this way, the author communicates that his research is focused on finding a way to limit or counteract the influence of cognitive biases on strategic

decision-making in the field of cybersecurity. This also comes down to examining the impact of emotions and heuristics on the decision-making process.

In connection with this main objective, the author formulated the following research objectives:

- to investigate the significance of biases and heuristics affecting strategic decision-making in cyber-related questions as it relates to IT professionals and cyber-expert across mid-market companies and large-enterprises in Germany, Austria, and Switzerland;
- to evaluate specifically how cognitive biases such as *optimism, overconfidence,* and the *availability heuristic* lead to distortions in the assessment of cyber-threats, the implementation of safeguards, and the mitigation of cyber-attacks;
- to study the emergence of cybercrime including the supporting elements and threat actors exacerbating the situation and ultimately exposing organizations to cyber-threats;
- to examine and contextualize the cyber-risk landscape and illustrate the economic consequences of flawed decision-making; to close the theoretical gap in existing literature when it comes to cyber-related biases; and
- to provide practical advice to practitioners what action can be taken to make more informed decisions and derive at better outcomes to reduce their organization's cyber-risk exposure.

The research objectives were used to formulate 3 research questions:

1. When it comes to cyber-related questions, what are the cognitive biases that hinder subject matter experts in their decision-making and impact the effectiveness of countermeasures?

2. What are the driving forces behind the proliferation of cyber-threats, and how do cognitive biases shape the effectiveness of countermeasures in the evolving cybercrime landscape?

3. How are the economic consequences of cyber-security incidents underestimated due to cognitive biases, and what are the broader implications for businesses and societal resilience?

The dissertation also indicates in which chapters answers to the above questions can be found. Quantitative and qualitative research methods were used to verify these questions. In addition to a critical analysis of the literature, expert interviews were conducted, allowing the author to narrow the issues down to three main patterns — availability heuristics, optimism, and overconfidence. The quantitative phase included developing a questionnaire, the responses of which were analyzed using structural equation modeling (SEM) and SPSS software.

The layout of the chapters is clearly presented in Table 2.

The structure of the dissertation is logical, and the research objectives have been framed in three research questions. The topic, formulated by the doctoral candidate, is timely and is gaining increasing importance in the context of ongoing economic digitalization and the digital transformation of enterprises. Vulnerability to threats is increasing as cybercriminals increasingly utilize knowledge from sociology and psychology, similar to what happens in the real world. However, in cyberspace, the scope of action extends globally, as it is not limited by national borders. Furthermore, an economy based on constant growth leads to distortions and greed, as noted by Sedlacek (T. Sedlacek, *Economics of Good and Evil*, 2012) and Zuboff (S. Zuboff, *The Age of Surveillance Capitalism*, 2020). Therefore, the topic undertaken by the doctoral candidate should be regarded as very important and aligned with the latest research trends.
The style and language of the dissertation are appropriate.

Detailed Comments

In the first chapter, the author provides an overview of the dynamic state of Internet usage worldwide. Key global risks identified in the WEF report are also discussed, with cyberattack risk ranked 8th. The conclusions from the literature review conducted by the doctoral candidate are particularly interesting. It is not surprising that increased exposure to cyberattacks is linked to the proliferation and rapid development of new technologies as a result of the pandemic. However, the Internet also fosters a "split" personality, where actions in the real world operate under different rules than in the virtual world. Honest individuals suddenly change their behavior and become criminals online. Cybercrime is further driven by increased Internet accessibility, and higher education or income does not hinder it but sometimes even accelerates it.
The subsequent chapters aim to integrate theory and practice to diagnose how biases and excessive optimism among employees impact digital security risk levels.
In the third chapter, the author focuses on a literature review and a theoretical approach to cybersecurity, considering technological aspects. An essential element is the demonstration of how "black markets" operate and the challenges faced by law enforcement agencies.

The next chapter characterizes the hacker environment and their motivations, based on behavioral economics analyses. This section also highlights the complexity of the cybercrime ecosystem and key factors influencing its maintenance and development. The result of these considerations is an analysis of the dual role of digital technology in enabling cybercrime and increasing vulnerability. The spiral linking technological progress to the development of cybercrime appears endless. The economy's increasing dependence on new technologies, combined with the expanding areas affected by digitalization, also broadens the concept of critical infrastructure. Thus, the goal of this section is to present a holistic understanding of the cybersecurity ecosystem. In the final part, the author analyzes the effectiveness of current measures to mitigate cyberattack risk. He also highlights the underestimation of cognitive errors, such as availability heuristics, overconfidence, and optimism bias, which significantly reduce the effectiveness of strategies implemented to defend against cyberattacks.

