Identyfikacja luki cyfrowej

2024

oraz zagrożeń wynikających z wprowadzania technologii cyfrowych do przedsiębiorstw

Przegląd międzynarodowy i krajowy

Platforma Przemysłu Przyszłości

2024

Identyfikacja luki cyfrowej

oraz zagrożeń wynikających
z wprowadzania technologii cyfrowych
do przedsiębiorstw

Przegląd międzynarodowy i krajowy

Warszawa, styczeń 2024

Platforma
Przemysłu
Przyszłości

Materiał przygotowany w ramach prac grupy ds. Identyfikacji zagrożeń związanych z cyfryzacją Fundacji Platforma Przemysłu Przyszłości

Opracowali:
prof. dr hab. Marian Gorynia
dr hab. Joanna Kuczewska
gen. broni (w st. spocz.) dr Andrzej Fałkowski
dr hab. Krzysztof Pietrusewicz, prof. ZUT

Redakcja:
dr Piotr Kryjom
Zastępca Dyrektora
Dział Zarządzania Wiedzą

Fundacja Platforma Przemysłu Przyszłości
ul. Malczewskiego 24
26-609 Radom

Platforma Przemysłu Przyszłości

Przedmowa

Niniejsze opracowanie jest jednym z dwóch raportów dotyczących zagrożeń wprowadzania technologii cyfrowych do przedsiębiorstw. Pierwszy raport dotyczy identyfikacji luki cyfrowej oraz zagrożeń wynikających z wprowadzania technologii cyfrowych do przedsiębiorstw, natomiast drugi raport zawiera rekomendacje i praktyczne zalecenia. Pierwszy raport ma charakter teoretyczny i definiuje podstawowe koncepcje oraz pojęcia, natomiast raport drugi odnosi się do praktycznych aspektów działania przedsiębiorstwa i wskazuje najważniejsze zagrożenia zarówno w odniesieniu do poszczególnych technologii cyfrowych jak i procesów biznesowych. Na szczególną uwagę zasługują rekomendacje, które odnoszą się zarówno do polityki gospodarczej oraz działania samorządu gospodarczego jak i praktyki działania poszczególnych przedsiębiorstw.

Wybór tego tematu nie był przypadkowy. Od kilku lat obserwujemy proces przyspieszonej transformacji cyfrowej polskiej gospodarki. Odbywa się on pod wpływem naturalnego trendu wykorzystania nowych technologii cyfrowych i włączania polskich przedsiębiorstw do globalnych łańcuchów wartości. Na ten proces nakładają się także skutki kryzysu pandemicznego COVID-19 oraz rozwój zagrożeń wynikających z wojny w Ukrainie. W tej sytuacji kluczowe wydaje się pogłębienie refleksji na temat przemyślanego wprowadzania nowych rozwiązań do przedsiębiorstw uwzględniającego nie tylko krótkoterminowe cele związane z podnoszeniem efektywności, ale również zagrożenia związane z interesem publicznym i bezpieczeństwem narodowym.

Oddajemy w Państwa ręce raport dotyczący identyfikacji luki cyfrowej oraz zagrożeń wynikających z wdrażania nowych technologii cyfrowych do przedsiębiorstw. Niniejsza publikacja jest kolejnym opracowaniem powstałym w ramach prac think tanku powołanego przez Platformę Przemysłu Przyszłości. Tym razem skoncentrowaliśmy się na zagrożeniach jakie związane są z nowymi technologiami oraz ich wpływie na przedsiębiorstwo oraz jego otoczenie. W tym przypadku zagrożenia dotyczące pojedynczych podmiotów są także rozpatrywane z punktu widzenia całej gospodarki i bezpieczeństwa narodowego.

Chciałbym bardzo podziękować autorom, Panu prof. Marianowi Goryni, Pani dr hab. Joannie Kuczewskiej, Panu gen. broni (w st. spocz.) dr Andrzejowi Fałkowskiemu oraz Panu dr hab. Krzysztofowi Pietrusewiczowi, za przekazaną wiedzę, otwartość i zaangażowanie. Mam nadzieję, że publikacja spotka się z Państwa życzliwym zainteresowaniem i pozytywnym odbiorem.

dr Piotr Kryjom
Zastępca Dyrektora
Działu Zarządzania Wiedzą

Spis treści

Streszczenie

Celem opracowania jest wskazanie zagrożeń związanych z wprowadzaniem technologii cyfrowych do przedsiębiorstw w kontekście bezpieczeństwa państwa. Szczególna uwaga została poświęcona małym i średnim przedsiębiorstwom (MŚP), których podstawę działalności stanowi działalność produkcyjna. Cyfryzacja z jednej strony jest wielką szansą dla MŚP, ponieważ może prowadzić do zwiększenia wydajności, produktywności i efektywności ich działań, szczególnie biorąc pod uwagę wysoką elastyczność działania i szybkość reagowania na zmiany. Z drugiej jednak strony procesom digitalizacji towarzyszą liczne zagrożenia, których rozpoznanie stanowi podstawę do budowania strategii zapobiegania im, albo zmniejszenia poziomu ich dolegliwości i rozmiarów. Przyjęte zostało również autorskie rozumienie bezpieczeństwa państwa, które w szerokim znaczeniu wiąże się z zapewnieniem konkurencyjności sektora MŚP.

Na podstawie studiów literatury, dorobku organizacji międzynarodowych i krajowych oraz instytucji i przedsiębiorstw jako kluczowe technologie cyfrowe autorzy przyjęli następujące: Internet Rzeczy (Internet of Things), łańcuch bloków (Blockchain), Internet nowej generacji (5G), chmura obliczeniowa (Cloud computing), sztuczna inteligencja (Artificial Intelligence) i uczenie maszynowe (Machine Learning), analiza danych i analiza dużych zbiorów danych (Big Data), cyberbezpieczeństwo, superkomputery i komputery kwantowe, cyfrowe modelowanie i produkcja (Digital Modeling and Fabrication) oraz systemy autonomiczne i robotyzacja. Wykorzystując koncepcję luki cyfrowej, która bazuje na eklektycznej definicji konkurencyjności przedsiębiorstwa autorzy zdiagnozowali podstawowe zagrożenia związane z wdrażaniem technologii cyfrowych. „Zasypanie owej luki cyfrowej" jest jednym z kluczowych wyzwań stojących przed MŚP. Dzięki przyjęciu określonego modelu postępowania prowadzącego do minimalizacji luki cyfrowej, firmy są w stanie eliminować zagrożenia związane np. z przerastającymi kompetencje firmy wyzwaniami metodologicznymi bądź technologicznymi. Jednym z takich modeli jest ADMA. Na bazie tego modelu zidentyfikowane zostały szanse i zagrożenia oraz precyzyjnie wskazane zostały obszary wdrażania technologii cyfrowych. Zagrożenia dotyczą różnych obszarów działalności przedsiębiorstwa i wiążą się ze zmniejszeniem potencjału konkurencyjnego, tym samym ograniczając możliwości osiągania przewag konkurencyjnych. Brak lub niejasno zdefiniowana strategia cyfryzacji przedsiębiorstwa może być przyczyną ograniczonej akceptacji zmian wynikających z tej strategii wśród pracowników. Negatywny efekt mogą wzmocnić również ograniczone kompetencje cyfrowe pracowników lub ich brak. Ponadto źródłami zagrożeń mogą być: konieczność dostosowania się do zmian rynkowych, konkurencja ze strony dużych firm – np.: udział w łańcuchach dostaw oraz zależność od dostawców technologii w związku z koniecznością stałego aktualizowania technologii i wiedzy o ich rozwoju. Istotnym wyzwaniem dla MŚP jest brak lub ograniczona standaryzacja i kompatybilność systemów w związku z wprowadzeniem nowych technologii cyfrowych a także wysokie koszty inwestycji związane z zakupem oprogramowania i wdrażania technologii cyfrowych we wszystkich obszarach ADMA. W końcu wdrażanie nowych technologii cyfrowych wywoływać może problemy związane z prywatnością danych oraz zwiększać zagrożenia związane z cyberbezpieczeństwem.

Funkcjonowanie gospodarki narodowej, czyli de facto państwa w wymiarze gospodarczym nie jest prostą sumą działań indywidualnych przedsiębiorstw, ale może tutaj wystąpić zarówno pozytywny, jak i negatywny efekt synergii. Państwo jest ważnym komponentem tego, co dzieje się na poziomie wyższym, czyli całej gospodarki i dlatego problematyka jego bezpieczeństwa pojawia się jako istotny kontekst procesów konkurowania zachodzących na poziomie przedsiębiorstw i branż, które one konstytuują. Najważniejsze czynniki i wyzwania, które dotyczą tego poziomu to: zagrożenia cyberbezpieczeństwa i cyberataki, incydenty i obrona cybernetyczna oraz zamachy na narodową infrastrukturę krytyczną. Ponadto to regulacje prawne zarządzania ryzykiem cyfrowym, szkolenia i konieczność podnoszenia świadomości cyfrowej oraz zagrożenia dla rynku pracy wynikające z automatyzacji i cyfryzacji procesów.

Jeżeli chodzi o stronę metodyczną, to opracowanie bazuje głównie na danych wtórnych zebranych na podstawie literatury przedmiotu a także nawiązuje do doświadczenia eksperckiego autorów zbudowanego w ramach realizacji konkretnych projektów analitycznodoradczych.

Abstract

The primary objective of this study is to investigate the potential threats related to the integration of digital technologies into enterprises, emphasizing their implications for state security. Particular emphasis is placed on small and medium-sized enterprises (SMEs) primarily engaged in manufacturing activities. On the one hand, digitalisation presents a noteworthy opportunity for SMEs, offering the prospect of heightened operational efficiency, productivity, and overall effectiveness. This is particularly relevant given the inherent flexibility and rapid adaptability of SMEs to changing circumstances. However, concurrently, the process of digitization is fraught with manifold risks. The identification of these risks serves as the foundational bedrock for constructing strategies aimed at either preemptively averting their occurrence or mitigating their impact and scale. Additionally, the study subscribes to the author's conceptualization of state security, which is comprehensively inter-twined with the imperative of ensuring the competitiveness of the SME sector.

Drawing from an extensive review of literature, insights from international and national organizations, as well as inputs from various institutions and companies, the authors have identified key digital technologies. These include: the Internet of Things (IoT), Blockchain, Next Generation Internet (5G), Cloud Computing, Artificial Intelligence (AI) and Machine Learning (ML), Data Analytics and Big Data, Cybersecurity, Supercomputing and Quantum Computing, Digital Modelling and Fabrication, and Autonomous Systems and Robotization. Employing the concept of the digital gap, rooted in an inclusive definition of a company's competitiveness, the authors have conducted a diagnostic analysis of the primary risks entailed by the integration of digital technologies. Addressing this digital gap emerges as a pivotal challenge for SMEs. By embracing a tailored behavioural model aimed at minimizing the digital gap, enterprises can effectively mitigate risks associated with methodological or technological challenges that may exceed the company's competence. The ADMA model stands out as one such paradigm. Built upon the ADMA model, the study identifies both opportunities and threats, meticulously pinpointing areas conducive to the implementation of digital technologies. Threats manifest across diverse facets of a company's operations, correlating with a weakening of competitive potential and, consequently limiting the opportunities to achieve competitive advantages. The absence or unclearly defined digitisation strategy of a company may be the reason for limited acceptance of the changes resulting from this strategy among employees. The negative effect may also be reinforced by limited or non-existent digital competences of employees. Furthermore, challenges manifest in the imperative for adaptability to market dynamics, competition from larger enterprises especially in the context of supply chain participation and dependence on technology suppliers due to the need for constant updating of technology and knowledge of its development. A significant challenge for SMEs is the lack or limited standardisation and compatibility of systems due to the implementation of new digital technologies and also the high investment costs associated with the purchase of software and the implementation of digital technologies in all areas of ADMA. Finally, the implementation of new digital technologies can raise data privacy issues and increase cybersecurity risks.

