dr hab. Grzegorz Bełz

OCENA OSIĄGNIĘĆ

dr Joanny Antczak

ubiegającej się o nadanie stopnia doktora habilitowanego
w dziedzinie nauk społecznych w dyscyplinie nauk o zarządzaniu i jakości
w związku z postępowaniem habilitacyjnym wszczętym w dniu 28 października 2025 roku

I. Podstawy formalne recenzji

Podstawę formalną sporządzenia recenzji stanowi pismo dr hab. Agaty Mesjasz-Lech, prof. PCz., Przewodniczącej Rady Dyscypliny Naukowej Nauki o Zarządzaniu i Jakości Politechniki Częstochowskiej z dnia 20 stycznia 2026 roku informujące o wyznaczeniu mnie w dniu 10 grudnia 2025 roku przez Radę Doskonałości Naukowej na recenzenta w postępowaniu habilitacyjnym dr Joanny Antczak oraz powołaniu mnie w dniu 20 stycznia 2026 roku przez Radę Naukową Dyscypliny Nauki o Zarządzaniu i Jakości Politechniki Częstochowskiej w skład komisji habilitacyjnej.

Podstawą do przeprowadzenia oceny były następujące dokumenty oraz prace przesłane przez Habilitanta:

- wniosek dr Joanny Antczak do Rady Doskonałości Naukowej o przeprowadzenie postępowania w sprawie nadania stopnia doktora habilitowanego z dnia 28 października 2025,
- skan dyplomu doktora w dziedzinie nauk ekonomicznych w dyscyplinie ekonomii,
- autoreferat przedstawiający opis dorobku i osiągnięć naukowych opracowany w języku polskim,
- wykaz osiągnięć naukowych w tym monografii przedstawionej jako osiągnięcie naukowe stanowiące znaczny wkład w rozwój dyscypliny nauki o zarządzaniu i jakości, o którym mowa w art. 219 ust. 1 pkt 2 lit. a Ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce,
- oświadczenia współautorów,
- kopie dokumentów potwierdzających określone osiągnięcia,
- kopie pozostałych osiągnięć naukowych.

Recenzja niniejsza została opracowana w oparciu o wymogi określone w art. 219. Ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce (tekst jednolity w oparciu o Dz. U., 2022 rok, poz. 574; przywoływana dalej w tekście recenzji jako „Ustawa z dnia 20 lipca 2018 roku").

Udostępniona do recenzji monografia oraz zbiór publikacji stanowiących pozostały dorobek naukowo-badawczy uważam za zbiór pozwalający na dokonanie przeze mnie oceny osiągnięć naukowych Habilitantki. W powiązaniu z pozostałymi przedstawionymi powyżej danymi, w mojej ocenie dokumentacja jest kompletna a Habilitantka spełnia wymogi formalne dopuszczenia do postępowania habilitacyjnego. Oświadczam jednocześnie, że nie jestem współautorem żadnej z publikacji przedłożonych do niniejszej oceny.

Poniżej przedstawiam kolejno: podstawowe dane o przebiegu pracy naukowo-badawczej Habilitantki, ocenę osiągnięcia naukowego, ocenę istotnej aktywności naukowej a w zakończeniu przedstawiam konkluzje mojej oceny.

II. Podstawowe dane o przebiegu pracy naukowo-badawczej i dydaktycznej Habilitanta

Dr Joanna Antczak uzyskała w 2001 roku stopień magistra w Wyższej Szkoke Ubezpieczeń i Bankowości w Warszawie. W roku 2010 na podstawie przewodu doktorskiego, którego promotorem był prof. dr hab. Aldon Zalewski, uzyskała stopień naukowy doktora nauk ekonomicznych w zakresie ekonomii w Akademii Finansów w Warszawie w oparciu o pracę pt. „Wpływ controllingu na wyniki ekonomiczne przedsiębiorstw".

W okresie swojej pracy zawodowej pracowała w Akademii Finansów i Biznesu Vistula w Warszawie (2006-2015), Wojskowej Akademii Technicznej w Warszawie (2015-2018), Akademii Sztuki Wojennej w Warszawie (2018-2021) oraz ponownie Wojskowej Akademii Technicznej w Warszawie (gdzie pracuje obecnie od 2021).

Doświadczenie dydaktyczne Habilitantki obejmuje niemal dwie dekady pracy na kilku uczelniach, w tym w szczególności na Wojskowej Akademii Technicznej, Akademii Sztuki Wojennej oraz Akademii Finansów i Biznesu Vistula. W tym czasie prowadziła zajęcia we wszystkich podstawowych formach (wykłady, ćwiczenia, laboratoria, konwersatoria) na kierunkach Zarządzanie, Logistyka oraz Finanse i Rachunkowość. Uwagę zwraca szeroki zakres przedmiotów, wśród których znalazły się w szczególności: podstawy zarządzania, rachunkowość finansowa i zarządcza, mikro- i makroekonomia. Dzieli się także wiedzą z obszaru własnych zainteresowań badawczych, czego wyrazem jest prowadzenie konwersatorium z zarządzania cyberbezpieczeństwem na studiach Master of Business Administration w Akademii Finansów i Biznesu Vistula (Filia w Olsztynie).

Na uwagę zasługuje także umiejętność przekładania kompetencji eksperckich na nowatorskie formy kształcenia – w szczególności autorskie warsztaty z negocjacji multilateralnych, udokumentowane publikacjami naukowymi. Jakoś pracy dydaktycznej Habilitantki potwierdzają wyróżnienia (m.in. „Złota kreda" przyznana przez samorząd studencki ASzWoj w 2019 roku), a zaangażowanie w kształcenie kadr poświadcza opieka nad kilkudziesięcioma pracami dyplomowymi oraz pełnienie funkcji promotora pomocniczego w postępowaniach doktorskich. Całość świadczy o ugruntowanych i wszechstronnych kompetencjach dydaktycznych.

III. Ocena osiągnięcia naukowego dr Joanny Antczak

We wniosku o przeprowadzenie postępowania habilitacyjnego z dnia 28 października 2025 roku Habilitantka wskazała jako swoje osiągnięcie naukowe monografię pt. „Zarządzanie

cyberbezpieczeństwem w przedsiębiorstwie. Doświadczenia wybranych państw Unii Europejskiej".

W tej części recenzji skupiam się na ocenie ww. cyklu jako osiągnięcia naukowego w rozumieniu art. 219 ust. 1, pkt 2 lit. a Ustawy z dnia 20 lipca 2018 roku. Odnoszę się przy tym do zadeklarowanego przez Habilitantkę znacznego wkładu przedkładanego osiągnięcia w rozwój dyscypliny nauk o zarządzaniu i jakości.

Znaczenie i zasadność podejmowanej problematyki badawczej

Tematyka podjęta przez Habilitantkę – zarządzanie cyberbezpieczeństwem w przedsiębiorstwie, ujęte na tle doświadczeń państw Trójkąta Weimarskiego (Francja, Niemcy, Polska) – jest aktualna, doniosła i dobrze osadzona w bieżącym dyskursie zarówno praktyki, jak i teorii zarządzania.

Wybór tej tematyki znajduje silne uzasadnienie w skali i dynamice zjawiska, którego dotyczy. Według raportu Światowego Forum Ekonomicznego aż 72% badanych organizacji odnotowuje wzrost ryzyk cybernetycznych, przy czym ransomware pozostaje jednym z głównych zagrożeń, a niemal 47% wskazuje na zagrożenia wynikające z wpływu generatywnej sztucznej inteligencji jako swoją podstawową obawę (World Economic Forum, 2025). W ujęciu makroekonomicznym prognozy wskazują, że koszty cyberprzestępczości na świecie osiągnęły w 2025 roku około 10,5 bln USD rocznie, a najnowszy raport przewiduje ich dalszy wzrost do 12,2 bln USD rocznie do 2031 roku (Cybersecurity Ventures, 2025). Wielkości te czynią z zarządzania cyberbezpieczeństwem zagadnienie o pierwszorzędnym znaczeniu dla trwałości i konkurencyjności przedsiębiorstw, co uzasadnia podjęcie problemu w dyscyplinie nauki o zarządzaniu i jakości.

Trafność tematu wzmacnia jego strategiczno-zarządcze a nie wyłącznie techniczne ujęcie. Stanowisko globalnych firm doradczych potwierdza, że perspektywa przyjęta przez Habilitantkę odpowiada bieżącej praktyce ładu korporacyjnego. McKinsey na przykład wskazuje, że postrzeganie zarządzania ryzykiem cybernetycznym ewoluowało od inwestycji w unikanie straty ku traktowaniu cyberbezpieczeństwa, jako źródła przewagi konkurencyjnej i ochrony aktywów krytycznych, a rola dyrektora do spraw bezpieczeństwa informacji (CISO) przesunęła się z funkcji technologa ku partnerowi biznesowemu (McKinsey & Company, 2025). Aktualność problemu potęgują dwa zjawiska eksponowane także w monografii: ryzyko łańcucha dostaw oraz sztuczna inteligencja. Światowe Forum Ekonomiczne podaje, że 54% dużych organizacji uznaje wyzwania związane z łańcuchem dostaw za największą barierę osiągnięcia odporności cybernetycznej (WEF, 2025). Dobrze koresponduje to z trafnie dobranym przez Habilitantkę studium przypadku ataku NotPetya, ilustrującym ponadpaństwowy i łańcuchowy charakter współczesnych zagrożeń. Z kolei zwrócenie przez Habilitantkę uwagi na sztuczną inteligencję wpisuje się w obserwowaną przez IBM lukę w nadzorze nad tą technologią: aż 97% organizacji, które doświadczyły incydentu związanego ze sztuczną inteligencją, nie posiadało właściwej kontroli dostępu, a 63% nie miało żadnej polityki nadzoru nad nią (IBM, 2025). Podjęcie tych wątków świadczy o rozpoznaniu przez Habilitantkę najświeższych kierunków praktyki zarządzania.