Below, I will address the individual chapters, pointing to the key elements that justify my final conclusion.

In the second chapter, the author focuses on explaining his approach, which is based on behavioral economics. He also discusses the assumptions of various economic schools of thought, which relied heavily (like classical economics) or to a lesser extent (like neoclassical economics) on the assumption of human rationality and marginal utility. Institutional economics and new institutional economics assumptions are also discussed, highlighting the differences between these approaches. The role of broadly understood institutions and their impact on individual behavior, considering transaction costs, forms the foundation of this part of the dissertation. The next stage in the development of economic approaches may be neo-institutional economics. Discussions in emerging economic schools largely focus on the concept and significance of rationality in human choices. The question of whether individuals act as *homo economicus*, understood as rational agents pursuing self-interest and maximizing their preferences, thereby "optimizing" decisions, forms the basis of neo-institutional economics. Behavioral economics and empirical studies have contradicted this description of individuals, pointing out that biases, excessive optimism, emotions, and a lack of information are significant factors influencing economic decisions. The discourse described by the doctoral candidate has deeper roots and is also reflected in approaches to education. Narrow specialization in research or education is increasingly criticized, while interdisciplinary approaches are more valued. The doctoral candidate's dissertation is an example of this approach and provides a strong argument for incorporating psychology into the analysis of consumer behavior in the economic sphere.

This chapter also includes an analysis of various types of cognitive biases in terms of their impact on decision-making and cybersecurity. Perhaps the scope of the analyses is too broad, and the author could have selected specific cognitive biases to highlight their particular significance. However, I also appreciate the doctoral candidate's effort not only to discuss individual cognitive biases but also to demonstrate how they influence decisions in real-world scenarios. Referring to earlier analyses, the candidate notes that people's aversion to risk and potential losses causes IT departments to often refrain from updating software or supplementing it with newer versions.

In the next, third chapter, the doctoral candidate analyzes what cyberspace and cyberpolitics are. The rapid development of new technologies also necessitates the continual redefinition of cyberspace. However, cyberization, treated as a negative phenomenon, has already become widespread in the economy, science, and politics. Examples of cyberspace being used to influence election outcomes, build lobbying alliances, or shape public perception are described in detail by the doctoral candidate. It could be added that recent events in Romania, where elections were ultimately annulled, demonstrate an advanced level of cybercrime. The use of cyberattacks to disrupt international security is of particular importance and has become another form of warfare in the globalized world. One of the main limitations in counteracting cyberattacks is the

lack of legal regulations in this area. This also results from difficulties in attributing actions to specific entities, as continuously replicating bots are often the main actors in this scenario. It is difficult to determine where the organization, team, or even the individual who initiated the process is located.

The concept of cybercrime has been defined in both narrow and broad terms. It is important to distinguish whether the computer is the target of the attack or merely a tool used to commit the crime. Additionally, a distinction was made between the concepts of cybercrime and cyberwarfare, which has a clear political aspect. In the case of cyberwarfare, the primary goal is to disrupt the activities of critical communal infrastructure, as was exemplified by events in Ukraine. Consequently, all central systems (servers, databases) were relocated outside the territory where hostilities are taking place. The use of drones, controlled from safe locations, has made cyberwarfare a completely new military doctrine, as defined in the doctoral student's PhD thessis. The aim is to implement the 5D agenda, which stands for disinformation, deception, destabilization, disorganization, and tailored destruction.

The emergence of Cybercrime as a Service (CaaS) has created a new field of activity for hackers and cybercriminals. The barriers to entry have become significantly lower than before, and the ease of obtaining substantial profits has led to massive interest in criminal activities in cyberspace. An excerpt from the "Dark Web" price list of 2023, presented by the doctoral student, shows how cybercrime has evolved. At the same time, the availability of forged documents has become increasingly easier (p. 97). A challenge in efficiently obtaining statistics that allow for more effective management of cyberspace is the lack of clear distinction between various categories of crimes, which is also a consequence of the lack of uniform definitions. Therefore, estimating the costs of cyberattacks by category is very difficult. Additionally, these costs require consideration of various categories of losses – from hardware and supply chain disruptions (economic costs) to social and environmental costs. The literature review indicates that a significant portion of cybercrimes remains unidentified. The lack of disclosures and reports makes it difficult to determine the scale of the phenomenon. The problem lies in the lack of knowledge about reporting procedures for cybercrimes, as well as a lack of faith in the effective actions of law enforcement agencies when reporting. According to FBI analyses from 2019, it is estimated that about 90% of all cybercrimes go unreported. This means there is a vast dark area in this field. The suggested solution of standardizing and uniformly categorizing cybercrime encounters the problem known in other areas of digital transformation – the lack of reliable data and difficulty in obtaining it.