The functioning of the national economy, i.e. the de facto state in economic terms, is not the simple sum of the activities of individual enterprises, but both positive and negative synergies can occur here. The state plays a pivotal role in the overarching dynamics at a higher level, namely the entire economy. Consequently, the issue of state security assumes a critical contextual significance for the competitive processes unfolding at the enterprise and industry levels. Key factors and challenges at this macroeconomic level include cybersecurity threats and cyberattacks, cyber incidents and defence, as well as attacks on the national critical infrastructure. In addition, it is the legal regulation of digital risk management, trainings fostering digital awareness, and the threats to the labour market posed by automation and digitisation of processes.

As regards the methodological side, the study is mainly based on secondary data collected from the literature on the subject and also refers to the authors' expert experience built up in the implementation of specific analytical and consultancy projects.

Wstęp

Niniejszy raport powstał w ramach prac grupy ds. Identyfikacji zagrożeń związanych z cyfryzacją Fundacji Platforma Przemysłu Przyszłości. Jego celem jest wskazanie zagrożeń związanych z wprowadzaniem technologii cyfrowych do przedsiębiorstw, szczególnie małych i średnich (MŚP) w kontekście bezpieczeństwa państwa. Należy podkreślić, że cyfryzacja wielu aspektów funkcjonowania MŚP jest z jednej strony wielką szansą mogącą doprowadzić do zwiększenia wydajności, produktywności i efektywności ich działań oraz poprzez to przyczynić się do zwiększenia ich konkurencyjności zarówno na rynku krajowym, jak i w perspektywie międzynarodowej. Cyfryzację postrzegamy więc jako instrument prowadzący do podwyższenia dobrobytu społecznego. Jest ona przede wszystkim olbrzymią szansą rozwojową, której niewykorzystanie byłoby karygodnym zaniedbaniem. Jednocześnie jednak, z drugiej strony, procesom digitalizacji towarzyszą liczne zagrożenia, których adekwatne rozpoznanie może stanowić podstawę do budowania strategii zapobiegania im, albo zmniejszenia poziomu ich dolegliwości i rozmiarów związanych z tym negatywnych konsekwencji. Na tym tle przyjmujemy autorskie rozu-mienie bezpieczeństwa państwa, które w szerokim tego słowa znaczeniu wiążemy przede wszystkim z zapewnieniem konkurencyjności sektora MŚP. Utratę lub zmniejszenie konkurencyjności tegoż sektora należy bowiem traktować jako fundamentalnie sprzeczne z interesem państwa.

Raport ukierunkowany jest na udzielenie odpowiedzi na następujące dwuczłonowe pytanie badawcze: 1/ jakie zagrożenia związane z wdrażaniem technologii cyfrowych przyczyniają się do powstania luki cyfrowej w zarejestrowanych w Polsce MŚP? oraz 2/ jakie mogą być konsekwencje tych zagrożeń w kontekście bezpieczeństwa państwa?

Prowadzone przez autorów rozważania dotyczą identyfikacji zagrożeń związanych z wprowadzaniem technologii cyfrowych, tworzących lukę cyfrową w MŚP w kontekście bezpieczeństwa państwa.

Wprowadzanie technologii cyfrowych to jedno z najważniejszych współczesnych wyzwań stojących przed przedsiębiorstwami. Absorpcja i implementacja technologii cyfrowych są jednym z najważniejszych warunków budowania, utrzymania oraz poprawy konkurencyjności. Z kolei konkurencyjność, jej właściwy poziom, jest filarem bezpieczeństwa państwa w wąskim, gospodarczym tego słowa znaczeniu, ale także w szerszym kontekście – bez konkurencyjnej gospodarki bezpieczne funkcjonowanie państwa jest utrudnione albo niemożliwe w obliczu niedoborów zasobów potrzebnych do spełniania przez państwo przynależnych mu funkcji.

Technologie cyfrowe rodzą dla przedsiębiorstw określone szanse i zagrożenia. Zgod-nie z elementarnymi rekomendacjami zarządzania strategicznego szanse należy wykorzystać, zagrożenia trzeba oddalić, zneutralizować albo trzeba im przeciwdziałać. Tak ujęta filozofia zarządzania strategicznego jest obiecującym podejściem do rozwiązywania problemów zasygnalizowanych w tytule tego opracowania. Trudno byłoby przecenić wagę podejmowanej problematyki, albowiem wiąże się ona z kardynalnymi uwarunkowaniami unkcjonowania państwa, wśród

których bezpieczeństwo należy do niepodlegających dyskusji aksjomatów. Czym innym jest jednak taki aksjomat sformułować i przyjąć, a czym innym zastosować go w działaniu. Niniejsze opracowanie koncentruje uwagę na aplikacyjnych aspektach zapewnienia bezpieczeństwa państwa biorąc pod uwagę perspektywę działania MŚP w zakresie technologii cyfrowych.

Identyfikacja zagrożeń związanych z wprowadzaniem nowych technologii cyfrowych w MŚP w kontekście bezpieczeństwa państwa została dokonana w oparciu o wykorzystanie następujących źródeł:

- przegląd literatury międzynarodowej i krajowej,
- analiza dostępnych wyników badań naukowych,
- analiza doniesień medialnych,
- zaprezentowanie studiów przypadków polskich MŚP,
- analiza regulacji prawnych,
- analiza własnych obserwacji i doświadczeń autorów wynikających ze współpracy i bezpośrednich kontaktów z przedsiębiorstwami – konsultacje, analizy, ekspertyzy, zasiadanie w radach nadzorczych, itp.

1 Identyfikacja kluczowych technologii cyfrowych istotnych dla MŚP

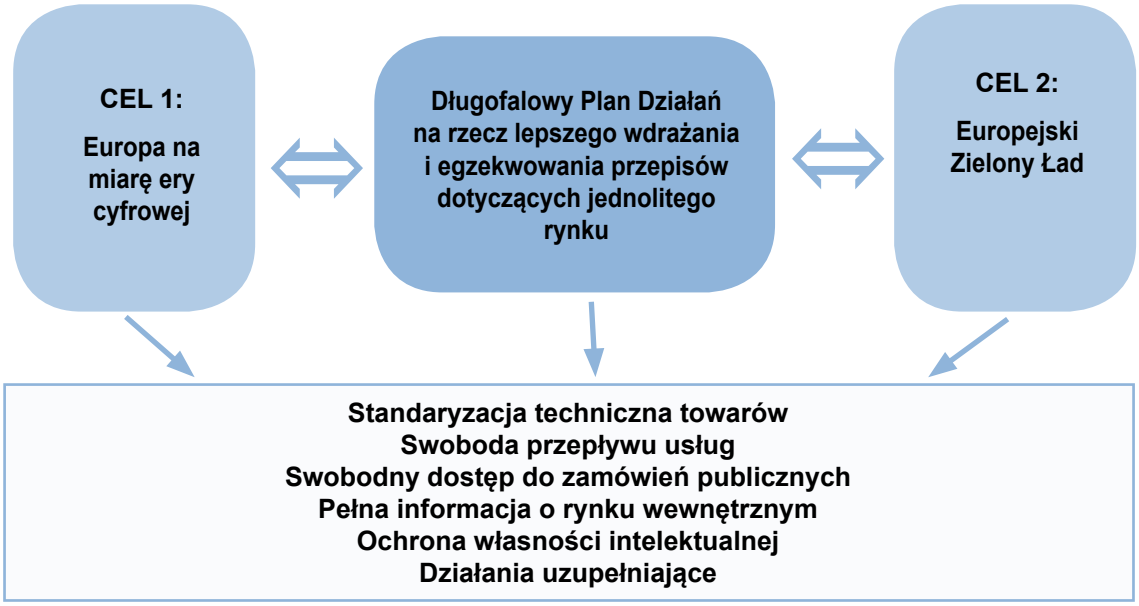
Wprowadzenie kluczowych technologii cyfrowych stało się nieodłącznym elementem strategii rozwoju i konkurencyjności MŚP na całym świecie. W obliczu drastycznego przyspieszenia rewolucji cyfrowej przy jednoczesnej głębokiej niestabilności i nieprzewidywalności otoczenia biznesowego spowodowanych pandemią i wojną w Ukrainie, MŚP zmuszone są do realizacji strategii transformacji cyfrowej, aby utrzymać pozycję konkurencyjną i sprostać rosnącym oczekiwaniom klientów. Wdrażanie nowoczesnych technologii cyfrowych, takich jak sztuczna inteligencja (AI), Internet Rzeczy (IoT), czy chmura obliczeniowa, staje się kluczowym elementem strategii biznesowych MŚP.

Wdrażane kluczowych technologii cyfrowych stało się jednym z głównych priorytetów Unii Europejskiej, stąd kluczowe dokumenty w nowej strategii przemysłowej dla Europy [1] oraz strategii MŚP na rzecz zrównoważonej i cyfrowej Europy [2] wskazują technologie istotne w procesie transformacji cyfrowej (Rysunek 1).

Komisja Europejska uczyniła ostatnie lata cyfrową dekadą Europy, co w odniesieniu do rynku wewnętrznego przekłada się na działania związane ze strategią przemysłową oraz eliminacją utrudnień na jednolitym rynku i możliwością wykorzystywania technologii, produktów i usług cyfrowych w skali stymulującej ich wydajność i globalną konkurencyjność [3]. W ramach zaprojektowanych działań, Komisja realizuje trzy kluczowe cele:

- Technologia przynosząca korzyści ludziom - technologie pozytywnie wpływające na życie obywateli.
- Uczciwa i konkurencyjna gospodarka – MŚP wprowadzają technologie cyfrowe w skali stymulującej ich wydajność i globalną konkurencyjność.
- Otwarte, demokratyczne i zrównoważone społeczeństwo - europejski sposób transformacji cyfrowej, który ugruntowuje demokratyczne wartości, zakłada poszanowanie naszych praw podstawowych i przyczynia się do zrównoważonej, zasobooszczędnej i neutralnej dla klimatu gospodarki.

Jednocześnie podkreślone zostało znaczenie bezpieczeństwa w cyberprzestrzeni. Coraz większe wzajemne powiązania w świecie wirtualnym zwiększyły istotnie powiązania pomiędzy uczestnikami sieci.