Z kolei w warstwie teoretycznej zasadność tematu wynika z wyraźnego przesunięcia, jakie dokonuje się w naukach o zarządzaniu: cyberbezpieczeństwo przestaje być rozpatrywane jako problem działu informatyki, a staje się przedmiotem zarządzania strategicznego, nadzoru korporacyjnego i poniekąd kultury organizacyjnej. Nurt ten jest dziś intensywnie rozwijany w czołowych czasopismach z zakresu zarządzania. Przykładowo autorzy związani z konsorcjum

Cybersecurity at MIT Sloan dowodzą na łamach Harvard Business Review, że rady nadzorcze powinny przeformułować dyskusję o cyberbezpieczeństwie wokół wpływu na działalność biznesową i traktować wydatki na nie jako inwestycję strategiczną (Pearlson i Barsky, HBR, 2025). W najnowszych publikacjach diagnoza ta jest pogłębiana: organy nadzorcze powinny postrzegać cyberbezpieczeństwo mniej jako kwestię zgodności regulacyjnej, a bardziej jako problem konkurencyjnej odporności operacyjnej (Proudfoot i Madnick, HBR, 2026), zaś rozwój sztucznej inteligencji przekształca ryzyko cybernetyczne z problemu technicznego w sprawdzian przywództwa, wymagający od zarządów założenia kompromitacji systemów oraz budowania odporności (Gibson, HBR, 2026). Habilitantka, definiując problem badawczy jako pytanie o determinanty zarządzania cyberbezpieczeństwem i odwzorowując je na funkcje zarządzania, sytuuje swoje badania dokładnie w tym obszarze, istotnym z perspektywy teorii zarządzania.

Walorem teoretycznym jest również osadzenie cyberbezpieczeństwa w klasycznym aparacie pojęciowym nauk o zarządzaniu, czyli w funkcjach planowania, organizowania, przewodzenia i kontrolowania. Zabieg ten nadaje pracy spójność dyscyplinarną i pozwala jednoznacznie powiązać dorobek techniczno-normatywny z teorią organizacji. Należy jednak przy tym zastrzec, że zasadność teoretyczna podjętej tematyki nie jest tożsama z oryginalnością proponowanego rozwiązania. Przypisywanie kanonu funkcji kierowniczych wyłącznie ujęciu Griffina pomija jego rodowód sięgający Fayola, a samo odwzorowanie funkcji na obszar cyberbezpieczeństwa wymaga wykazania wartości dodanej wobec uznanych ram (NIST CSF, ISO/IEC 27001). Są to jednak kwestie oceny wkładu i metodyki odrębne od pytania o zasadność samej tematyki, która pozostaje wysoka.

Warto także zwrócić uwagę, że podejmowana przez Habilitantkę tematyka jest nie tylko istotna obecnie, ale pozostanie istotna w nadchodzącej przyszłości. Pierwszym czynnikiem przesądzającym o jej narastającej doniosłości jest sztuczna inteligencja, która przekształca krajobraz zagrożeń jednocześnie po stronie ataku i obrony. Światowe Forum Ekonomiczne wskazuje, że choć 66% organizacji oczekuje, iż sztuczna inteligencja wywrze najistotniejszy wpływ na cyberbezpieczeństwo w nadchodzącym roku, to jedynie 37% dysponuje procesami oceny bezpieczeństwa narzędzi opartych na tej technologii przed ich wdrożeniem (WEF, 2025). Luka ta zapowiada systemowe ryzyko narastające wraz z upowszechnieniem się technologii. Skutki finansowe są już mierzalne: według IBM wysoki poziom tak zwanego „*shadow* AI", to jest niekontrolowanego korzystania z nieautoryzowanych narzędzi sztucznej inteligencji, dodawał średnio 670 tys. USD do kosztu naruszenia danych (IBM, 2025). Najnowszy dyskurs zarządczy przesuwa zarazem ciężar problemu z warstwy technicznej na zarządczą: sztuczna inteligencja przekształca ryzyko cybernetyczne z problemu technicznego w wyzwanie dla systemów zarządzania, kultury organizacyjnej oraz przywództwa, wymagając od zarządów założenia kompromitacji systemów oraz budowania odporności i biegłości w zakresie tej technologii poza działem informatyki (Gibson, HBR, 2026). Podjęcie przez Habilitantkę wątku sztucznej inteligencji trafnie antycypuje zatem kierunek, w którym zmierza zarówno praktyka, jak i teoria zarządzania, czyniąc tematykę jej badań zarówno aktualną, jak i nabierającą coraz większego znaczenia.

Drugim czynnikiem o charakterze systemowym jest perspektywa technologii kwantowych, która redefiniuje horyzont planowania bezpieczeństwa informacji w przedsiębiorstwie. Wystarczająco wydajny komputer kwantowy, wykorzystując algorytm Shora, zdolny będzie złamać powszechnie stosowane szyfrowanie z kluczem publicznym (RSA, ECC), a konsensus prognostyczny lokuje tak zwany Q-Day około 2030 roku z odchyleniem rzędu dwóch lat (Federal Reserve Board, 2025). Zagrożenie ma jednak charakter natychmiastowy ze względu na model zbieraj teraz, odszyfruj

później (*harvest now, decrypt later*): napastnicy gromadzą zaszyfrowane dane już dziś, by odszyfrować je, gdy technologia kwantowa na to pozwoli, co czyni dane o wieloletnim okresie poufności narażonymi w chwili obecnej (Palo Alto Networks, 2025). W odpowiedzi amerykański NIST sfinalizował w sierpniu 2024 roku pierwsze trzy standardy szyfrowania postkwantowego, zachęcając organizacje do rozpoczęcia migracji (NIST, 2024), a regulacje europejskie (NIS2, DORA) coraz częściej wymagają kryptografii na najwyższym dostępnym poziomie oraz zwinności kryptograficznej. Dla zarządzania przedsiębiorstwem oznacza to konieczność strategicznego, wyprzedzającego planowania inwentaryzacji i wymiany infrastruktury kryptograficznej, a więc zadania o horyzoncie wieloletnim, lokującego się dokładnie w obszarze strategicznego planowania i oceny ryzyka wyodrębnionym w modelu Habilitantki.

Tematyka osiągnięcia jest więc aktualna, ważka praktycznie i dobrze zakorzeniona teoretycznie. Odpowiada na realny i narastający problem zarządczy o wymiarze finansowym, operacyjnym i geopolitycznym, a jednocześnie wpisuje się w wyraźnie zarysowany w światowej literaturze zarządczej zwrot ku traktowaniu cyberbezpieczeństwa jako strategicznego przedmiotu zarządzania i nadzoru. Aspekty takie jak sztuczna inteligencja oraz nadchodząca era obliczeń kwantowych dodatkowo wzmacniają prognozę rosnącej, a nie malejącej, doniosłości tej problematyki. Wybór państw Trójkąta Weimarskiego nadaje pracy walor komparatywny, użyteczny w kontekście europejskiej polityki regulacyjnej.

Z punktu widzenia recenzenta zasadność i znaczenie podjętej problematyki nie budzą wątpliwości i stanowią mocną stronę monografii; kwestią odrębną, rozstrzyganą w dalszych częściach oceny, pozostaje natomiast to, w jakim stopniu zrealizowane badania wnoszą oryginalny i znaczny wkład naukowy adekwatny do tak istotnego tematu.

Ogólna charakterystyka przedstawionego osiągnięcia naukowego

Habilitantka przedstawiła jako osiągnięcie monografię pt. „Zarządzanie cyberbezpieczeństwem w przedsiębiorstwie. Doświadczenia wybranych państw Unii Europejskiej".

W związku z powyższym w tej części recenzji skupiam się na ocenie tejże monografii jako osiągnięcia naukowego stanowiącego znaczny wkład w rozwój dyscypliny nauki o zarządzaniu i jakości w rozumieniu art. 219 ust. 1, pkt 2 lit. a Ustawy z dnia 20 lipca 2018 roku. Odnoszę się przy tym do przedstawionych w Autoreferacie Habilitantki deklaracji co do aspektów teoriopoznawczych, metodycznych oraz praktycznych stanowiących Jej zdaniem o znacznym wkładzie w rozwój dyscypliny nauk o zarządzaniu i jakości.

Analizowana monografia pt. „Zarządzanie cyberbezpieczeństwem w przedsiębiorstwie – doświadczenia wybranych państw Unii Europejskiej" (Difin, Warszawa 2024) składa się z wprowadzenia, pięciu rozdziałów, zakończenia, bibliografii oraz trzech załączników: słownika pojęć, kwestionariusza ankiety i kwestionariusza wywiadu eksperckiego. Każdy rozdział zawiera podrozdział zawierający podsumowanie i wnioski, a układ całości ma charakter sekwencyjny – od podstaw teoretycznych, przez kontekst zagrożeń i analizę porównawczą państw, po część empiryczną i propozycję modelu.