In the next chapter, the author addresses the types of cyber threats, dividing them into international, internal, threats in the supply chain of goods and services, and threats resulting from average local operational capabilities. The distinction between security and protection is emphasized, as well as the threats related to physical security (threat to life) and the security of data and infrastructure. Since the cyber landscape is dynamic, cyber threats are divided into three different categories: those aimed at the integrity of a particular IT system or network, those aimed at availability, and those targeting

confidentiality breaches. This division is presented by the doctoral student in Table 5. In the following sections, the doctoral student discusses specific types of threats: ransomware, WannaCry, NotPetya, providing specific examples of their use. A significant factor that hinders countering cyberattacks is the asymmetry characteristic of cyberspace, which the author elaborates on extensively. This asymmetry allows cybercriminals to employ a wide range of tactics, while victims are continually searching for appropriate tools and analyzing attacks to counter them in the future. Due to inconsistent methods of identifying and categorizing criminal activities (economic crimes such as theft, fraud, money laundering, and intellectual property crimes) in different countries, combating them encounters significant difficulties. Therefore, the doctoral student proposes adopting a specific typology, presented in Table 10 (p. 125). The following sections characterize individual groups and indicate their motivations and scale of impact. Such a detailed division, although undoubtedly allowing for a better understanding of their operating principles, may pose some challenges in collecting data on threats or incidents in different countries. Another complication is the blurred boundaries between these groups, which the author also mentions in the PhD thesis.

The author primarily addresses groups that act maliciously, violating ethical principles to achieve personal satisfaction and/or financial gain. Subsequent generations, even after Generation Z, raised in a highly digitalized world, engage in hacking attempts somewhat for fun. In the cyber world presented by the doctoral student, crime seems to be in its early stages of development, similar to the early stages of organizational functioning principles in the early development of civilization. Attempts to prevent cybercrimes by organizations created in the real world are inherently characterized by low effectiveness. Perhaps creating such organizations fighting cybercrime in the metaverse would help better understand and utilize tools. Therefore, I ask the doctoral student to analyze this variant during the defense, indicating both positive and negative aspects of this solution. It is also worth noting that several countries (including Russia, North Korea, China, Iran, Nigeria, and Vietnam) specialize in sponsoring criminal groups, whose actions ultimately lead to the destabilization of political and economic situations in the target countries.

In the next chapter, the author focused on analyzing the scope of cyber risks and the principles of management in this area. The definition adopted from Wrede et al. that it is "any risk arising from the use of information and communication technologies (ICT) that compromises the confidentiality, integrity, or availability of data or services" necessitates considering risk in all its complexity. This requires indicating the connections between technical, economic, and social factors, which the doctoral student attempted in their dissertation. A significant element of this section is the distinction between risk management, which involves creating systems that identify and then mitigate threats, and resilience to risk. Resilience is understood in this context as the ability of an organization to quickly restore business operations after a successful attack but also to anticipate, withstand, recover from, and adapt to adverse conditions in systems operated by cyber resources. Given that more and more organizations have transitioned or are in the process of digital transformation, cyber resilience is fundamental to their functioning. The business