Rysunek 1. Plan strategiczny Komisji Europejskiej na lata 2019-2024 dotyczący rynku wewnętrznego

Źródło: Kuczewska J., Stefaniak J. (2021) [4].

Przewodnicząca Komisji Europejskiej Ursula von der Leyen ogłosiła, iż w 2030 roku Europa powinna osiągnąć suwerenność cyfrową. Wskazała europejską chmurę obliczeniową jako kluczową w dziedzinie etycznej sztucznej inteligencji, bezpieczną tożsamość dla wszystkich użytkowników sieci oraz infrastrukturę superkomputerów i łączności [5].

Unia Europejska wskazuje ponadto wiodącą rolę MŚP jako istotnego źródła innowacji oraz zakłada, iż przy wsparciu ponad 200 ośrodków innowacji cyfrowych oraz klastrów przemysłowych do 2030 roku europejskie MŚP powinny mieć dostęp do technologii cyfrowych i danych na sprawiedliwych warunkach. Zakładanym poziomem osiągnięcia wyznaczonych celów jest by do 2030 roku [5]:

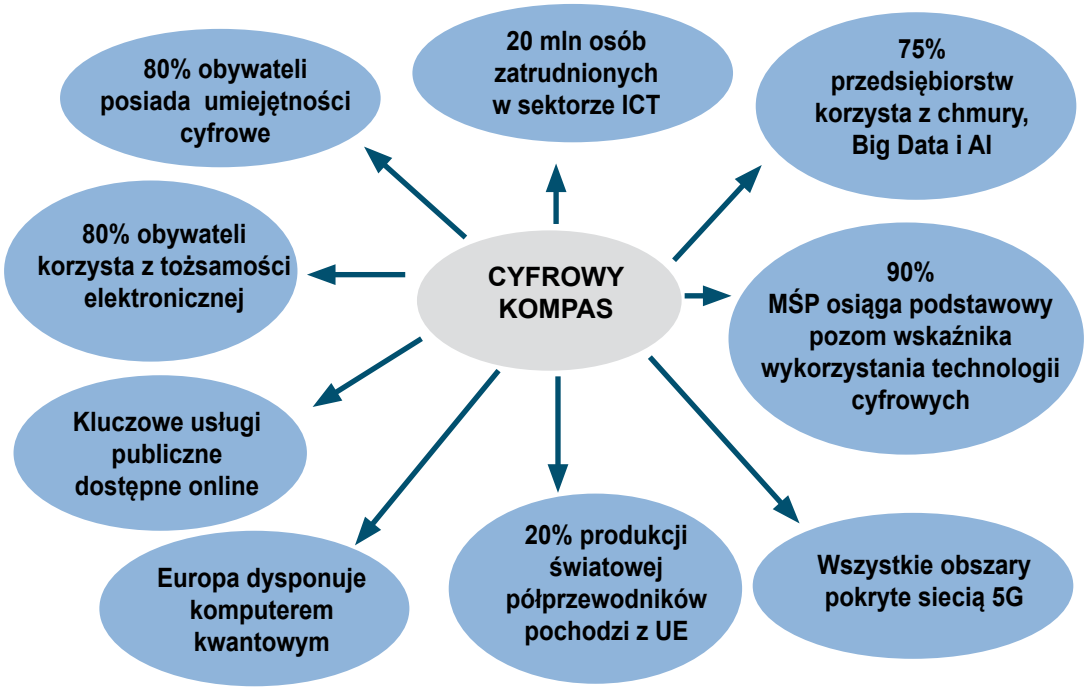
- 75 % europejskich przedsiębiorstw korzystało z usług w chmurze, dużych zbiorów danych i sztucznej inteligencji,
- ponad 90 % europejskich MŚP osiągnęło co najmniej podstawowy poziom wskaźnika wykorzystania technologii cyfrowych,
- Europa powiększała swoją sieć innowacyjnych przedsiębiorstw scale-up i poprawiła ich dostęp do finansowania, co doprowadzi do podwojenia liczby jednorożców[1] w Europie.

W ramach realizacji strategii cyfrowej Unia Europejska wskazała listę uzgodnionych z krajami członkowskimi projektów cyfrowych wskazując jednocześnie kluczowe technologie cyfrowe istotne dla MŚP [5]:

1 Jednorożce oznaczają: 1) zrealizowanego jednorożca, tj. przedsiębiorstwo założone po 1990 r., którego pierwsza oferta publiczna lub sprzedaż na rzecz inwestora branżowego przyniosła powyżej 1 mld USD oraz 2) niezrealizowanego jednorożca, tj. przedsiębiorstwo, które w ostatniej rundzie prywatnego finansowania kapitału wysokiego ryzyka wyceniono na co najmniej 1 mld USD (tzn. wyceny nie potwierdzono w transakcji wtórnej)

- budowa wspólnej i wielofunkcyjnej ogólnoeuropejskiej wzajemnie połączonej **infrastruktury przetwarzania danych** oraz rozwijanie zdolności przetwarzania danych na obrzeżach sieci w czasie,
- projektowanie **układów elektronicznych** oraz wprowadzenie nowej generacji spraw-dzonych procesorów i innych elementów elektronicznych o niskim poborze mocy,
- wdrożenie w całej Europie **korytarzy 5G**,
- uzyskanie **superkomputerów i komputerów kwantowych** podłączonych do sieci komunikacyjnej powstałej w ramach Wspólnego Przedsięwzięcia w dziedzinie Europejskich Obliczeń Wielkiej Skali o niezwykle dużej przepustowości,
- opracowanie i wdrożenie ultrabezpiecznej **kwantowej infrastruktury komunikacyjnej**,
- wprowadzenie sieci **centrów monitorowania bezpieczeństwa** obsługiwanej przez sztuczną inteligencję, w celu wczesnego wykrywania,
- podłączona do sieci administracja publiczna,
- europejska infrastruktura usług **w technologii blockchain**,
- **europejskie ośrodki innowacji cyfrowych** (EDIH), które są „punktami komplek-sowej obsługi" służącymi m.in. do dostarczania MŚP fachowej wiedzy technicznej, zapewniania możliwości „testowania przed inwestowaniem", udzielania porad fi-nansowych i przeprowadzania szkoleń,
- partnerstwa w zakresie zaawansowanych technologii na rzecz umiejętności cy-frowych w ramach paktu na rzecz umiejętności.

Potwierdzeniem intensywności działań UE na rzecz rozwoju strategii cyfryzacji jest również nowe narzędzie zwane cyfrowym kompasem [5] (Rysunek 2).



Rysunek 2. Cyfrowy kompas UE – cele strategiczne

Źródło: opracowanie własne na podstawie [1].

Obejmuje cztery obszary: realizację celów strategicznych, strukturę zarządzania (wraz z zasadami sprawozdawczości), monitorowanie zasad cyfrowych oraz mechanizm planowania i realizacji projektów wielonarodowych. Do celów strategicznych cyfrowego kompasu do 2030 roku zaliczono [5]:

- Umiejętności: co najmniej 80% wszystkich osób dorosłych powinno posiadać podstawowe umiejętności cyfrowe, a w UE powinno być zatrudnionych 20 milionów specjalistów w dziedzinie ICT.
- Przedsiębiorstwa: 75% przedsiębiorstw powinno korzystać z usług w chmurze, dużych zbiorów danych i sztucznej inteligencji; ponad 90% małych i średnich przed-siębiorstw w UE powinno osiągnąć przynajmniej podstawowy poziom wskaźnika wykorzystania technologii cyfrowych, a liczba jednorożców w UE powinna się podwoić.
- Infrastruktura: wszystkie gospodarstwa domowe w UE powinny mieć łączność giga-bitową, a wszystkie zaludnione obszary znajdować się w zasięgu sieci 5G; produkcja najnowocześniejszych i zrównoważonych półprzewodników w Europie powinna stanowić 20% produkcji światowej; w UE powinno zostać uruchomionych 10 000 neutralnych dla klimatu węzłów brzegowych oferujących wysoki stopień bezpieczeń-stwa; Europa powinna dysponować swoim pierwszym komputerem kwantowym.
- Usługi publiczne: wszystkie kluczowe usługi publiczne powinny być dostępne online; wszyscy obywatele będą mieli dostęp do swoich elektronicznych dokumentacji medycznych, a 80% obywateli powinno korzystać z rozwiązań w zakresie tożsamości elektronicznej.

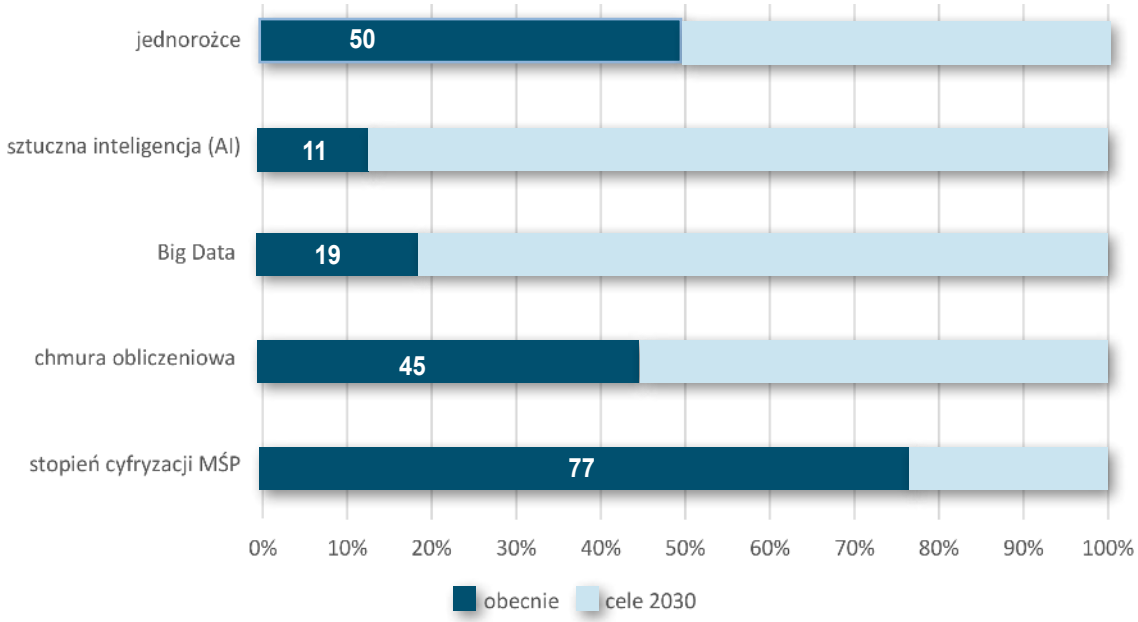
Program realizacji polityki Cyfrowa Dekada 2030 zakłada współpracę komisji Europejskiej i państw członkowskich oparty na rocznym mechanizmie współpracy, który obejmuje [5]:

- ustrukturyzowany, przejrzysty i wspólny system monitorowania oparty na wskaźniku gospodarki cyfrowej i społeczeństwa cyfrowego (*Digital Economy and Society Index* – DESI),
- roczne sprawozdanie Komisji Europejskiej, w którym oceniane są postępy realizacji strategii cyfrowej,
- co dwa lata dostosowane strategiczne plany działania na rzecz dekady cyfrowej,
- mechanizm wspierający realizację projektów obejmujących wiele krajów – konsorcjum na rzecz europejskiej infrastruktury cyfrowej (*European Digital Infra-structure Consortium*).