We wstępie monografii Habilitantka osadza tematykę w realiach cyfryzacji, wskazując ewolucję cyberbezpieczeństwa od obszaru niszowego do kluczowego elementu strategii bezpieczeństwa narodowego, gospodarczego i korporacyjnego oraz narastanie złożoności zagrożeń niezależnie od wielkości i branży przedsiębiorstwa. Problem badawczy ujęty został w postaci pytania: jakie

determinanty mają wpływ na zarządzanie cyberbezpieczeństwem w przedsiębiorstwie. Z problemu wyprowadzona została hipoteza główna o konieczności zidentyfikowania kluczowych determinant skutecznego zarządzania cyberbezpieczeństwem wobec dynamicznie zmieniających się zagrożeń oraz sześć hipotez szczegółowych (H1-H6), obejmujących między innymi integrację klasycznych funkcji zarządzania, wykorzystanie determinant do budowy modelu, rolę szkoleń i świadomości pracowników, znaczenie wyodrębnionego budżetu, zróżnicowanie podejść w zależności od cech przedsiębiorstwa oraz wyzwania związane ze sztuczną inteligencją. Habilitantka sformułowała cel główny jako identyfikację kluczowych determinant zarządzania cyberbezpieczeństwem, a także cele szczegółowe podzielone na poznawcze, metodyczne i utylitarne. Zadeklarowała wyznaczenie luki badawczej w toku krytycznego przeglądu literatury a także triangulację metod ilościowych oraz jakościowych w celu zwiększenia wiarygodności badań. Procedurę badawczą przedstawiła jako trzynastoetapowy schemat prowadzący od analizy literatury i dokumentów zastanych, przez badania jakościowe i ilościowe, do wizualizacji wyników oraz sformułowania wniosków, rekomendacji i propozycji modelu. Wstęp zamyka syntetyczna tabela zestawiająca treść poszczególnych rozdziałów z zastosowanymi metodami, realizowanymi celami i weryfikowanymi hipotezami.

Rozdział pierwszy, podzielony został na pięć podrozdziałów oraz podsumowanie. Ma on charakter wprowadzający i osadza problematykę cyberbezpieczeństwa w kontekście teorii zarządzania przedsiębiorstwem. Habilitantka omawia w nim koncepcje zarządzania jednostką gospodarczą, wskazując, że współczesne organizacje wymagają profesjonalizacji, rozwiązań systemowych i narzędzi wspierających, a kluczowe funkcje zarządzania obejmują planowanie, organizowanie, przewodzenie i kontrolowanie. Przedstawia zalety i wady omawianych koncepcji oraz wskazuje determinanty poszczególnych podejść, które mogą zostać wykorzystane przy budowie modelu zarządzania cyberbezpieczeństwem. Następnie definiuje zarządzanie cyberbezpieczeństwem, odwołując się do ujęcia funkcji zarządzania według Griffina i odwzorowując je na działania w obszarze ochrony informacji. Rozdział porządkuje także podstawowe pojęcia i definicje z zakresu cyberbezpieczeństwa oraz charakteryzuje środowisko, w którym funkcjonują i są narażone systemy informatyczne przedsiębiorstwa. Zamyka go omówienie wymagań w obszarze cyberbezpieczeństwa, jakim muszą sprostać przedsiębiorstwa. Warstwę dowodową stanowi analiza literatury oraz dokumentów, w tym aktów prawnych. Rozdział realizuje cele poznawcze i odnosi się do hipotez H1 oraz H2.

Rozdział drugi przedstawia rodzaje zagrożeń oraz aktorów występujących w cyberprzestrzeni, akcentując zróżnicowanie form cyberzagrożeń oraz znaczenie zrozumienia struktury kosztów i korzyści cyberprzestępczości i mechanizmów działania sprawców. Habilitantka omawia w nim wybrane modele zarządzania bezpieczeństwem IT, w tym model CIA oraz warstwowe i fundamentalne ujęcia bezpieczeństwa informacyjnego. Znaczącą część rozdziału poświęcono normalizacji, w szczególności rodzinie norm ISO/IEC 27000 – z normą ISO/IEC 27001 jako de facto standardem systemu zarządzania bezpieczeństwem informacji, jej nowym wydaniem z 2022 roku oraz powiązanymi normami ISO/IEC 27002, 27005 i 27032. Przedstawiono strukturę zabezpieczeń załącznika A tej normy, obejmującą zabezpieczenia organizacyjne, osobowe, fizyczne i technologiczne, proces zarządzania ryzykiem oraz logikę ciągłego doskonalenia. Trzeci wątek rozdziału stanowi zarządzanie kosztami cyberbezpieczeństwa przedsiębiorstwa. Wnioski rozdziału akcentują potrzebę wdrażania rygorystycznych praktyk niezależnie od wielkości organizacji, regularnych analiz zagrożeń i testów penetracyjnych oraz systematycznego budowania świadomości pracowników. Rozdział opiera się na analizie literatury, norm i danych

statystycznych dotyczących certyfikacji ISO, realizując cele metodyczne i odnosząc się do hipotez H2 oraz H4.

W rozdziale trzecim Habilitantka wprowadza perspektywę porównawczą międzynarodową, charakteryzując zarządzanie cyberbezpieczeństwem we Francji, w Niemczech i w Polsce. Habilitantka przedstawia genezę i charakterystykę Trójkąta Weimarskiego oraz uzasadnia wybór tych państw rolą Niemiec i Francji jako największych gospodarek Unii Europejskiej i pozycją Polski wśród nowych członków Unii. Rozdział omawia nakłady na cyberbezpieczeństwo w trzech krajach, sięgając do danych Eurostatu i Europejskiej Agencji Obrony, oraz zestawia wybrane wskaźniki rozwoju, w tym indeksy konkurencyjności i gotowości cyfrowej. W rozdziale tym przedstawione zostały także ramy prawne cyberbezpieczeństwa obowiązujące w Unii Europejskiej, w tym rola ENISA, oraz analiza krajowych strategii cyberbezpieczeństwa poszczególnych państw. Przeprowadzone porównanie służyć ma wypracowaniu rekomendacji prezentowanych w końcowej części pracy. Warstwę źródłową stanowią literatura, akty prawne, raporty firm audytorsko-doradczych oraz dane instytucjonalne.

Rozdział czwarty analizuje wpływ cyberataków na działalność przedsiębiorstwa, omawiając zróżnicowane formy zagrożeń, takie jak ransomware, phishing, wycieki danych i ataki zaawansowane, oraz wykorzystywanie przez sprawców nowych technologii, w tym sztucznej inteligencji. W pierwszej kolejności, na podstawie raportów firm audytorsko-doradczych, Habilitantka rekonstruuje krajobraz zagrożeń, ze szczególnym uwzględnieniem państw Trójkąta Weimarskiego oraz zróżnicowania ryzyk w zależności od wielkości przedsiębiorstwa. Następnie prezentuje przegląd ataków hakerskich w Europie i na świecie, by osadzić zagadnienie w szerszej perspektywie. Rdzeń empiryczny rozdziału stanowią dwa studia przypadku: atak NotPetya, omawiany jako wydarzenie istotne dla rozwoju myślenia o cyberbezpieczeństwie i zagrożeniach dla łańcuchów dostaw, oraz przypadek CD Projekt, ilustrujący podejście organizacji do incydentu i wdrażanie polityki zarządzania ryzykiem. Analiza obejmuje odrębnie wpływ ataku typu ransomware oraz typu wyciek danych na zarządzanie przedsiębiorstwem. Rozdział łączy analizę literatury, dokumentów zastanych i metodę studium przypadku, realizując cele metodyczne i utylitarne oraz odnosząc się do hipotez H3 oraz H4.

Rozdział piąty prezentuje wyniki ilościowych i jakościowych badań własnych. Część ilościową stanowią badania ankietowe zrealizowane techniką wywiadu telefonicznego na próbie 150 przedsiębiorstw, opisanej jako podmioty z branży informatycznej państw Trójkąta Weimarskiego, w oparciu o kwestionariusz złożony z 29 pytań jednokrotnego i wielokrotnego wyboru. Ankieta obejmowała dwa bloki tematyczne: zagadnienia ogólne zarządzania cyberbezpieczeństwem oraz zarządzanie nakładami finansowymi na cyberbezpieczeństwo, a charakterystykę próby przeprowadzono między innymi według akcjonariatu i rodzaju przedsiębiorstwa. Część jakościową tworzą wywiady eksperckie przeprowadzone na przełomie maja i czerwca 2024 roku w trzech obszarach: (a) trudności przedsiębiorców w zarządzaniu bezpieczeństwem informacji, (b) prawdopodobieństwa wystąpienia cyberataków w horyzoncie od roku do pięciu lat oraz (c) sztucznej inteligencji w kontekście cyberbezpieczeństwa. Na podstawie uzyskanych wyników Habilitantka wyodrębnia kluczowe determinanty zarządzania cyberbezpieczeństwem i formułuje propozycję autorskiego modelu, porządkującego przedmiot w siedmiu obszarach: strategiczne planowanie i ocena ryzyka, organizacja i alokacja zasobów, procesy operacyjne i ciągłe doskonalenie, kultura cyberbezpieczeństwa i edukacja, współpraca i wymiana informacji, kontrola i reakcja na cyberincydenty oraz adaptacja do zmieniających się warunków. Rozdział zamykają podsumowanie i wnioski. Odnosi się on do większości hipotez oraz hipotezy głównej.