continuity plan, undervalued in the pre-pandemic phase, has proven to be a strategic resource also in the event of other actions leading to sudden and unexpected supply chain disruptions. As the author, based on literature analysis, describes three possible states after an attack: service restoration, improvement through analyzing the situation, and deterioration if the negative event persists and the organization cannot respond quickly enough. From the reviewer's analysis (a broader description of this issue will be found in the monograph edited by H. Brdulak, International Management in Uncertainty Conditions - Sustainable Development and Digitalization, OW SGH, 2025), organizations consider 24 hours as the desirable time frame in case of an unexpected event. However, in the case of a cyberattack, this may lead to system activation and process blockage in a much shorter time, as also noted by the doctoral student. Conducting systematic attack simulation exercises strengthens employee awareness within the organization, while excessive optimism and self-confidence pose a significant threat. Additionally, the threat increases with the number of electronic devices users utilize, some of which are private and some belong to the organization they work for. Often, there is no distinction between private and work-related access, allowing communication within the organization from any device the user possesses. This also affects the blurring of boundaries between work time and personal time. Additional threats are also created by intermediate systems (APIs) commonly used in organizations, the Internet of Things, and Cloud Computing. The scale of threats, according to research, is high. Detailed data is provided by the doctoral student. Often, a direct attack penetrates the entire organization and can have negative consequences not only for the organization itself but also for the entire value chain in which the attacked entity participates. The spillover effect and its consequences are not yet fully identified but are a significant element of risk and processes involved in building resilience. Particularly important is defining critical infrastructure that should have safeguards to face any unexpected events and cyberattacks. The doctoral student draws attention to this by providing examples of the impact of attacks on critical infrastructure elements in organizations and individual countries.

After such a detailed discussion on the definitions of cyber threats, the cyber ecosystem with its main actors, as well as risk and building resilience, the doctoral student addresses research gaps in the sixth chapter, showing the results of their empirical research. In decision-making, the doctoral student identified a gap in the form of a lack of comprehensive research (detailed studies were cited in the dissertation) on the significance of bias in cybersecurity-related decisions. This problem particularly concerns IT specialists and cybersecurity professionals. Another gap identified by the doctoral student is the lack of consideration of misunderstandings and psychological barriers in analyses. This includes excessive attachment to industry standards or waiting for more information to take preventive actions. Still, half of the CEOs believe that the cost of implementing cyber resilience systems exceeds the costs of a cyberattack. Despite the increase in cyberattacks and their growing impacts, the losses resulting from supply chain disruptions are still underestimated. Overconfidence and convictions constitute another gap identified by the doctoral student. Misconceptions about vulnerability to cyberattacks, combined with unjustified confidence in one's security, are significant causes of neglect in safeguarding

against cyber threats. Despite media coverage on this topic, decision-makers tend to focus on parts of the message that support their beliefs rather than raising awareness of new threats. Additionally, the complexity of problems related to the cybercrime ecosystem, which continues to grow, makes it difficult to understand them. There has been little progress in this area over the past 10 years. Cybercrime threats should be made aware at every organizational level, which, according to CISCO research, is not always the case. Awareness of these risks at the management and ownership levels is a key element of risk management in this area but not sufficient. Training and procedures, which should be systematically reviewed for relevance, as well as awareness of cognitive biases, will impact building organizational cyber resilience.

Despite research on cognitive biases conducted by scholars in recent years, there is a lack of a comprehensive approach in the field of cybersecurity and practical guidance for managers. The PhD candidate seeks to fill this gap by focusing on the analysis of managerial behaviors from the DACH region, which has been the least explored from a research perspective.

The PhD candidate clearly and unambiguously demonstrates how his dissertation fills the research gap in the area of cybersecurity in connection with cognitive biases. Additionally, he indicates directions for future research, which are also related to certain limitations of his study, which the candidate clearly defines. The research conducted by the candidate, with high methodological rigor, combines both qualitative and quantitative approaches. Despite the insufficient number of responses and the ambiguity of statistical results necessary for generalizing conclusions, the candidate addressed the research questions posed in the introductory section of the dissertation.

To properly construct the questionnaire, four expert interviews were conducted to diagnose the problem. The careful selection of experts, which is thoroughly explained in the dissertation, also had a significant impact on the final form of the questions in the questionnaire. One of the selection criteria—20 years of experience in the field of cybersecurity—might, however, trigger one of the cognitive biases, namely overconfidence. Could the author of the dissertation address this risk during the defense? What is his opinion on the likelihood that it could have occurred?

During the interviews, the lack of a strategic approach to cybersecurity, in contrast to the digital transformation process, was identified. Cybersecurity is treated as a technical, rather than strategic, issue. As a result, the implementation of new technologies is often not accompanied by thorough risk analysis, and the speed of technology adoption does not foster such analysis. Expert voices within the organization are not sufficiently appreciated or taken into account due to the siloed organizational structure.