Pierwsze roczne sprawozdanie Komisji Europejskiej oceniające postępy realizacji strategii cyfrowej opublikowane zostało we wrześniu 2023 roku [2]. Implementacja celów strategicznych cyfrowego kompasu dedykowanych transformacji cyfrowej przedsiębiorstw pokazuje następujące tendencje [6]:

- Przyjęcie technologii cyfrowych przez europejskie przedsiębiorstwa jest nadal znacznie poniżej celów cyfrowej dekady, w szczególności tych dotyczących wykorzystania sztucznej inteligencji i dużych zbiorów danych. Cele wyznaczone do 2030 roku nie

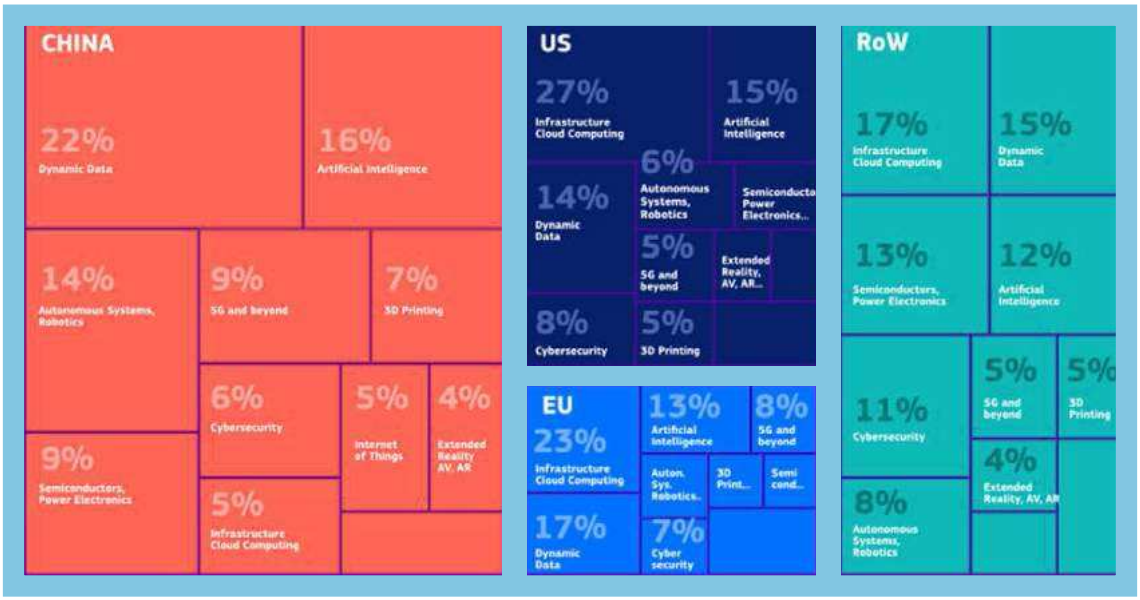
zostaną osiągnięte: przewidywana trajektoria bazowa wskazuje, że tylko 66% przedsiębiorstw będzie korzystać z chmury (na 75% przedsiębiorstw prognozowanych), 34% z dużych zbiorów danych (na 75% przedsiębiorstw prognozowanych) i 20% ze sztucznej inteligencji (również na 75% prognozowanych) (Rysunek 3).



Rysunek 3. Transformacja cyfrowa przedsiębiorstw w UE

Źródło: opracowanie własne na podstawie [6].

- Postęp w kierunku cyfryzacji MŚP jest niewystarczający i dość nierównomierny w całej UE. Jest on również niższy niż w USA, gdzie jest dwa razy więcej MŚP z międzynarodowym portfelem tzw. patentów 4IR (Internet rzeczy – IoT, chmura, 5G, sztuczna inteligencja) niż w UE (Rysunek 4).



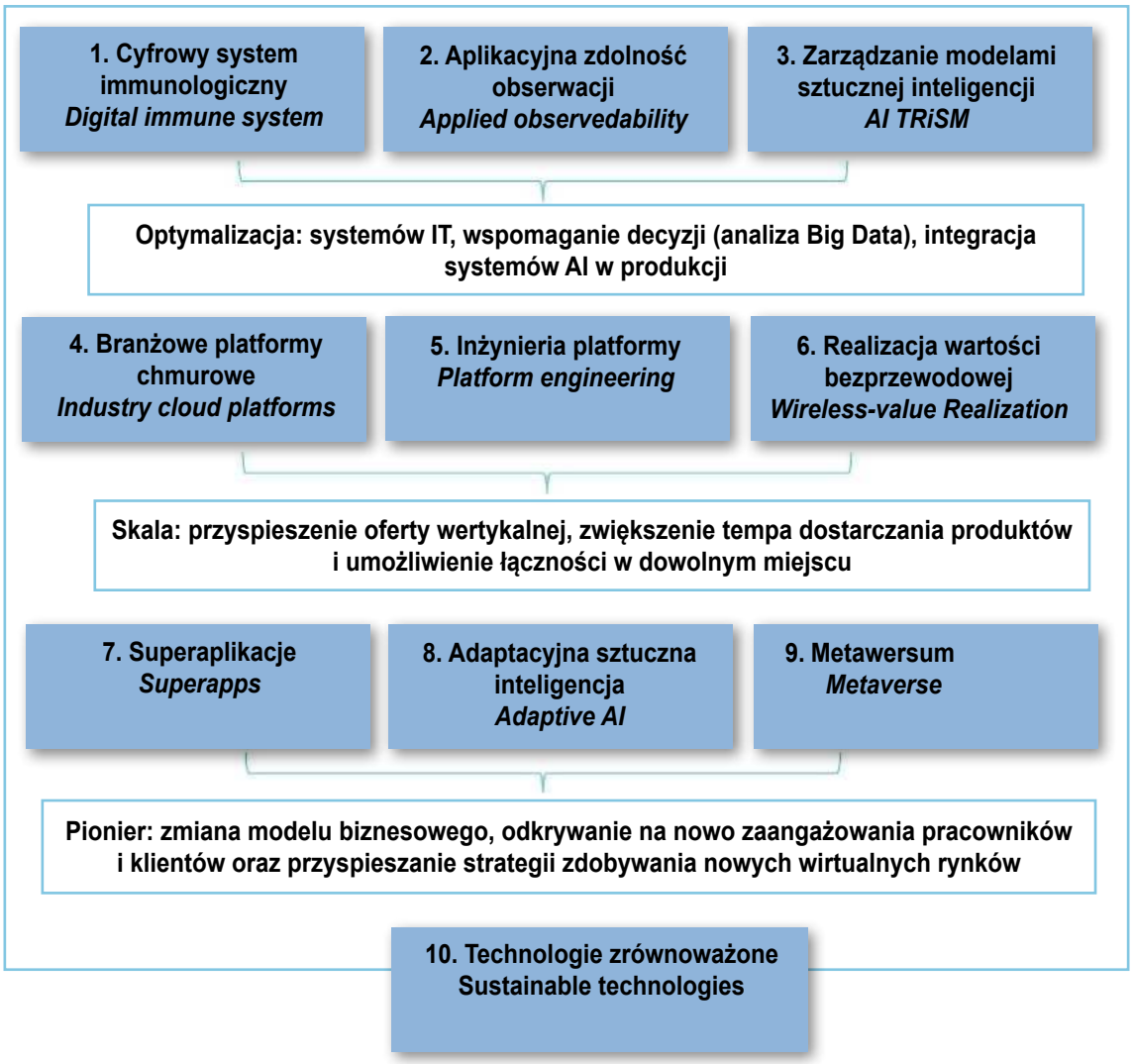
Rysunek 4. Kluczowe czynniki (technologie) cyfrowej transformacji Europy w 2022 roku

Źródło: Komisja Europejska 2023, s. 7 [2].

W celu zapewnienia przyszłej, trwałej konkurencyjności przemysłu UE Ursula von der Leyen w 2022 roku zapowiedziała uruchomienie Platformy Technologii Strategicznych dla Europy (*Strategic Technologies for Europe Platform* – STEP). Platforma pomaga zachować europejską przewagę w zakresie krytycznych i powstających technologii istotnych dla transformacji ekologicznej i cyfrowej, od technologii związanych z obliczeniami, w tym mikroelektroniki, obliczeń kwantowych i sztucznej inteligencji; do biotechnologii i biomanufacturingu oraz technologii net-zero. Jednym z celów STEP jest zapewnienie szerokiego dostępu do finansowania wszelkich działań w tym obszarze, również z uwzględnieniem dofinansowania sektora MŚP [7].

Podsumowując działania UE w zakresie wdrażania technologii cyfrowych istotnych dla MŚP wyróżnić można trzy zaawansowane technologie kluczowe dla przyszłości Europy tj.: Internet rzeczy (IoT), łańcuch bloków (Blockchain) oraz Internet nowej generacji.

Trendy w rozwoju kluczowych strategicznych technologii w tym technologii cyfrowych prezentuje firma doradcza Gartner [8] (Rysunek 5).



Rysunek 5. Kluczowe trendy technologiczne

Źródło: opracowanie własne na podstawie [8].

Dziesięć kluczowych trendów technologii podzielonych zostało na trzy grupy spełniające określone funkcje: optymalizacji, tworzeniu skali oraz posiadających funkcje pionierskie [8]. Do głównych trendów technologicznych Gartner zalicza:

- Cyfrowy system immunologiczny (*DIS*): praktyki i technologie projektowania oprogramowania, rozwoju, operacji i analizy w celu ograniczenia ryzyka biznesowego.
- Aplikacyjna zdolność obserwacji (*Applied Observability*): wykorzystanie sztucznej inteligencji do analizy i formułowania zaleceń, które pozwalają przedsiębiorstwu podejmować szybsze i dokładniejsze decyzje.
- Zarządzanie modelami sztucznej inteligencji (AI TRiSM): metody wyjaśniania wyników sztucznej inteligencji, szybkie wdrażanie nowych modeli, aktywne zarządzanie bezpieczeństwem sztucznej inteligencji oraz kontrola kwestii prywatności i etyki.
- Branżowe platformy chmurowe (Industry cloud platforms): łączą oprogramowanie, platformę i infrastrukturę jako usługę. W większości oparte na usługach chmury publicznej.
- Inżynieria platform (Platform engineering): modernizacja dostarczania oprogramowania dla przedsiębiorstw, w szczególności na potrzeby transformacji cyfrowej.
- Realizacja wartości bezprzewodowej (Wireless-Value Realization): dostarczanie bezprzewodowych usług sieciowych zapewniając lokalizację i inne informacje w czasie rzeczywistym oraz wgląd w dane analityczne.
- Superaplikacje (Superapps): połączenie funkcji aplikacji, platformy i ekosystemu w jednej aplikacji, tworząc platformę do opracowywania i publikowania własnych miniaplikacji.
- Adaptacyjna sztuczna inteligencja (Adaptive AI): pozwala na zmianę zachowania modelu po wdrożeniu, wykorzystując informacje zwrotne.
- Technologie zrównoważone (Sustainable technologies): rozwiązania, które zwiększają efektywność energetyczną i wydajność usług IT.