W Zakończeniu Habilitantka odnosi się do realizacji celów i weryfikacji hipotez, wskazując potwierdzenie hipotezy głównej oraz wszystkich sześciu hipotez szczegółowych i zestawiając je z odpowiednimi tabelami i rysunkami. Rekapituluje zidentyfikowane kluczowe determinanty zarządzania cyberbezpieczeństwem oraz przypomina zaproponowany na ich podstawie model. Habilitantka sformułowała tu także zestaw rekomendacji adresowanych do kadry zarządzającej, dotyczących między innymi zwiększenia częstotliwości audytów bezpieczeństwa IT, regularności szkoleń, przejrzystości komunikacji wewnętrznej oraz integracji zarządzania bezpieczeństwem z innymi procesami organizacyjnymi. Część końcowa zawiera również świadomie wskazane ograniczenia badań w zakresie podmiotowym, czasowym oraz złożoności mierzonych zjawisk, a także kierunki dalszych badań inspirowane uzyskanymi wynikami. Habilitantka pozycjonuje przedstawione osiągnięcie jako pomost między teorią i ramami koncepcyjnymi a praktyką organizacyjną, w której cyberbezpieczeństwo staje się integralnym elementem strategii, zarządzania ryzykiem i procesów operacyjnych.

Ocena przedstawionego osiągnięcia naukowego

Przechodząc do oceny monografii pragnę powtórzyć, że Habilitantka trafnie rozpoznaje fakt, iż zarządzanie cyberbezpieczeństwem przestało być zagadnieniem rezerwowanym dla służb informatycznych, a stało się elementem zarządzania strategicznego, ryzykiem i ciągłością działania przedsiębiorstwa. Trafnie też zmianę tą czyni osią pracy, przenosząc cyberbezpieczeństwo z poziomu kwestii technicznej na poziom kategorii zarządczej osadzonej w dyscyplinie nauki o zarządzaniu i jakości.

Już sam wybór i ujęcie tematu należy ocenić pozytywnie – praca odpowiada na realne zapotrzebowanie poznawcze w polskim piśmiennictwie z zakresu zarządzania, w którym problematyka ta pozostaje rozpoznana w stopniu niewspółmiernym do jej wagi.

Na uznanie zasługuje rozległość i interdyscyplinarność ujęcia. Habilitantka konsekwentnie integruje perspektywy techniczną, prawną, organizacyjną, strategiczną oraz kulturową, dążąc do całościowego obrazu zjawiska, a nie do jego fragmentarycznego opisu. W warstwie konstrukcyjnej monografia jest spójna: od osadzenia pojęciowego, przez przegląd zagrożeń i uwarunkowań, po część empiryczną i propozycję autorskiego modelu. Habilitantka podjęła przy tym ambitną próbę zbudowania zintegrowanego modelu zarządzania cyberbezpieczeństwem, co – niezależnie od późniejszej oceny jego oryginalności i statusu metodologicznego – świadczy o dojrzałym zamyśle badawczym i woli wniesienia własnego, uporządkowanego wkładu, a nie jedynie zreferowania stanu wiedzy.

Wyróżnikiem pracy może być, przynajmniej na pierwszy rzut oka, jej wymiar empiryczny i porównawczy. Habilitantka przeprowadziła badania własne łączące metody ilościowe i jakościowe: badanie ankietowe, wywiady eksperckie oraz studia przypadku. Badaniami ankietowymi objęła przedsiębiorstwa z trzech państw Trójkąta Weimarskiego. Zamysł triangulacji metod oraz międzynarodowa, porównawcza perspektywa stanowią wartościowe i niełatwe organizacyjnie przedsięwzięcie badawcze, które wykracza poza typowy zakres opracowań krajowych i tworzy materiał o potencjale do dalszych analiz porównawczych. Komponent ten – z zastrzeżeniami, które będą przedmiotem szczegółowej analizy w dalszej części recenzji – należy uznać za jeden z istotnych atutów monografii.

Jako pozytywną, mocną stronę monografii uznaję również jej zorientowanie praktyczne oraz rzetelność warsztatową w kilku istotnych aspektach. Habilitantka formułuje rekomendacje adresowane do kadry zarządzającej i wskazuje możliwe zastosowania wyników w projektowaniu szkoleń, audytów i działań benchmarkingowych, co odpowiada utylitarnemu celowi pracy z obszaru nauk o zarządzaniu. Baza źródłowa jest szeroka i obejmuje aktualną literaturę międzynarodową oraz obowiązujące standardy i regulacje, a Habilitantka transparentnie wskazuje ograniczenia własnych badań oraz kreśli kierunki ich kontynuacji. Należy uznać, że jest przejawem dojrzałości badawczej i samokrytycyzmu.

Powyższe mocne strony wymagają jednak nie tylko rozpoznania zalet, lecz także wnikliwego rozważenia obszarów, w których przyjęte rozwiązania teoretyczne, metodologiczne i empiryczne budzą wątpliwości lub wymagają pogłębienia. Tym zagadnieniom poświęcona jest przedstawiona poniżej dalsza część mojej oceny.

Zatem przechodząc do słabości, grupuję je w cztery aspekty: podstawy teoretyczne, oryginalność modelu wobec uznanych ram, status metodologiczny modelu oraz próba badawcza.

Słabość teoretycznego rdzenia z obszaru nauk o zarządzaniu

Pierwszy aspekt dotyczy słabości teoretycznego rdzenia osiągnięcia, a więc odwzorowania zarządzania cyberbezpieczeństwem na funkcje zarządzania. Habilitantka opiera go wyłącznie na koncepcji R.W. Griffina, do którego odsyła formułą „według Griffina" i którego definicję cytuje niemal dosłownie (monografia, s. 82-84, tabela 9; autoreferat, tabela 2). Tymczasem czteroelementowy kanon funkcji zarządzania (planowanie, organizowanie, przewodzenie, kontrolowanie) nie jest oryginalną koncepcją Griffina, lecz klasycznym dorobkiem dyscypliny o rodowodzie wywodzącym się od Henriego Fayola, który jako pierwszy wyodrębnił funkcje kierownicze. Griffin jest autorem konkretnego ujęcia, co istotne – ujęcia podręcznikowego, na które praca słusznie się powołuje, lecz nie jest on twórcą samej klasyfikacji. W tekście brak jednak rozpoznania tej genezy. W pracy habilitacyjnej z nauk o zarządzaniu i jakości, w której znajomość kanonu jest elementarna, posłużenie się wyłącznie perspektywą jednego podręcznika sprawia wrażenie wywodu dydaktycznego, a nie poprawnie przeprowadzonych studiów literaturowych, które wykazywałyby ekspercki poziom wiedzy Habilitantki w tym umiejętność poprawnej rekonstrukcji ewolucji koncepcji i jej istoty.

Oryginalność modelu

Habilitantka prezentuje Model jako oryginalny konstrukt teoretyczny stanowiący istotny wkład w dyscyplinę nauk o zarządzaniu i jakości (autoreferat, podrozdział 4.1, wkład teoretyczny; monografia, rozdział 5, rysunki 62-63). Modelowi przypisuje jednocześnie funkcję opisową i normatywną oraz zdolność do diagnozowania dojrzałości organizacyjnej i identyfikacji obszarów do doskonalenia, a jako wartość dodaną wskazuje integrację elementów zarządzania strategicznego, a także zarządzania jakością, ryzykiem, wiedzą i projektami. Strukturalnie Model porządkuje przedmiot w siedmiu obszarach: strategiczne planowanie i ocena ryzyka, organizacja i alokacja zasobów, procesy operacyjne i ciągłe doskonalenie, kultura cyberbezpieczeństwa i edukacja, współpraca i wymiana informacji, kontrola i reakcja na cyberincydenty oraz adaptacja do zmieniających się warunków.

Każdy obszar Habilitantka uzupełniła kilkoma podelementami (np. wyspecjalizowana kadra, budżetowanie i inwestycje, struktura organizacyjna w obszarze drugim; TQM, Kaizen, Six Sigma, Lean Management, reengineering w obszarze trzecim), a relacje między obszarami zilustrowała liniami ciągłymi i przerywanymi opatrzonymi adnotacją „opracowanie własne". Deklarowana ranga konstruktu

(„oryginalny", „teoretyczny", o funkcjach normatywnych i diagnostycznych) wyznacza wysokie oczekiwania co do wykazania oryginalności autorskiego wkładu. Ocena tej deklaracji wymaga zestawienia Modelu z standardami, które obejmują ten sam przedmiot i które monografia sama przywołuje, a następnie wykazania, czy i w jakim zakresie Model wnosi coś, czego te standardy nie zapewniają.

Pierwszym z tych standardów jest NIST Cybersecurity Framework w wersji 2.0, opublikowany 26 lutego 2024 roku (NIST CSWP 29). Porządkuje on zarządzanie ryzykiem cyberbezpieczeństwa w trójpoziomowej hierarchii funkcji, kategorii i podkategorii. Na szczycie tej hierarchii znajduje się sześć funkcji: Govern, Identify, Protect, Detect, Respond i Recover. Funkcję Govern (w oficjalnym tłumaczeniu NIST: nadzór), której zakres odpowiada ładowi (organizacyjnemu) w zakresie cyberbezpieczeństwa, obejmując strategię zarządzania ryzykiem, role i odpowiedzialności, politykę oraz nadzór, wprowadzono jako szóstą i nadrzędną. Należy przy tym zwrócić uwagę, że polska terminologia związana z tłumaczeniem pojęcia *governance* pozostaje niejednoznaczna i poniekąd rozproszona. Spotyka się zarówno „nadzór", „ład" jak i „zarządzanie". W dalszej części recenzji, ze względu na zgodność z obowiązującym oficjalnym tłumaczeniem NIST, posługuję się terminem „nadzór".