The research was conducted on an online platform from April 9 to July 26, 2024, using both English and German versions of the questionnaire. During this period, various cybersecurity incidents could have occurred, which might have influenced the responses given. The author focused on analyzing response time differences, though it may have been valuable to investigate whether the responses were linked to specific events occurring

within the organization. The questionnaire was constructed using multilevel factor analysis, based on Rhee et al. (2012). These studies took into account optimistic bias and the illusion of control in decision-making related to cybersecurity. They also considered the respondents' practical experience, organizational characteristics, and the existence of specific procedures (crisis communication plan, annual audit practices, regular fire drills). The study was conducted in Germany, Austria, and Switzerland—an area that had previously been minimally studied. In this way, the research gap was filled. Ethical aspects of the study were also carefully considered. Respondents were senior and middle management, representing both large and medium-sized enterprises. Ultimately, 144 responses (over a 5% response rate) were qualified for analysis.

The demographic analysis of the respondents presented by the author is interesting. Over 55% are individuals over the age of 50, primarily men (over 88%), with more than 15 years of experience (almost 48%). Their areas of activity include IT, cybersecurity, risk management, legal compliance, and data security. They primarily represent the IT, manufacturing, professional services, and trade sectors. Information regarding the respondents' country of origin was missing. According to the reviewer, the culture of the country may also influence respondents' behavior. As a result, several correlations were identified that provide interesting insights into these phenomena and shed new light on cybersecurity issues. Systematic audits, for example, led to overconfidence in security, which was also associated with excessive optimism. The candidate also noted (although not fully statistically confirmed) that the reporting process might influence the formation of cognitive biases. In cases where a manager reports to someone outside the IT department, a deeper understanding of the issue is necessary (involving "slow thinking") to explain the matter to someone outside the technology field. Previous experiences with attacks without significant negative consequences and increased awareness do not diminish cognitive errors, which the candidate had previously defined, and may even reinforce them. Although this conclusion requires further confirmation, it is a valuable research insight.

Thus, due to the ambiguity of the statistical results, it is difficult to confirm or reject the hypotheses(research questions) formulated by the candidate earlier. Additionally, the analysis of other researchers' results does not lead to clear conclusions. However, linking cybersecurity actions to the analysis of cognitive biases points to a significant research area, which the candidate has already partially explored.

The analysis of limitations made by the candidate in the final chapter of the dissertation, some of which were already mentioned in this review, is also worth emphasizing.

In the conclusion, the candidate addressed the research questions, comparing the results of his own research with findings available in the literature. The entire dissertation constitutes an engaging material for the reader. The careful approach to analysis, literature review, argumentation, and, finally, the research demonstrate the candidate's high competencies in the analyzed area. Unlike the evaluation of directors' competencies by managers (referred

to in the research results, the so-called "halo effect"), my evaluation is based on strong arguments found in the dissertation.

Nonetheless, I would also point out a few areas that could be improved. One of them is the excessive reliance on and constant reference to the work of other authors. This is evidenced by the 52 pages of references cited in the dissertation. On one hand, this is an expected requirement for PhD candidates; on the other hand, it may lead to the conclusion that the candidate is reluctant to develop independent arguments and refers every conclusion to a particular piece of literature. Finding the balance between these two areas is a significant challenge for a researcher. Another area concerns the repeated restating of content that has already been presented. Again, this makes it easy to follow the candidate's argument, but it could be beneficial to restructure the dissertation's narrative to reduce repetitive conclusions without compromising the substance.

Finally, I would like to suggest that the candidate focus on the Z and/or Alpha generations. Since these groups are underrepresented in the presented studies, focusing on younger individuals could lead to interesting conclusions, especially considering the ongoing changes in management models. The new generation is also taking on more leadership positions.

Somewhat anecdotal, but I would still like to ask: which of the cognitive biases analyzed by the candidate, mentioned at the beginning of the dissertation, did the candidate identify as one that also affected him during the writing process? It would be interesting if the candidate could address this question during the defense, providing supporting arguments.

Final Conclusion

The PhD dissertation by MA Marcin Wilczek, titled "Decision-Making under Constraints: A Behavioral Economics Perspective on Cyber-Related Heuristics and Biases," prepared under the supervision of dr. hab. prof. UG Monika Bąk, presents an original solution to a scientific problem based on the conducted research. I confirm that the candidate has a general theoretical knowledge required in the discipline of economics and finance and is capable of conducting independent analysis and synthesis of this knowledge. The research methods applied indicate a good understanding of the tools needed to address the research questions. It is also worth emphasizing that the candidate combines the ability to argue based on literature with a pragmatic approach to reality. Therefore, I confirm that the reviewed dissertation meets the statutory criteria required for PhD dissertations. I also recommend the candidate for public defense and suggest awarding the dissertation with a distinction and publishing it in a compact form after necessary abbreviations.