Bieżący monitoring trendów technologicznych prowadzą również korporacje: McKinsey oraz Delloite. W ostatnim raporcie z 2023 roku McKinsey prezentuje piętnaście wiodących trendów [9], tj.: stosowana sztuczna inteligencja (Applied AI); uprzemysłowienie uczenia maszynowego (Industrializing Machine Learning); generatywna sztuczna inteligencja (Generative AI); tworzenie oprogramowania nowej generacji (Next-generation Software Development); architektury zaufania i tożsamość cyfrowa (Trust Architectures and Digital Identity); Web3 (zdecentralizowany Internet z otwartymi standardami i protokołami, przy jednoczesnej ochronie praw własności cyfrowej); zaawansowana łączność (Advanced Connectivity - bezprzewodowe sieci o niskim poborze mocy, sieci komórkowe 5G/6G, Wi-Fi 6 i 7, satelity na niskiej orbicie okołoziemskiej i inne technologie); technologie rzeczywistości immersyjnej (Immersive-reality Technologies, technologia wirtualna); chmura i przetwarzanie brzegowe (Cloud and Edge Computing); technologie kwantowe (Quantum Technologies); technologie mobilności (Mobility Technologies); bioinżynieria (Bioengine-

ering); przyszłość technologii kosmicznych (Future of Space Technologies); elektryfikacja i odnawialne źródła energii (Electrification and Renewables) oraz technologie klimatyczne poza elektryfikacją i odnawialnymi źródłami energii (Climate Technologies).

Delloite natomiast w 2023 roku wskazuje sześć trendów technologicznych, dzieląc je na dwie kategorie: „oczy skierowane w niebo" oraz „stopy mocno na ziemi". Do pierwszej kategorii Delloite zalicza trzy trendy: przez szybę, czyli wciągający internet dla przedsiębiorstw; otwarcie na sztuczną inteligencję: uczenie się od naszych kolegów zajmujących się sztuczną inteligencją oraz ponad chmurami: oswajanie chaosu wielochmurowego. Do drugiej zaś kategorii: elastyczność, najlepsza umiejętność: pozostać pracownikiem technologicznym; ufamy sobie: zdecentralizowane architektury i ekosystemy (ekosystemy oparte na blockchain) oraz łącz i rozszerzaj: modernizacja mainframe nabiera tempa [10].

Identyfikacja nowoczesnych technologii – w tym technologii cyfrowych – istotnych dla MŚP odbywa się również na łamach artykułów naukowych. Potwierdzają to dane uzyskane przez grupę badaczy (Maciej Wilamowski, Kristóf Gyódi, Michał Paliński, Łukasz Nawaro), którzy metodami analityki Big Data i webscrapingu przebadali 140 tysięcy artykułów w pismach branżowych i 800 tysięcy w pismach naukowych. Na tej podstawie wyodrębnili technologie zyskujące na znaczeniu. Z przeprowadzonego badania wynika, iż w 2018 roku najczęściej pojawiały się pojęcia wiążące się z dwiema grupami innowacji: systemami rozproszonymi (w tym kryptowalutami oraz blockchainem) oraz sztuczną inteligencją (w tym również robotami oraz wirtualną rzeczywistością). Kolejne pozycje pod względem częstotliwości pojawiania się zajmowały sieci 5G, pojazdy autonomiczne, kwantowe przetwarzanie informacji, Internet rzeczy oraz rozwiązania chmurowe [11].

W 2022 roku Quach i inni [12] podzielili wiodące technologie cyfrowe związane z analizą Big Data na cztery grupy: rejestracja danych; agregacja, przetwarzanie i przechowywanie danych; modelowanie danych i programowanie oraz wizualizacja danych i projektowanie interakcji. Ponadto w grupie inteligentna autonomia usług wyróżnili: roboty usługowe, Metaverse, sztuczną inteligencję, technologie ubieralne, inteligentne technologie samoobsługowe oraz generatywną sztuczną inteligencję.

Z kolei Wynn i Jones [13] definiując technologie cyfrowe jako „ ….narzędzia elektroniczne, systemy automatyczne i urządzenia technologiczne, które generują, przetwarzają i przechowują informacje, i są powszechnie postrzegane jako zakłócające i przekształcające praktyki i modele biznesowe" wskazali na dwa współczesne akronimy pozwalające na skategoryzowanie tych technologii tj.: akronimy SMAC – Social media, Mobile, Analytics/Big data, Cloud (media społecznościowe, telefonia komórkowa, analiza dużych zbiorów danych/Big data, chmura) i BRAID – Blockchain, Robotics, Automation of knowledge work/artificial intelligence, Internet of Things and Digital fabrication (łańcuch bloków, robotyka, automatyzacja pracy opartej na wiedzy/sztuczna inteligencja, Internet rzeczy i cyfrowa produkcja).

Zdaniem Chauhan wraz z zespołem [14] metody i technologie cyfrowe można ująć w kilku głównych kategoriach: symulacja Big Data i analityka, Internet rzeczy, systemy cyberfizyczne (CPS), cyberbezpieczeństwo w chmurze obliczeniowej, rzeczywistość rozszerzona, komunikacja maszyna-maszyna oraz roboty współpracujące.

Paschek i inni [15] zapowiedzieli kolejny etap rewolucji przemysłowej wynikający z wysokiego zapotrzebowania konsumentów na indywidualizację nabywanych produktów – Przemysł 5.0. Zwiększona współpraca między ludźmi a inteligentnymi systemami jest jego główną cechą. Na tym etapie maszyny przejmą wszystkie powtarzalne zadania, podczas gdy ludzie przejmą stronę kreatywną.

Ponadto Ministerstwo Cyfryzacji przeprowadziło w 2023 roku wśród MSP badania na temat gotowości wdrożenia, poziomu wiedzy i wykorzystania nowych technologii cyfrowych. Zakres badań obejmował następujące obszary: elektroniczna wymiana informacji, media społecznościowe, duże zbiory danych, chmura, sztuczna inteligencja, ICT na rzecz zrównoważenia środowiskowego, e-faktury, MŚP prowadzące sprzedaż internetową, obroty z tytułu handlu elektronicznego, transgraniczna sprzedaż internetowa. Za kluczowe technologie uznane zostały: sztuczna inteligencja, Internet Rzeczy oraz e-usługi [16].

Ministerstwo Cyfryzacji za kluczowe przełomowe technologie cyfrowe uznało [17]:

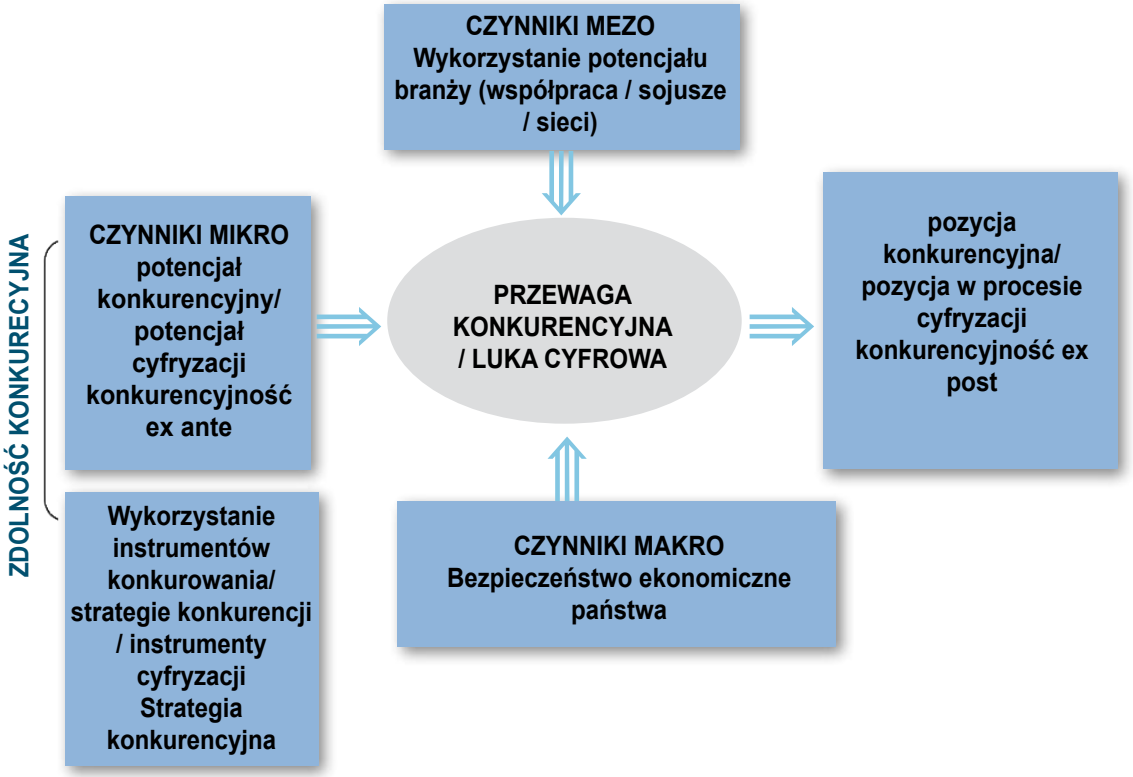
- Internet rzeczy (IoT);
- Sztuczną Inteligencję *(AI)*;
- Blockchain / rejestry rozproszone;
- Bezpieczną komunikację kwantową;
- Obliczenia dużych wydajności (HPC).

Podsumowując, różnorodność podejść w kategoryzowaniu technologii cyfrowych istotnych dla MŚP pozwala na wyodrębnienie następujących kluczowych technologii cyfrowych:

1. Internet Rzeczy (Internet of Things) – monitorowanie i zbierania danych z urządzeń.
2. *Łańcuch bloków (Blockchain)* – rejestr zdecentralizowanych danych, bezpiecznie współużytkowanych.
3. Internet nowej generacji (5G).
4. Chmura obliczeniowa (Cloud computing).
5. Sztuczna inteligencja (Artificial Intelligence) i uczenie maszynowe (Machine Learning).
6. Analiza danych i analiza du*żych zbiorów danych (Big Data).*
7. Cyberbezpieczeństwo.
8. Superkomputery i komputery kwantowe.
9. Cyfrowe modelowanie i produkcja (Digital modeling and fabrication).
10. Systemy autonomiczne i robotyzacja.

2 Koncepcja luki cyfrowej[2]

W zaprezentowanym poniżej rozumowaniu pojęciem kluczowym, które chcemy zdefiniować i zoperacjonalizować jest pojęcie luki cyfrowej. Można do tego wykorzystać koncepcję luki konkurencyjnej i *per analogiam* przemianować ją na lukę cyfrową. Daje się wtedy wyróżnić trzy wymiary luki cyfrowej – potencjał cyfryzacji (jako ekwiwalent potencjału konkurencyjnego), pozycja w procesie cyfryzacji (jak odpowiednik pozycji konkurencyjnej) oraz instrumenty cyfryzacji (jako odpowiednik instrumentów konkurowania), składające się na strategię cyfryzacji, czyli wykorzystania technologii cyfrowych w MŚP (Rysunek 6).