Wagę funkcji nadzoru oddaje fakt, że obejmuje ona blisko trzydzieści procent ze stu sześciu podkategorii standardu, z silnym naciskiem na zarządzanie ryzykiem i łańcuch dostaw. Standard nie ogranicza się przy tym do warstwy pojęciowej: obok sześciu funkcji i dwudziestu dwóch kategorii NIST udostępnia poziomy wdrożenia (*tiers*) charakteryzujące rygor praktyk, profile (*profiles*) opisujące stan bieżący i docelowy, przykłady wdrożeniowe (*implementation examples*) przypisane do poszczególnych podkategorii oraz odniesienia informacyjne (*informative references*) mapujące ten standard na inne istniejące standardy, w tym na katalog zabezpieczeń NIST SP 800-53. Jest to zatem ustrukturyzowane, mierzalne i powiązane z resztą ekosystemu narzędzie diagnozy i planowania.

Norma ISO/IEC 27001:2022 reprezentuje uzupełniające podejście systemowe. Jej trzon stanowią obligatoryjne wymagania systemu zarządzania bezpieczeństwem informacji ujęte w klauzulach 4-10 (kontekst, przywództwo, planowanie, wsparcie, działania operacyjne, ocena skuteczności, doskonalenie), a Załącznik A zawiera dziewięćdziesiąt trzy zabezpieczenia uporządkowane w czterech kategoriach: organizacyjnej, osobowej, fizycznej i technologicznej. Wytyczne wdrożeniowe dla każdego zabezpieczenia dostarcza norma towarzysząca ISO/IEC 27002:2022, która objaśnia cel i sposób stosowania kontroli oraz wprowadza atrybuty pozwalające je klasyfikować. Rewizja z 2022 roku dodała jedenaście nowych zabezpieczeń odpowiadających współczesnym ryzykom, między innymi wywiad o zagrożeniach i bezpieczeństwo w chmurze.

Dobór zabezpieczeń odbywa się na podstawie oceny ryzyka i jest dokumentowany w deklaracji stosowalności (*statement of applicability*), a zgodność podlega niezależnej certyfikacji ważnej przez trzy lata, z corocznymi audytami nadzoru i audytem recertyfikacyjnym. Norma dostarcza więc nie tylko katalogu treści, lecz pełnego, audytowalnego mechanizmu uprawomocnienia. Oba omawiane standardy są przy tym komplementarne: NIST CSF dostarcza zorientowanej na ryzyko ramy strategicznej, a ISO/IEC 27001 certyfikowalnego systemu zarządzania.

Porównanie Modelu Habilitantki z powyższymi dwoma standardami ujawnia dysproporcję skali i głębi. Siedem obszarów Modelu Habilitantki odpowiada – w warstwie pojęciowej i bez wprowadzenia nowej szczegółowości – temu, co standardy ujmują w sposób nieporównanie bardziej rozbudowany. Strategiczne planowanie i ocena ryzyka pokrywają się z funkcjami nadzoru (*govern*) i identyfikacji oraz z klauzulami planistycznymi i organizacyjnymi zabezpieczeniami ISO. Organizacja i alokacja zasobów odpowiadają kategoriom ról, odpowiedzialności i zasobów oraz zabezpieczeniom organizacyjnym i

osobowym. Procesy operacyjne i ciągłe doskonalenie znajdują odzwierciedlenie w funkcjach ochrony i wykrywania oraz w klauzuli doskonalenia i zabezpieczeniach technologicznych. Kultura i edukacja odpowiadają zabezpieczeniom osobowym ISO i podkategoriom ochrony. Współpraca i wymiana informacji odpowiadają kategoriom łańcucha dostaw i komunikacji. Kontrola i reakcja na cyberincydenty odpowiadają z kolei funkcjom wykrywania, reagowania i odzyskiwania oraz zabezpieczeniom dotyczącym monitorowania i zarządzania incydentami. I w końcu adaptacja do zmieniających się warunków odpowiada mechanizmom doskonalenia, profilom i poziomom wdrożenia.

Każdy obszar Modelu ma zatem bezpośredni odpowiednik w tych dwóch przywołanych standardach, a równocześnie żaden z obszarów nie wnosi rozróżnień, których standardy by nie zawierały. Przeciwnie, tam, gdzie Model zatrzymuje się na siedmiu blokach z kilkoma hasłowymi podelementami, NIST oferuje sto sześć mierzalnych podkategorii, a ISO dziewięćdziesiąt trzy zabezpieczenia z wytycznymi wdrożeniowymi w normie towarzyszącej. Różnica nie jest niuansem redakcyjnym, lecz różnicą rzędu wielkości w zakresie szczegółowości, operacyjności i sprawdzalności.

Dysproporcja pogłębia się przy uwzględnieniu warstw, których w Modelu w ogóle brak. Standardy dostarczają mechanizmów pomiaru (poziomy i profile NIST, deklaracja stosowalności i audyt ISO), powiązań z innymi katalogami (odniesienia informacyjne NIST, mapowanie na SP 800-53) oraz wytycznych implementacyjnych dla każdej jednostki treści. Model nie zawiera żadnej z tych warstw – relacje między obszarami są autorskimi propozycjami graficznymi, a nie zależnościami wyprowadzonymi czy zmierzonymi, brak zaś jakiejkolwiek skali, wskaźnika lub narzędzia oceny. W tym świetle można postawić tezę, że Model jest wręcz uboższy od istniejących standardów i nie będzie to niestety figurą retoryczną, lecz uprawnionym wnioskiem strukturalnym.

Rozwijając ten aspekt należy podkreślić, że najbardziej wymowną luką Modelu wobec istniejących i uznanych standardów, jest brak nadzoru jako odrębnej, nadrzędnej funkcji. Jest to dokładnie ten element, który NIST w 2024 roku wyodrębnił i uczynił rdzeniem standardu, przypisując mu blisko jedną trzecią wszystkich podkategorii właśnie ze względu na jego fundamentalne znaczenie dla skuteczności pozostałych funkcji. W Modelu nadzór nie występuje jako kategoria pierwszorzędna, lecz rozprasza się pośrednio w obszarach strategicznego planowania i organizacji zasobów.

Słabość ta jest tym bardziej uderzająca, że profil naukowy Habilitantki dowodzi pełnej świadomości wagi tej problematyki biorąc pod uwagę, że w drugi nurt badawczy (patrz: Autoreferat) wprost analizuje systemy zarządzania z perspektywy wartości, w tym ładu korporacyjnego i strategii ESG. Wiedza o centralnej roli nadzoru i ładu była zatem dostępna, lecz nie znalazła odzwierciedlenia w architekturze Modelu.

A do tego dochodzi okoliczność warsztatowa wzmacniająca zarzut. W przeglądzie standardów (monografia, rozdział 2, tabela 18) Habilitantka opisuje NIST CSF jako ramę składającą się z pięciu głównych funkcji: identyfikacji, ochrony, wykrywania, reagowania i przywracania, a więc odwołuje się do wersji 1.1, mimo że wersja 2.0 z funkcją nadzoru jako szóstą i nadrzędną została opublikowana w lutym 2024 roku, a więc w roku wydania monografii. Oznacza to, że Model nie tylko nie dorównuje rygorem aktualnemu standardowi, lecz został skonfrontowany z jego nieaktualnym ujęciem, co osłabia argument o usytuowaniu pracy w aktualnym dorobku wiedzy w dyscyplinie. W postępowaniu toczącym się w latach 2025-2026 właściwym układem odniesienia jest więc NIST CSF 2.0, względem którego Model wypada znacznie słabiej.

Deklarowana wartość dodana Modelu – funkcje opisowa i normatywna oraz diagnoza dojrzałości organizacyjnej – pokrywa się z tym, co standardy zapewniają, i to w sposób operacyjnie pełniejszy. Funkcję opisowo-normatywną realizuje w NIST hierarchia funkcji, kategorii i podkategorii wraz z

przykładami wdrożeniowymi, a w ISO odzwierciadlają ją obligatoryjne wymagania systemu zarządzania wraz z katalogiem zabezpieczeń. Diagnozę dojrzałości zapewniają poziomy wdrożenia i profile NIST oraz cykl audytowy ISO z deklaracją stosowalności.

Tymczasem Model deklaruje zdolność diagnozowania dojrzałości, nie dostarczając ani skali dojrzałości, ani wskaźników, ani narzędzia oceny. Zadeklarowana funkcja diagnostyczna pozostaje więc obietnicą, a nie własnością konstruktu teoretycznego Habilitantki. Diagnoza dojrzałości wymaga mierzalnych poziomów odniesienia, których Model nie definiuje. Twierdzenie o przewadze lub choćby równorzędności względem tych uznanych standardów nie znajduje zatem oparcia w faktycznej zawartości Modelu.

Recenzowanemu osiągnięciu można więc zarzucić istotną słabość w kontekście oryginalności a co za tym idzie znacznego wkładu w rozwój dyscypliny. Być może błąd Habilitantki wynika z chęci zbudowania oryginalnego nowego konceptu „na siłę", gdy zasadne byłoby raczej rzetelne przeredagowanie jego statusu epistemologicznego – z oryginalnego konstruktu teoretycznego na syntezę porządkująco-dydaktyczną osadzającą cyberbezpieczeństwo w teorii zarządzania. Wymagałoby to natomiast znacznej rozbudowy składowych teorii zarządzania, w których cyberbezpieczeństwo możnaby osadzić. Odniesienie jedynie do funkcji zarządzania zdefiniowanych przez Fayola a przedstawionych jako model Griffina sugeruje, że wymagałoby to jednak poszerzonych studiów literaturowych.