Rysunek 6. Koncepcja konkurencyjności przedsiębiorstwa versus koncepcja luki cyfrowej
Źródło: opracowanie własne.

Niżej rozwinięto rozumowanie prowadzące do stworzenia zapowiedzianej siatki pojęciowej zorientowanej wokół pojęcia luki cyfrowej, która – w naszym przekonaniu – może być przydatna w analizie problematyki technologii cyfrowych odniesionych do MŚP.

2 Przy redakcji rozdziału wykorzystano fragmenty prac [18, 52, 53, 54, 55]: Gorynia, M. (2009), Teoretyczne aspekty konkurencyjności, w pracy [54]; Gorynia, M. (2009), Konkurencyjność w ujęciu mikroekonomicznym, w pracy [54].

Alternatywny, bardziej ogólny sposób rozumowania zawarty jest natomiast w koncepcji różnicy cyfrowej, która *a priori* nie zawiera w sobie hipotezy, że rozwiązania w zakresie technologii cyfrowych w polskich MŚP nie są konkurencyjne w stosunku do ich rywali zagranicznych. Koncepcja różnicy cyfrowej zawiera w sobie dwie możliwości: lukę cyfrową (jako zestaw deficytów w rywalizacji na rynku w porównaniu z konkurentami) albo przewagę cyfrową (jako zestaw nadwyżek, przewag w zestawieniu z rywalami). Stwierdzenia te zostaną rozwinięte w dalszej części opracowania.

Rozwijana niżej koncepcja luki cyfrowej jest konsekwencją wykorzystania koncepcji zarządzania strategicznego i ich odniesienia do sfery cyfryzacji przedsiębiorstwa. Punktem wyjścia w naszym rozumowaniu jest więc ogólna koncepcja strategii konkurencyjnej przedsiębiorstwa, która integruje wszystkie aspekty jego działania i stanowi niezwykle ważny kontekst działań w zakresie cyfryzacji. Uzasadnieniem dla przyjęcia takiego szerszego kontekstu luki/różnicy cyfrowej jest dążenie do uniknięcia często spotykanego w zarządzaniu strategicznym błędu polegającego na rozpatrywaniu w odosobnieniu poszczególnych części aktywności przedsiębiorstwa. Przyjęcie założenia o autonomizacji i niezależności procesów cyfryzacji od pozostałych sfer aktywności firmy byłoby ciężkim wykroczeniem przeciwko zaleceniom podejścia systemowego do funkcjonowania przedsiębiorstwa. Podejście redukcjonistyczne (koncentrowanie uwagi tylko na jednym aspekcie bez uwzględnienia sprzężeń zwrotnych pomiędzy różnymi częściami/aspektami działania przedsiębiorstwa) grozi zawsze wystąpieniem suboptymalizacji częściowej, miejscowej, jednakże ze stratą dla efektywności i skuteczności działania firmy jako całości. Innymi słowy nie powinniśmy zapominać o tym, że cyfryzacja nie jest jedynym i najważniejszym celem przedsiębiorstwa; jest natomiast ważnym instrumentem służącym realizacji celu głównego, którym jest zachowanie istnienia i dobre prosperowanie firmy, a te z kolei możliwe są tylko i wyłącznie wtedy, gdy jest ona konkurencyjna.

Konkurencyjność można rozumieć na co najmniej dwa sposoby: 1/ cecha, atrybut, wynik, rezultat albo 2/ proces. Drugie znaczenie należy wiązać z dochodzeniem do cechy, atrybutu, wyniku, rezultatu, jakim jest konkurencyjność. Jest to, więc proces, przez który trzeba przejść, aby stać się konkurencyjnym. Jest to, innymi słowy, konkurowanie. Można z uproszczeniem przyjąć, że bliskim synonimem tak rozumianej konkurencyjności jest opisywana w literaturze konkurencja w sensie czynnościowym.

Konkurencyjność w pierwszym znaczeniu najczęściej rozpatrywana jest w odniesieniu do zagadnień gospodarczych. Konkurencyjność jest pojęciem odnoszącym się do gospodarki rynkowej. Istota tej gospodarki polega na tym, że uczestnicy życia gospodarczego rywalizują z sobą na rozmaitych płaszczyznach.

Pojęcie konkurencyjności należy do tzw. pojęć teoretycznych. Teoretyczny charakter tego pojęcia oznacza, że nie jest ona znakiem żadnej konkretnej rzeczy ani osoby, ani czegokolwiek, co sobie jako rzecz albo osobę wyobrażamy, czyli nie posiada desygnatów dających się określić wprost. W celu wyjaśnienia, co pojęcie to oznacza, konieczna jest jego dekompozycja, przez którą rozumie się tutaj wyróżnienie wymiarów konkurencyjności. Wątek ten zostanie podjęty w dalszej części tego rozdziału.

W uproszczeniu można przyjąć, że konkurencyjność oznacza umiejętność konkurowania, a więc działania i przetrwania w konkurencyjnym otoczeniu. *De facto* konkurencyjność w sensie procesowym (czynnościowym) wiąże się nierozerwalnie z konkurencyjnością w sensie atrybutowym (rezultatowym). Konkurencyjność procesowa prowadzi do osiągnięcia konkurencyjności w sensie atrybutowym. Tak rozumianą konkurencyjność można odnosić do różnych poziomów bytu gospodarczego. Zagadnienie to zostanie podjęte niżej. Wątpliwe byłoby twierdzenie, że konkurencyjność jest cechą absolutną, a więc taką, którą można orzec o danym podsystemie gospodarczym, używając do tego terminów, których znaczenie nie zakłada jakiegoś odniesienia do cech innych podsystemów, jakiegoś typu relacji łączących dany podsystem z innymi podsystemami. Nawet jeśli można sobie wyobrazić skalę do mierzenia konkurencyjności, to zawsze występuje w niej element odniesienia cech obiektu, którego konkurencyjność badamy, do cech innych obiektów, z którymi dany obiekt rywalizuje. Wydaje się więc, że konkurencyjność jest przede wszystkim cechą relatywną, a więc taką, której znaczenie zakłada jakiś typ relacji łączącej obiekt, o którym coś orzekamy, z jakimiś innymi obiektami. Ujmując rzecz jeszcze dokładniej, należałoby zaliczyć konkurencyjność do tej kategorii cech relatywnych, która określana jest jako własności porównawcze. Własności porównawcze obiektów polegają na przypisywaniu im pewnych własności w wyniku porównania ich z innymi obiektami lub jakimś standardem porównania (na przykład średnią dla całej zbiorowości).

Konkurencyjność można odnosić do różnych poziomów bytu (systemu) gospodarczego. W ekonomii wyróżnia się zasadniczo sześć głównych poziomów hierarchii systemów gospodarczych: mikro-mikro, mikro, mezo, makro, regionalny (w odniesieniu do grupy krajów), globalny.

Poziom mikro-mikro jest najniższy odnosi się do indywidualnych konsumentów, do indywidualnych przedsiębiorców oraz do pojedynczych pracowników. Jest to podstawowy poziom analizy w naukach ekonomicznych. Jednostką analizy są tutaj ekonomiczne aspekty zachowań człowieka. Poziom mikro obejmuje przedsiębiorstwa (nie jednoosobowe) oraz gospodarstwa domowe, składające się z liczby konsumentów przewyższających jeden. Formalnie rzecz ujmując do tego poziomu zalicza się przedsiębiorstwa o bardzo zróżnicowanych rozmiarach, co niewątpliwie utrudnia dokonywanie uogólnień. Poziom mezo to poziom średniego szczebla. Najczęściej odnosi się go do branż, sektorów, gałęzi i innych podobnych składników gospodarki narodowej. Są to więc wyodrębnione podmiotowo i/lub przedmiotowo fragmenty gospodarki jakiegoś kraju. Poziom mezo bywa także odnoszony do wyodrębnionych terytorialnie fragmentów gospodarki jakiegoś kraju (np. województwa, prowincje, stany, itp.). Poziom makro dotyczy gospodarek narodowych (krajowych) poszczególnych państw. Trzeba podkreślić, że poziom ten obejmuje obiekty (podsystemy) o bardzo zróżnicowanej wielkości. Poziom regionalny w przyjętym tutaj znaczeniu odnosi się do grup krajów (gospodarek narodowych). Może na przykład obejmować ugrupowania integracyjne różnych państw. Wreszcie poziom globalny to gospodarka całego globu.

Należy dodać, że coraz częściej w badaniach konkurencyjności podnoszony jest aspekt terytorialny (przestrzenny). Mówi się o konkurencyjności gmin, powiatów, województw, regionów, makroregionów itp. – są to wyodrębnione w sensie przestrzennym fragmenty gospodarki narodowej. Można więc mówić, że jest to pewna odmiana mezosystemów gospodarczych, w przypadku których nakreślając ich granice wykorzystuje się kryterium o charakterze geograficznym.

Cecha konkurencyjności może przysługiwać większości, ale nie wszystkim poziomom bytu gospodarczego. Jeśli konkurencyjność jest cechą relatywną, to może ona odnosić się do poziomów: mikro-mikro, mikro, mezo, regionalnego i makro, ale nie do poziomu globalnego. Można mówić o konkurencyjności pojedynczego pracownika (np. umiejętności menedżerskie kierownika, wydajność pracy pracownika fizycznego, itp.), konkurencyjności przedsiębiorstwa (np. zmiany udziału w rynku), konkurencyjności branży (np. zmiany udziału w produkcie krajowym brutto) oraz konkurencyjności gospodarki narodowej (np. zdolności trwałego wzrostu gospodarczego). Natomiast w wypadku poziomu globalnego (gospodarki światowej) mówienie o jego konkurencyjności będzie niemożliwe, gdyż nie ma punktu odniesienia, zależności, oddziaływań i kontekstu, z którymi można by zestawić cechy gospodarki światowej.

Istotne może być także spostrzeżenie, że dokonując badań i analiz konkurencyjności trzeba pamiętać o tym, aby porównywać wielkości porównywalne, czyli obiekty należące do tej samej kategorii. Trudno bowiem porównywać konkurencyjność pracownika z konkurencyjnością branży *x* lub regionu *y*.

Ponadto wstępnie zauważmy w tym miejscu, że badania nad konkurencyjnością odnoszoną do różnych poziomów prowadzone były w zasadzie w sposób autonomiczny, często oderwany od siebie, co przejawiało się między innymi w tym, że nie wykształcono jednolitej terminologii służącej do opisu konkurencyjności na różnych poziomach.

Dla dalszych rozważań użyteczne może być rozróżnienie konkurencyjności *ex ante* i konkurencyjność *ex post.* Biorąc pod uwagę upływ czasu, konkurencyjność można rozpatrywać w sposób dynamiczny oraz statyczny. Mówiąc o jakimś obiekcie, że posiada atrybut konkurencyjności, mamy zazwyczaj na myśli jakiś moment, w którym rozpatrujemy i porównujemy konkurencyjność. Konkurencyjność rozumiana w sensie statycznym jest czymś w rodzaju fotografii zestawu cech jakiegoś obiektu, które opisują jego konkurencyjność.

Konkurencyjność w sensie dynamicznym jest natomiast zestawem, ciągiem, sekwencją stanów, które ujmują aspekt statyczny. Dynamiczne podejście do konkurencyjności zakłada więc ujęcie jego rozwoju wraz z upływem czasu. W świetle uwag poczynionych wcześniej nasuwa się tutaj spostrzeżenie, że konkurencyjność w ujęciu statycznym jest odpowiednikiem cechy, atrybutu, rezultatu, wyniku, a więc konkurencyjności w sensie atrybutowym (rezultatowym).

Z kolei konkurencyjność rozpatrywana z dynamicznego punktu widzenia koresponduje z konkurencyjnością rozumianą procesowo, czyli z dochodzeniem do określonego stanu konkurencyjności.

Proponuje się, aby niezależnie od poziomu, na którym prowadzone są badania konkurencyjności przyjąć następującą konwencję terminologiczną:

- Konkurencyjność *ex post* to obecna pozycja konkurencyjna, czyli fotografia stanu konkurencyjności jakiegoś obiektu w danym momencie. Osiągnięta pozycja konkurencyjna jest wypadkową zrealizowanej strategii konkurencyjnej i strategii konkurencyjnych rywali. Konkurencyjność *ex post* to pozycja osiągnięta w efekcie procesu konkurowania, czyli konkurencyjności w sensie procesowym.

- Konkurencyjność *ex ante* jest to przyszła (prospektywna) pozycja konkurencyjna. Jest ona określona między innymi przez relatywną (odniesioną do umiejętności rywali) zdolność obiektu do konkurowania w przyszłości, czyli przez jego potencjał konkurencyjny. Innymi słowy jest to konkurencyjność atrybutowa (rezultatowa) możliwa do zrealizowania w przyszłości.

Budowę, a następnie wykorzystanie potencjału konkurencyjnego opisuje strategia konkurencyjna planowana lub zamierzona. Strategia konkurencyjna obiektu uczestniczącego w procesie konkurowania jest więc kategorią analityczną umożliwiającą przejście od potencjału konkurencyjnego, czyli konkurencyjności potencjalnej (*ex ante*) do konkurencyjności rzeczywistej, czyli zrealizowanej (*ex post*). Strategie konkurowania są stosowane po to, aby konkurujący obiekt mógł zająć jak najlepszą pozycję konkurencyjną. Osiągnięcie pożądanej pozycji konkurencyjnej, czyli przewagi konkurencyjnej w sensie zajmowanej pozycji uwarunkowane jest posiadaniem przewagi konkurencyjnej w zakresie potencjału konkurencyjnego i/lub strategii konkurencyjnej. Innymi słowy posiadanie przewagi konkurencyjnej w zakresie potencjału i/lub strategii jest warunkiem koniecznym dla zajęcia dobrej pozycji konkurencyjnej. Przewaga konkurencyjna w zakresie pozycji konkurencyjnej jest efektem zastosowania zbioru instrumentów konkurowania, które są składnikami strategii konkurowania. Jeśli obiektem, którego konkurencyjność rozpatrujemy jest przykładowo przedsiębiorstwo, to zestaw instrumentów konkurowania może obejmować, takie składniki jak: jakość produktów, cena, odmienność oferowanych produktów, elastyczność dostosowywania produktów do potrzeb odbiorców, częstsze od innych wprowadzanie na rynek nowych produktów itd.

Dodatkowo konieczne jest precyzyjne zdefiniowanie pojęć potencjału konkurencyjnego i pozycji konkurencyjnej. Potencjał konkurencyjny rozpatrywanego obiektu może być rozumiany w wąskim i szerokim znaczeniu. W wąskim znaczeniu potencjał konkurencyjny to wszystkie zasoby wykorzystywane lub możliwe do wykorzystania przez ten obiekt. Jeśli, przykładowo, rozpatrujemy konkurencyjność obiektu, jakim jest przedsiębiorstwo, to zasoby dają się zakwalifikować do trzech grup: pierwotne, wtórne i wynikowe.

W szerszym znaczeniu potencjał konkurencyjny przedsiębiorstwa obejmuje następujące elementy: kultura przedsiębiorstwa, jego zasoby (szeroko rozumiane), struktura organizacyjna przedsiębiorstwa, wizja strategiczna przedsiębiorstwa, właściwy dla przedsiębiorstwa sposób zachowania się (proces tworzenia strategii).

Zasoby przedsiębiorstwa wyznaczają mu pole manewru w otoczeniu gospodarczym i społecznym. Ich ilość ogranicza skalę działania. Ich elastyczność i mobilność wpływają na możliwości zmiany pozycji przedsiębiorstwa w otoczeniu. Szeroko rozumiane zasoby przedsiębiorstwa obejmują zasoby kadrowe, technologiczne, materiałowe, finansowe oraz zasoby niematerialne (np. reputację). Dostępne przedsiębiorstwu zasoby redukują zbiór zachowań możliwych (w danych warunkach otoczenia) do zbioru zachowań wykonalnych. Ilość, charakter i alokacja zasobów przedsiębiorstwa wpływają też na możliwości uzyskania przewagi konkurencyjnej. Ze względu na ograniczone rozmiary tego opracowania nie ma tutaj miejsca na szersze rozwijanie zagadnień potencjału konkurencyjnego.

W literaturze przedmiotu w odniesieniu do przedsiębiorstwa stosuje się zamiennie pojęcia potencjału konkurencyjnego lub potencjału konkurencyjności. W rozważaniach dotyczących gospodarek narodowych najczęściej używa się określenia zdolności konkurencyjnej. Proponuje się, aby w badaniach konkurencyjności o walorze uniwersalnym wymienione pojęcia traktować jako tożsamości. Można je łącznie określić jako konkurencyjność potencjalną.

Z kolei przez pozycję konkurencyjną należy rozumieć rezultat procesu konkurowania, czyli konkurencyjność w sensie atrybutowym (rezultatowym). Pozycja konkurencyjna to wynik zastosowania określonej strategii konkurencyjnej (zestawu instrumentów konkurowania) w odniesieniu do określonego potencjału konkurencyjnego (zestawu zasobów). Odnosząc ponownie rozważania do przykładowego obiektu, jakim jest przedsiębiorstwo, powiemy, że pozycja konkurencyjna przedsiębiorstwa jest to wynik oceny przez rynek (w szczególności przez nabywców) tego, co przedsiębiorstwo na nim oferuje. Najbardziej podstawowymi i syntetycznymi miarami pozycji konkurencyjnej każdego przedsiębiorstwa jest jego udział w rynku oraz osiągnięta sytuacja finansowa. Do kwantyfikacji pozycji konkurencyjnej można jednak wykorzystać znacznie szerszy zestaw następujących mierników: rentowność, poziom kosztów, udział w rynku itp.

Podsumowując przeprowadzone rozważania można zaproponować dekompozycję pojęcia konkurencyjności na trzy składniki:

- konkurencyjność potencjalna, czyli *ex ante* (zdolność konkurencyjna, potencjał konkurencyjny, potencjał konkurencyjności),
- strategia konkurencyjna (instrumenty konkurowania),
- konkurencyjność zrealizowana, czyli *ex post* (pozycja konkurencyjna).

W przeprowadzonych w tym punkcie rozważaniach wymienione składniki konkurencyjności zostały odniesione do poziomu przedsiębiorstwa. W podobny sposób należy postąpić przy rozważaniu konkurencyjności obiektów z innych poziomów systemu gospodarczego.

Pojęcie konkurencyjności można odnosić zarówno do strony podażowej, jak i do strony popytowej gospodarki. Wyróżnić trzeba także konkurencyjność wewnątrzbranżową i konkurencyjność międzybranżową. Ważne jest ponadto dokonanie rozróżnienia konkurencji na rynku krajowym i na rynku zagranicznym. Szersze ujęcie wymienionych aspektów konkurencyjności można znaleźć w przywołanej wcześniej publikacji [18].

Warto zwrócić uwagę na jeszcze jeden aspekt badania konkurencyjności, a mianowicie na porównania konkurencyjności, do których odnoszą się pojęcia różnicy, przewagi i luki konkurencyjnej oraz odpowiednio pojęcia różnicy, przewagi i luki cyfrowej.

Nietrudno spostrzec, że porównania konkurencyjności powinny dotyczyć obiektów z tego samego poziomu – o ile łatwo zgodzimy się, że sens ma porównywanie konkurencyjności na przykład grupy państw, o tyle trudno byłoby zaakceptować propozycję porównywania konkurencyjności gospodarki jakiegoś kraju z konkurencyjnością jakiejś firmy lub jakiegoś pracownika. Jeśli zaakceptujemy wyżej przedstawioną propozycję, że konkurencyjność każdego obiektu można rozpatrywać ze względu na trzy składniki (konku-

rencyjność potencjalna, czyli *ex ante*, strategia konkurowania, konkurencyjność zrealizowana, czyli *ex post*), to wydaje się, że różnice w odniesieniu do każdego składnika konkurencyjności mogą być określane jako przewaga konkurencyjna (różnica *in plus*) lub jako luka konkurencyjna (różnica *in minus*). Łącznie przewagę i lukę konkurencyjną można określić jako różnicę konkurencyjną.

Rozpatrując konkurencyjność dowolnego obiektu należy więc brać pod uwagę jej całościowy opis, który obejmuje elementy przedstawione w tabeli 1.

Tabela 1. Składniki konkurencyjności dowolnego obiektu

Składniki konkurencyjności	Różnica in plus	Różnica in minus
1. konkurencyjność potencjalna (ex ante) – potencjał konkurencyjny, potencjał konkurencyjności, zdolność konkurencyjna	przewaga w zakresie potencjału konkurencyjnego	luka w zakresie potencjału konkurencyjnego
2. strategia konkurencyjna (zestaw instrumentów konkurowania)	przewaga w zakresie strategii konkurencyjnej	luka w zakresie strategii konkurencyjnej
3. konkurencyjność zrealizowana (ex post) – pozycja konkurencyjna	przewaga w zakresie pozycji konkurencyjnej	luka w zakresie pozycji konkurencyjnej

Źródło: opracowanie własne.

Rozważania przeprowadzone powyżej mogą posłużyć za punkt wyjścia do dokonania konkretyzacji schematu analitycznego różnicy konkurencyjnej. Biorąc pod uwagę wcześniejsze ustalenia terminologiczne, można zaproponować wyróżnienie czterech wymiarów (aspektów) różnicy konkurencyjnej:

- różnica konkurencyjna jako odchylenia w bieżącej (aktualnej) pozycji konkurencyjnej danego obiektu w stosunku do rywali,
- różnica konkurencyjna jako odchylenia w przyszłej pozycji konkurencyjnej danego obiektu w stosunku do rywali,
- różnica konkurencyjna jako odchylenia w obecnym (wyjściowym) potencjale konkurencyjnym; potencjał konkurencyjny stanowi jeden z wyznaczników możliwości konkurowania obiektu; współwyznacza on także spectrum możliwych do zastosowania strategii konkurowania; przyjmujemy ponadto, że różnice w przyszłym (odniesionym do jakiegoś momentu przyszłości) potencjale konkurencyjnym będą istotne dla konkurowania w okresie, który nastąpi po tym momencie,
- różnica konkurencyjna jako odchylenia w strategii konkurowania w rozpatrywanym okresie; różnice w strategii konkurowania można sprowadzić do różnic w instrumentach konkurowania, których przykładową listę zaprezentowano wcześniej.