Uwagi do metodyki budowy i walidacji modelu

W autoreferacie i monografii Habilitantka przedstawia Model jako oryginalny konstrukt teoretyczny o walorze empirycznym, mający pełnić funkcje opisowe i normatywne oraz służyć diagnozie dojrzałości organizacyjnej (Autoreferat - podrozdział 4.1, monografia - rozdział 5). Tymczasem pod względem metodyki budowy jest to rama koncepcyjna: zależności między siedmioma obszarami, oddane liniami ciągłymi i przerywanymi, są autorskimi propozycjami opatrzonymi adnotacją „opracowanie własne" (monografia – rysunek 62), a nie parametrami oszacowanymi na danych ani relacjami wyprowadzonymi w sposób sprawdzalny. W naukach o zarządzaniu i jakości termin „model" niesie oczekiwanie określonych, testowalnych relacji między konstruktami. Schemat blokowo-strzałkowy o charakterze typologii lub heurystyki spełnia funkcję porządkującą, lecz nie czyni go modelem zwalidowanym. Sednem mojej uwagi jest więc niezgodność między zadeklarowanym statusem epistemologicznym a faktycznym charakterem wytworu, nie zaś samo istnienie ramy, która jako synteza może mieć wartość poznawczą.

W tym sensie rozstrzygające znaczenie ma miejsce Modelu w przyjętej procedurze. Trzynastoetapowy schemat procesu badawczego (monografia – rysunek 1, Autoreferat - opis etapów) prowadzi od analizy literatury, przez badania jakościowe i ilościowe, do etapu wizualizacji wyników (tabele, wykresy, macierz SWOT) i dopiero na tej podstawie do sformułowania wniosków, rekomendacji oraz propozycji Modelu. Model jest zatem produktem końcowym syntezy, a nie przedmiotem odrębnego testu. W sekwencji etapów nie występuje krok ewaluacji Modelu – nie ma fazy, w której zaproponowana struktura siedmiu obszarów i relacji między nimi zostałaby skonfrontowana z danymi w celu potwierdzenia lub odrzucenia. Przy deklarowanym statusie konstruktu empirycznie ugruntowanego brak tego etapu jest istotną luką metodyczną – konstrukt ugruntowany empirycznie wymaga wyodrębnionej procedury ugruntowania, której Habilitantka nie zaprojektowała.

Część empiryczna opiera się na badaniu sondażowym techniką CATI (150 przedsiębiorstw, kwestionariusz 29 pytań jednokrotnego i wielokrotnego wyboru w dwóch blokach: zagadnienia ogólne oraz nakłady finansowe), uzupełnionym wywiadami eksperckimi oraz dwoma studiami przypadku (NotPetya, CD Projekt). Zastosowana analiza ogranicza się do statystyki opisowej. Habilitantka deklaruje

„analizę częstości i korelacje” oraz zestawienia porównawcze między krajami, a integrację wyników domyka macierzą SWOT. Brakuje natomiast operacjonalizacji siedmiu obszarów Modelu w mierzalne zmienne, modelu pomiarowego, modelowania równań strukturalnych oraz raportowania rzetelności (np. spójności wewnętrznej) i trafności (zbieżnej i różnicowej).

Co istotne, sam instrument pomiarowy nie został zaprojektowany do uchwycenia struktury Modelu: dwa bloki tematyczne kwestionariusza mierzą zagadnienia ogólne i nakłady finansowe, a nie siedem obszarów, które należałoby traktować jako konstrukty ukryte, trudno mierzalne, do badania których należałoby dopasować kwestionariusz. Powołanie się na triangulację metod (za Dźwigołem i Czakonem) podnosi wiarygodność ustaleń o samym zjawisku, lecz nie zastępuje walidacji struktury Modelu – triangulacja i walidacja konstruktu to dwie różne procedury o różnych celach.

Habilitantka stwierdza, że uzyskane wyniki pozwoliły na potwierdzenie postawionych hipotez. Hipotezy te są jednak szerokimi propozycjami jakościowymi: integracja funkcji zarządzania (H1), możliwość wykorzystania determinant do opracowania modelu (H2), wpływ szkoleń i świadomości (H3), rola wyodrębnionego budżetu (H4), różnice według wielkości, profilu i formy własności (H5) oraz wyzwanie sztucznej inteligencji (H6). Ich uprawdopodobnienie nie waliduje ani siedmioobszarowej struktury, ani relacji wewnętrznych Modelu, ponieważ żadna z hipotez nie odnosi się do tych relacji jako testowanych zależności.

Rozziew pogłębia zestawienie z tabelą 3 autoreferatu: hipotezy o najsilniejszym znaczeniu konstytutywnym dla Modelu, czyli H1 (integracja funkcji zarządzania) oraz H2 (wykorzystanie determinant do budowy modelu), zostały zweryfikowane w rozdziale pierwszym za pomocą analizy literatury i dokumentów, a więc konceptualnie, nie zaś w drodze badania empirycznego. Oznacza to, że fundament Modelu jest ugruntowany piśmienniczo, a badanie ankietowe (H3-H6) testuje zagadnienia przyległe, które nie odwzorowują architektury Modelu. Twierdzenie o empirycznym ugruntowaniu konstruktu nie znajduje zatem pokrycia w logice weryfikacji hipotez.

Ten aspekt warto poddać szerszej refleksji, być może również podczas kolokwium habilitacyjnego. Uważam, że można przyjąć, że w dyscyplinie nauk o zarządzaniu i jakości model przechodzący od koncepcji do statusu wytworu uprawomocnionego naukowo buduje się jedną z dwóch komplementarnych dróg. Droga konfirmacyjna (dedukcyjna) zakłada, że badacz najpierw precyzyjnie definiuje konstrukty i hipotezy, następnie operacjonalizuje je w mierzalne wskaźniki, konstruuje i oczyszcza narzędzie pomiarowe, zbiera dane na adekwatnej próbie i poddaje model dwustopniowej ocenie: najpierw modelu pomiarowego (rzetelność i trafność), potem modelu strukturalnego (siła i istotność relacji). Droga indukcyjno-konstrukcyjna opiera się na innym podejściu: teorię lub artefakt wyprowadza się z danych jakościowych w sposób jawny i odtwarzalny. Wspólnym mianownikiem obu dróg jest istnienie wyodrębnionego, jawnego etapu, w którym proponowana struktura zostaje skonfrontowana z materiałem empirycznym według określonych kryteriów. To właśnie ten etap odróżnia model zwalidowany od ramy koncepcyjnej i jego brak w ocenianym badaniu jest sednem niniejszej uwagi.

Uwagę tą wzmacnia fakt, że wzorzec poprawnego postępowania był Habilitantce bezpośrednio dostępny. Schemat własnego procesu badawczego opiera Ona na opracowaniu W. Dyducha „Ilościowe badanie i operacjonalizacja zjawisk w naukach o zarządzaniu” w tomie pod redakcją W. Czakona (monografia, rysunek 1, przypis źródłowy) a więc na tekście, którego przedmiotem jest właśnie operacjonalizacja i pomiar. Powołanie standardu operacjonalizacji przy jednoczesnym zaniechaniu operacjonalizacji konstruktów Modelu pogłębia niespójność metodyczną i utrudnia obronę tezy o empirycznym ugruntowaniu.

Istotę powyższego uchybienia należy określić jako poważną słabość metodyki budowy i walidacji Modelu, rzutującą na ocenę wkładu teoretycznego i empirycznego. Mamy tu bowiem do czynienia z niezgodnością deklarowanego statusu Modelu (konstrukt empirycznie ugruntowany, pełniący funkcje normatywne i diagnostyczne) z faktycznie zastosowaną metodyką jego budowy (synteza koncepcyjna zilustrowana statystyką opisową).

Uwaga ta koresponduje z ustaleniem dotyczącym oryginalności Modelu: nierozstrzygnięty status metodyczny i niewykazana oryginalność wzajemnie się wzmacniają, łącznie osłabiając przesłankę znacznego wkładu w rozwój dyscypliny.

Wiarygodność części empirycznej badania

Ostatnia z moich uwag dotyczy wiarygodności badan empirycznych. Po pierwsze opis sposobu doboru próby jest wewnętrznie sprzeczny, i to w obrębie jednego dokumentu. W autoreferacie, w opisie etapu doboru próby (s. 14), autorka stwierdza: „Zastosowałam metodę doboru celowego, biorąc pod uwagę wielkość organizacji, profil działalności oraz kraj pochodzenia". Jest to jednoznaczna deklaracja doboru nielosowego, w którym jednostki dobiera się celowo według przyjętych kryteriów. Dwie strony dalej (s. 16), w opisie badań ankietowych, ta sama próba 150 podmiotów opisana jest odmiennie: „Próba miała charakter probabilistyczny (zwany losowym). Dobór jednostek do próby przeprowadzono z zastosowaniem metody prostego losowania". Identyczne sformułowanie o charakterze probabilistycznym powtarza monografia (rozdział 5, s. 239). Obie charakterystyki wykluczają się wzajemnie: dobór celowy i proste losowanie to dwa rozłączne schematy doboru, oparte na odmiennych założeniach i prowadzące do odmiennych uprawnień wnioskowania. Sprzeczność ta nie jest niuansem terminologicznym, lecz dotyczy fundamentu całej części ilościowej, ponieważ od charakteru doboru zależy, co wolno z danych wywnioskować.

Co istotne, ciężar dowodu przechyla się ku wersji o doborze celowym. Udokumentowany w rysunku 35 przebieg gromadzenia danych: etapowy, rozłożony w czasie i ukierunkowany na konkretne sektory i kraje, jest charakterystyczny dla doboru celowego lub kwotowego, a nie dla losowania prostego z operatu. Deklaracja o losowaniu prostym wydaje się zatem opisem nieadekwatnym do faktycznie zastosowanej procedury, choć ostateczne rozstrzygnięcie należy oprzeć na dokumentacji badania.

Niezależnie od przyjętej wersji opisu doboru próby Habilitantka wyprowadza tę samą konkluzję: że „wyniki można uogólnić na całą populację", powołując się na Gerringa (2001). Tak rozumiana deklaracja uogólnialności wyników jest metodologicznie nieuprawniona niezależnie od tego, którą wersję doboru uznać za prawdziwą. Jeżeli dobór był celowy, wnioskowanie statystyczne do populacji jest wykluczone, gdyż próby nielosowe nie pozwalają na uprawnione wnioskowanie o populacji, a ustalenia interpretuje się analitycznie i kontekstowo, nie zaś jako oszacowania parametrów populacyjnych. Jeżeli zaś przyjąć deklarowane losowanie proste, uprawnione wnioskowanie statystyczne wymagałaby spełnienia warunków, których praca nie wykazuje: zdefiniowania populacji docelowej, dysponowania operatem losowania (kompletną listą jednostek populacji), z którego dokonano losowania, oraz raportowania stopy zwrotu i błędu szacunku przy określonym poziomie ufności.

Żaden z tych elementów nie został przedstawiony. Populacja „przedsiębiorstw z branży IT" trzech krajów nie jest zdefiniowana operacyjnie, nie wskazano operatu losowania, nie podano stopy zwrotu ani marginesu błędu, a sama liczebność 150 podmiotów rozłożona na trzy kraje daje przy wnioskowaniu statystycznym szerokie przedziały ufności. W rezultacie twierdzenie o uogólnialności wyników „na całą populację" pozostaje deklaracją nieugruntowaną. Warto przy tym odróżnić dwa pojęcia, które w pracy się zlewają: reprezentatywność próby (własność doboru zapewniająca odwzorowanie struktury populacji) oraz możliwość uogólniania wyników (uprawnienie do wnioskowania statystycznego o

populacji). Powołanie autorytetu metodologicznego nie zastępuje wykazania, że warunki wnioskowania statystycznego zostały spełnione.

Druga, poważniejsza moja wątpliwość dotyczy faktycznego składu próby. Zarówno nagłówkowo (monografia, s. 241: „W badaniu wzięło udział 150 przedsiębiorstw z branży informatycznej z państw Trójkąta Weimarskiego"), jak i w Autoreferacie próbę przedstawia się jako jednorodną, próbę sektora IT pochodzącą z trzech krajów. Tymczasem schemat badań ankietowych (monografia, rysunek 35, s. 240) ujawnia odmienny obraz. Dane gromadzono etapowo: w styczniu 2020 roku objęła ona 60 przedsiębiorstw branży logistycznej w Polsce. W listopadzie 2020 roku kolejne 40 przedsiębiorstw logistycznych w Polsce oraz dopytanie 60 wcześniejszych. W kwietniu 2022 roku została rozszerzona o 100 przedsiębiorstw z różnych branż (bez logistycznej) w Polsce. W listopadzie 2022 roku dodatkowe 50 przedsiębiorstw branży IT w Polsce. Natomiast w listopadzie 2023 roku objęła po 50 przedsiębiorstw branży logistycznej we Francji i w Niemczech.

Z zestawienia tego wynika, że sektor IT pojawia się wyłącznie w podpróbie polskiej (50 podmiotów), natomiast podpróby francuska i niemiecka (łącznie 100 podmiotów) obejmują branżę logistyczną. Jeżeli ostateczna próba 150 podmiotów to 50 firm IT z Polski oraz po 50 firm logistycznych z Francji i Niemiec, to deklaracja o „150 przedsiębiorstwach z branży informatycznej" jest nieścisła dla dwóch trzecich próby, a kluczowa dla pracy analiza komparatywna państw Trójkąta Weimarskiego porównuje w istocie polski sektor IT z francuskim i niemieckim sektorem logistycznym. W takim układzie różnice między krajami są nierozłącznie splecione z różnicami między sektorami (kraj współwystępuje z branżą), co uniemożliwia przypisanie obserwowanych różnic czynnikowi narodowo-kulturowemu lub instytucjonalnemu, deklarowanemu jako przedmiot porównania. Dodatkowo deklarowane okno czasowe badania (na przestrzeni dwóch lat: od listopada 2022 do listopada 2023) nie obejmuje wcześniejszych etapów rozpoczętych w styczniu 2020 roku, co dodatkowo zaciera pochodzenie ostatecznej próby.

Ze względu na wagę tego ustalenia formułuję je ostrożnie, gdyż opiera się ono na odczytaniu rysunku 35 a nie weryfikacji danych źródłowych. Jeżeli jednak rysunek 35 wiernie oddaje strukturę próby, niespójność między deklarowaną a faktyczną kompozycją próby podważa zarówno porównywalność międzynarodową, jak i wiarygodność opisu części empirycznej, a w konsekwencji ważność wniosków formułowanych jako ustalenia o sektorze IT trzech krajów.

Dodatkowo, abstrahując nawet od sprzeczności i niespójności, sama konstrukcja próby ogranicza zakres uprawnionego wnioskowania. Próba liczy 150 podmiotów rozłożonych na trzy kraje, koncentruje się na wąsko zdefiniowanych sektorach, opiera się na technice CATI i jest uzupełniona siedmioma wywiadami eksperckimi. Jest to baza wystarczająca dla rzetelnego opisu i wstępnej eksploracji, lecz zbyt wąska, by udźwignąć mocne uogólnienia o populacji czy stanowcze twierdzenia porównawcze. Ograniczenie to Habilitantka częściowo sama sygnalizuje w sekcji ograniczeń badań, co należy odnotować na jej korzyść. Problem polega na rozbieżności między tym przyznaniem a równoległymi deklaracjami o możliwości uogólniania i o jednorodnej próbie sektora IT. Dla porządku warto dodać, że ograniczona możliwość wnioskowania statystycznego pojedynczego badania tej skali nie jest sama w sobie wadą dyskwalifikującą. Wiele wartościowych badań ma charakter eksploracyjny. Wadą jest natomiast niezgodność deklarowanego statusu wyników z tym, na co pozwala przyjęta próba.

Trzy powyższe ustalenia układają się w spójny obraz osłabienia wiarygodności części empirycznej. Sprzeczność w opisie doboru jest uchybieniem warsztatowym, które samo w sobie podważa zaufanie do precyzji opisu metody. Nieuprawniona deklaracja uogólnialności wyników jest błędem metodologicznym w warstwie wnioskowania statystycznego, niezależnym od rozstrzygnięcia

sprzeczności. Niespójność składu próby jest z kolei o tyle poważna, że dotyka trafności samego rdzenia badania porównawczego. Łącznie mankamenty te rzutują na to, w jakim stopniu wyniki ilościowe mogą uzasadniać formułowane wnioski oraz – pośrednio – stanowić deklarowane „empiryczne ugruntowanie" Modelu, co wiąże się z ustaleniami dotyczącymi metodyki budowy i walidacji Modelu. Charakter tego uchybienia należy określić jako rzutujący na wiarygodność części empirycznej.

Ocena wkładu w rozwój nauk o zarządzaniu i jakości

Monografia zgłoszona przez Habilitantkę jako osiągnięcie stanowiące znaczny wkład w rozwój nauk o zarządzaniu i jakości adresuje niewątpliwie ważną i aktualną tematykę, której znaczenie będzie rosło. Habilitantka objęła badaniami przedsiębiorstwa z trzech państw Trójkąta Weimarskiego co wraz z zamysłem triangulacji metod, stanowi wartościowe i niełatwe organizacyjnie przedsięwzięcie badawcze. Niestety zarówno w obszarze teoriotwórczym, metodycznym oraz badawczym Jej osiągnięcia występują istotne słabości i wady. Po pierwsze, w warstwie teoretycznej, koncepcji Habilitantki należy zarzucić brak oryginalności i przyrostowego wkładu koncepcyjnego jej Modelu wobec uznanych na świecie ram NIST CSF 2.0 i ISO/IEC 27001:2022. Po drugie, w warstwie metodycznej, poważną wadą jest niezgodność deklarowanego statusu Modelu jako konstruktu zwalidowanego z faktycznie zastosowaną metodyką syntezy zilustrowanej statystyką opisową. Po trzecie, istotną wadą w warstwie badawczej jest sprzeczny z deklarowanym przez Habilitantkę charakter próby badawczej, co dotyka nie tylko sposobu doboru, ale także faktu przynależności 2/3 przedsiębiorstw do odmiennego od deklarowanego sektora co dyskwalifikuje wartość porównań i wniosków.

Kierując się powyższym konkluduję, iż zgłoszona monografia nie daje podstaw do uznania jej za osiągnięcie stanowiące znaczny wkład dr Joanny Antczak w rozwój dyscypliny nauk o zarządzaniu i jakości w rozumieniu art. 219 ust. 1 pkt 2 lit. a Ustawy z dnia 20 lipca 2018 roku.

IV. Ocena aktywności naukowej dr Joanny Antczak

Poniżej skupiam się na ocenie aktywności naukowej Habilitantki. Zgodnie z art. 219 ust. 1 pkt 3 Ustawy z dnia 20 lipca 2018 roku w postępowaniu habilitacyjnym ocenie podlega fakt wykazywania się istotną aktywnością naukową.

Przedstawiona dokumentacja pozwala na ocenę dorobku Habilitantki w zakresie pozostałej aktywności naukowej poza monografią zgłoszoną jako osiągnięcie główne.

Działalność naukowo-badawcza Habilitantki prowadzona po uzyskaniu stopnia doktora układa się w dwa wzajemnie dopełniające się nurty tematyczne. Pierwszy to zarządzanie organizacją w środowisku cyfrowym i niepewnym, ujmowane jako cyfrowo-strategiczne zarządzanie ryzykiem. Obejmuje zarządzanie cyberbezpieczeństwem w przedsiębiorstwie, zarządzanie informacją, wiedzą i technologią oraz funkcjonowanie organizacji w warunkach niepewności i turbulencji otoczenia. Drugi nurt dotyczy strategicznego zarządzania odpowiedzialnością i bezpieczeństwem narodowym. Grupuje problematykę zrównoważonego rozwoju (ESG, CSR) oraz zarządzania w sektorze zbrojeniowym i obszarze bezpieczeństwa państwa. Tak zarysowana mapa zainteresowań cechuje się interdyscyplinarnością, łącząc nauki o zarządzaniu i jakości z ekonomią obronną i problematyką bezpieczeństwa, co należy uznać za walor świadczący o dojrzałości koncepcyjnej, choć wymagający czujności co do spójności metodologicznej między tak różnymi polami.

Dorobek publikacyjny zadeklarowany w wykazie osiągnięć obejmuje, obok monografii stanowiącej osiągnięcie, trzy monografie indywidualne, cztery monografie współautorskie oraz dwie publikacje pod redakcją Habilitantki, a ponadto 24 rozdziały w monografiach i 31 artykułów w czasopismach naukowych. Wśród czasopism odnotować można pozycje rozpoznawalne w dyscyplinie, jak Przegląd Organizacji, Zeszyty Naukowe Politechniki Śląskiej, Organizacja i Zarządzanie czy European Research Studies Journal. W dorobku Habilitantki przeważają publikacje krajowe oraz teksty współautorskie co jednak nie jest w żadnym stopniu zarzutem.

Aktywność konferencyjna Habilitantki można uznać za intensywną i systematyczną. Obejmuje zarówno wystąpienia na konferencjach krajowych (m.in. cykl Przedsiębiorstwa przyszłości polskiego przemysłu obronnego, Nowoczesne metody zarządzania, Multimedia w biznesie i administracji) oraz na arenie międzynarodowej, w tym w ramach kolejnych edycji konferencji IBIMA (Madryt, Grenada, Kordoba), gdzie Habilitantka pełniła także funkcję recenzenta. Uczestnictwo to wspiera przesłankę istotnej aktywności realizowanej w więcej niż jednej jednostce, w szczególności zagranicznej.

Wymiar mobilności naukowej dokumentują trzy staże. Najistotniejszy z perspektywy dyscypliny jest staż na Wydziale Zarządzania Politechniki Częstochowskiej (w okresie marzec-wrzesień 2023) pod opieką dr hab. inż. Joanny Nowakowskiej-Grunt, prof. PCz, którego wymiernym efektem były wspólne publikacje. Staż badawczy w Departamencie Innowacji i Rozwoju Technologicznego Polskiej Grupy Zbrojeniowej S.A. (w okresie styczeń-maj 2020) miał charakter aplikacyjny i powiązał aktywność naukową z praktyką sektora obronnego. Uzupełnia je wcześniejszy wyjazd szkoleniowy Erasmus na Fatih University w Turcji (w 2013 roku).

Habilitantka wykazuje się również aktywnością projektową i organizacyjną. Uczestniczy w międzynarodowym projekcie DIMAS (Erasmus+, 2023-2026), a w macierzystych jednostkach kierowała kilkoma zadaniami i grantami badawczymi (m.in. uczelniane granty badawcze WAT oraz zadania Akademii Sztuki Wojennej), co świadczy o zdolności do samodzielnego prowadzenia zespołów. Należy do Komisji Nauk Organizacji i Zarządzania Oddziału PAN w Katowicach (kadencja 2023-2026), Polskiego Towarzystwa Ekonomicznego oraz Naukowego Towarzystwa Informatyki Ekonomicznej. Pełni funkcje redakcyjne (Wiedza Obronna, redaktor tematyczny w czasopiśmie Nowoczesne Systemy Zarządzania) i recenzyjne (dziewięć recenzji czasopiśmienniczych, w tym dwie międzynarodowe, oraz recenzja monografii). Aktywność tę dopełnia współpraca z otoczeniem gospodarczym, w tym wdrożenia i audyty w spółkach grupy kapitałowej.

Pozostałą, wobec monografii zgłoszonej jako osiągnięcie, aktywność naukową Habilitantki obrazują kluczowe wskaźniki bibliometryczne, które według stanu na 2 października 2025 roku, kształtują się następująco: w bazie Google Scholar 90 cytowań przy indeksie Hirscha 4, w ResearchGate 64 cytowania przy indeksie 4. W bazach indeksowanych międzynarodowo wartości te wynoszą: 3 cytowania w bazie Scopus (h = 1), 1 cytowanie w bazie Web of Science (h = 1). Obraz ten wymaga wyważonej interpretacji. Dorobek jest rozpoznawalny w krajowym obiegu naukowym, lecz jego międzynarodowe oddziaływanie pozostaje ograniczone, co jest typowe dla dyscypliny i profilu publikacyjnego osadzonego w czasopismach krajowych. Kierunkiem wzmacniającym pozycję naukową byłoby zwiększenie udziału publikacji w czasopismach o wysokim współczynniku wpływu, indeksowanych w Scopus i Web of Science, co może stanowić obszar dalszego rozwoju aktywności naukowej Habilitantki.

Podsumowując ten element oceny uważam, że pozostałą aktywność naukową Habilitantki należy ocenić jako bogatą, wieloaspektową i konsekwentnie rozwijaną, dobrze udokumentowaną w zakresie mobilności, działalności projektowej i organizacyjnej oraz spełniającą przesłankę aktywności realizowanej w więcej niż jednej instytucji. Zidentyfikowane ograniczenia, a więc umiarkowane wskaźniki

cytowań w bazach międzynarodowych oraz przewaga prac współautorskich, nie podważają wartości dorobku, lecz wyznaczają racjonalne kierunki jego dalszego umiędzynarodowienia.

V. Konkluzja oceny

W oparciu o przeprowadzoną ocenę osiągnięć dr Joanny Antczak stwierdzam, że monografia pt.: „Zarządzanie cyberbezpieczeństwem w przedsiębiorstwie. Doświadczenia wybranych państw Unii Europejskiej" podejmuje tematykę niewątpliwie ważną, aktualną o rosnącym znaczeniu, a samo przedsięwzięcie badawcze – objęcie badaniami przedsiębiorstw z trzech państw Trójkąta Weimarskiego przy zamyśle triangulacji metod – należy uznać za wartościowe i organizacyjnie wymagające.

Walory te nie równoważą jednak istotnych słabości i wad ujawniających się we wszystkich trzech kluczowych warstwach osiągnięcia. W warstwie teoriotwórczej autorskiemu Modelowi należy zarzucić brak oryginalności i przyrostowego wkładu koncepcyjnego względem uznanych na świecie ram, wobec których stanowi on uboższe, porządkujące odwzorowanie pozbawione warstwy operacyjnej i mechanizmu uprawomocnienia. W warstwie metodycznej poważną wadą jest niezgodność deklarowanego statusu Modelu jako konstruktu zwalidowanego z faktycznie zastosowaną metodyką syntezy zilustrowanej statystyką opisową, która nie spełnia warunków walidacji w żadnym z uznanych paradygmatów. W warstwie badawczej istotną wadą jest sprzeczny z deklaracjami Habilitantki charakter próby, dotykający nie tylko sposobu doboru, lecz także struktury sektorowej, w której przynależność dwóch trzecich przedsiębiorstw do sektora odmiennego od deklarowanego dyskwalifikuje wartość porównań i rzetelność formułowanych wniosków. Na tej podstawie oceniam, że zgłoszona monografia nie daje podstaw do uznania jej za osiągnięcie stanowiące znaczny wkład dr Joanny Antczak w rozwój dyscypliny nauk o zarządzaniu i jakości w rozumieniu art. 219 ust. 1 pkt 2 lit. a Ustawy z dnia 20 lipca 2018 roku.

Równocześnie pozostałą aktywność naukową, dydaktyczną oraz organizacyjną Habilitantki w okresie od czasu uzyskania stopnia doktora oceniam jako wysoką.

Uwzględniając powyższe, w świetle ustawy z dnia 20 lipca 2018 roku, oceniam, iż przedstawione osiągnięcie naukowe Habilitantki nie spełnia kryteriów określonych w art. 219 tejże Ustawy. Wyrażam zatem negatywną opinię w sprawie nadania dr Joannie Antczak stopnia naukowego doktora habilitowanego w dziedzinie nauk społecznych w dyscyplinie nauk o zarządzaniu i jakości.

Wrocław, 18 czerwca 2026

Grzegorz Bełz