Mówiąc o różnicy konkurencyjnej między określonymi obiektami należy mieć na myśli równocześnie cztery wymienione wymiary tejże różnicy. Pomiar różnicy będzie musiał uwzględniać zmienne szczegółowe (miary) odnoszące się do wszystkich czterech wymiarów. W zapisie formalnym różnicę można przedstawić jako wektor:

$$RK = \begin{bmatrix} RBPK \\ RPPK \\ ROPK \\ RSK \end{bmatrix}$$

gdzie:

RBPK – różnice w bieżącej pozycji konkurencyjnej

RPPK – różnice w przyszłej pozycji konkurencyjnej

ROPK – różnice w obecnym potencjale konkurencyjnym

RSK – różnice w strategii konkurowania

Dla potrzeb prowadzenia diagnozy i analizy w konkretnych przedsiębiorstwach poszczególne wymiary różnicy konkurencyjnej winny zostać szczegółowo zidentyfikowane i opisane (zoperacjonalizowane) w odniesieniu do poszczególnych klas obiektów, których konkurencyjność może być przedmiotem badania. Operacjonalizacja powinna doprowadzić do określenia zmiennych szczegółowych, które są zmiennymi mierzalnymi. Przykłady takich działań zostaną podane w dalszej części opracowania.

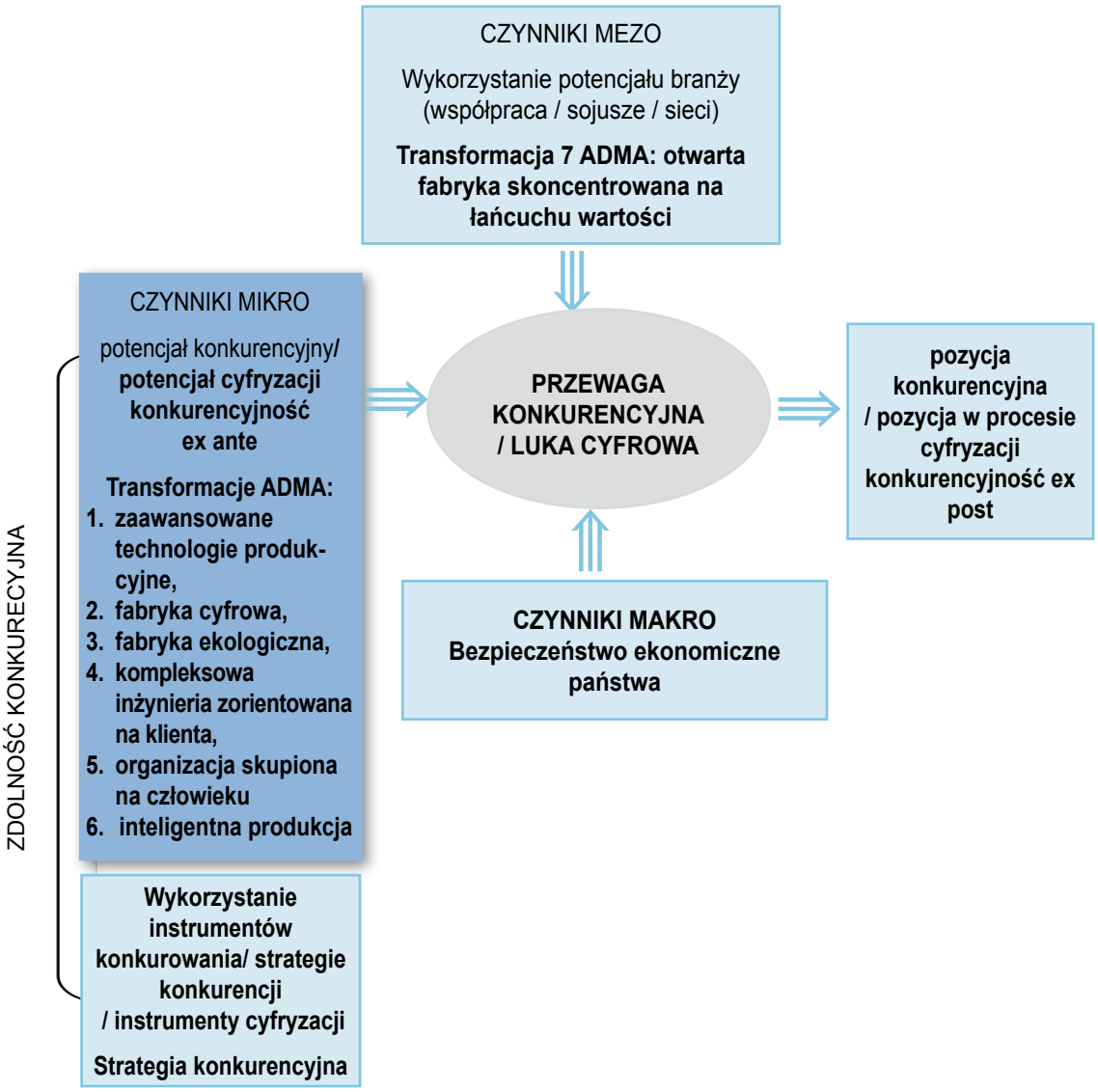
Podsumowując powyższe rozważania należy podkreślić, że konkurencyjność można rozumieć na co najmniej dwa sposoby: po pierwsze jako cecha, atrybut, wynik, rezultat, oraz, po drugie, jako proces. Konkurencyjność można odnosić do różnych poziomów bytu (systemu) gospodarczego. W ekonomii wyróżnia się zasadniczo sześć głównych poziomów hierarchii systemów gospodarczych: mikro-mikro, mikro, mezo, makro, regionalny (w odniesieniu do grupy krajów), globalny. Dodatkowo zasygnalizowano najważniejsze aspekty, takie jak: konkurencyjność *ex ante* i *ex post*, konkurencyjność podażowa i popytowa, konkurencyjność wewnątrzbranżowa i międzybranżowa oraz konkurencyjność na rynku krajowym i zagranicznym.

Przedstawiona wyżej propozycja terminologii mogącej służyć do opisu, analizy i oceny konkurencyjności obejmuje następujące główne składniki: potencjał konkurencyjny, strategia konkurencyjna i pozycja konkurencyjna. W odniesieniu do każdego składnika można mówić o występowaniu różnicy konkurencyjnej in plus (przewaga konkurencyjna) lub różnicy in minus (luka konkurencyjna). Zaprezentowana koncepcja konkurencyjności zostanie w dalszej części wykorzystana do przedstawienia koncepcji różnicy/luki/przewagi cyfrowej odnoszącej się do wykorzystania technologii cyfrowych w praktyce działalności MŚP.

Koncepcję luki cyfrowej wkomponowaną w eklektyczną definicję konkurencyjności przedsiębiorstwa znakomicie rozwija i uzupełnia metodyka ADMA. O ile ta pierwsza definicja jest kategorią teoretyczną, z natury rzeczy bardziej abstrakcyjną, aczkolwiek ujmującą istotę sprawy, o tyle celem metodyki ADMA jest określenie poziomu zaawansowania/dojrzałości przedsiębiorstw produkcyjnych (szczególnie MŚP) w zakresie transformacji niezbędnych do uruchomienia tzw. Fabryk Przyszłości. Obejmują one siedem transformacji korespondujących z poszczególnymi elementami potencjału konkurencyjnego i zdolności jego wykorzystania oraz potencjału branży. Wykorzystanie metodyki ADMA pozwoli na doprecyzowanie szans i zagrożeń wpływających na rozmiar i wymiary luki cyfrowej przedsiębiorstw. Tak więc można uznać, że metodyka ADMA sta-

nowi swoistą konkretyzację i sposób uporządkowania różnorakich aspektów występowania luki cyfrowej, będącej szczególnym przypadkiem luki konkurencyjnej. W tym miejscu należy po raz wtóry wskazać na potrzebę kompleksowego rozpatrywania wszystkich aspektów luki konkurencyjnej i integralnego ich ujmowania na poziomie całości firmy.

Poszczególne transformacje w ADMA korespondują z potencjałem konkurencyjnym przedsiębiorstwa tj.: transformacja 1: zaawansowane technologie produkcyjne; transfor-macja 2: fabryka cyfrowa; transformacja 3: fabryka ekologiczna; transformacja 4: kompleksowa inżynieria zorientowana na klienta; transformacja 5: organizacja skupiona na człowieku oraz transformacja 6: inteligentna produkcja. Ostatnia transformacja 7: otwarta fabryka skoncentrowana na łańcuchu wartości obejmująca diagnozę powiązań sieciowych i współpracy przedsiębiorstw może z powodzeniem zostać przypisana do otoczenia konkurencyjnego (potencjału branży) (Rysunek 7).



Rysunek 7. Konkurencyjność przedsiębiorstwa, koncepcja luki cyfrowej i metodyka ADMA
Źródło: opracowanie własne.

3 Rozwój MŚP w oparciu o technologie cyfrowe

„Zasypanie luki cyfrowej" jest jednym z kluczowych wyzwań stojących przed MŚP, chcącymi dokonywać transformacji swojego biznesu. Dzięki przyjęciu określonego modelu postępowania (modelu danych, modelu procesów) prowadzącego do minimalizacji luki cyfrowej, firmy są w stanie eliminować zagrożenia związane np. z przerastającymi kompetencje firmy wyzwaniami metodologicznymi bądź technologicznymi. Modele takie nazywane są modelami dojrzałości lub gotowości cyfrowej. Jednym z takich modeli jest właśnie ADMA.

Model ADMA pozwala z jednej strony zidentyfikować szanse [19][3] i zagrożenia, z drugiej zaś bardzo precyzyjnie wskazuje obszary wdrażania technologii cyfrowych, dzięki czemu MŚP już w trakcie diagnozy w iteracyjny sposób minimalizuje określoną uprzednio lukę.

3.1. Szanse i zagrożenia dla wybranych obszarów działalności MŚP

O istotności wybranych aspektów wdrażania technologii cyfrowych możemy się przekonać, analizując liczby prac indeksowanych w największych światowych bazach danych. Jedną z najważniejszych jest obecnie Web of Science (WoS) Core Collection[4], zawierająca najbardziej cytowane prace, z tym książki, artykuły i materiały konferencyjne od roku 1900, z uwzględnieniem nie tylko prac technologicznych, ale również społecznych czy humanistycznych.

W pracy „Mapping Industry 4.0 Enabling Technologies into United Nations Sustainability Development Goals" [20] powiązano cele zrównoważonego rozwoju z technologiami wspierającymi czwartą rewolucję przemysłową.

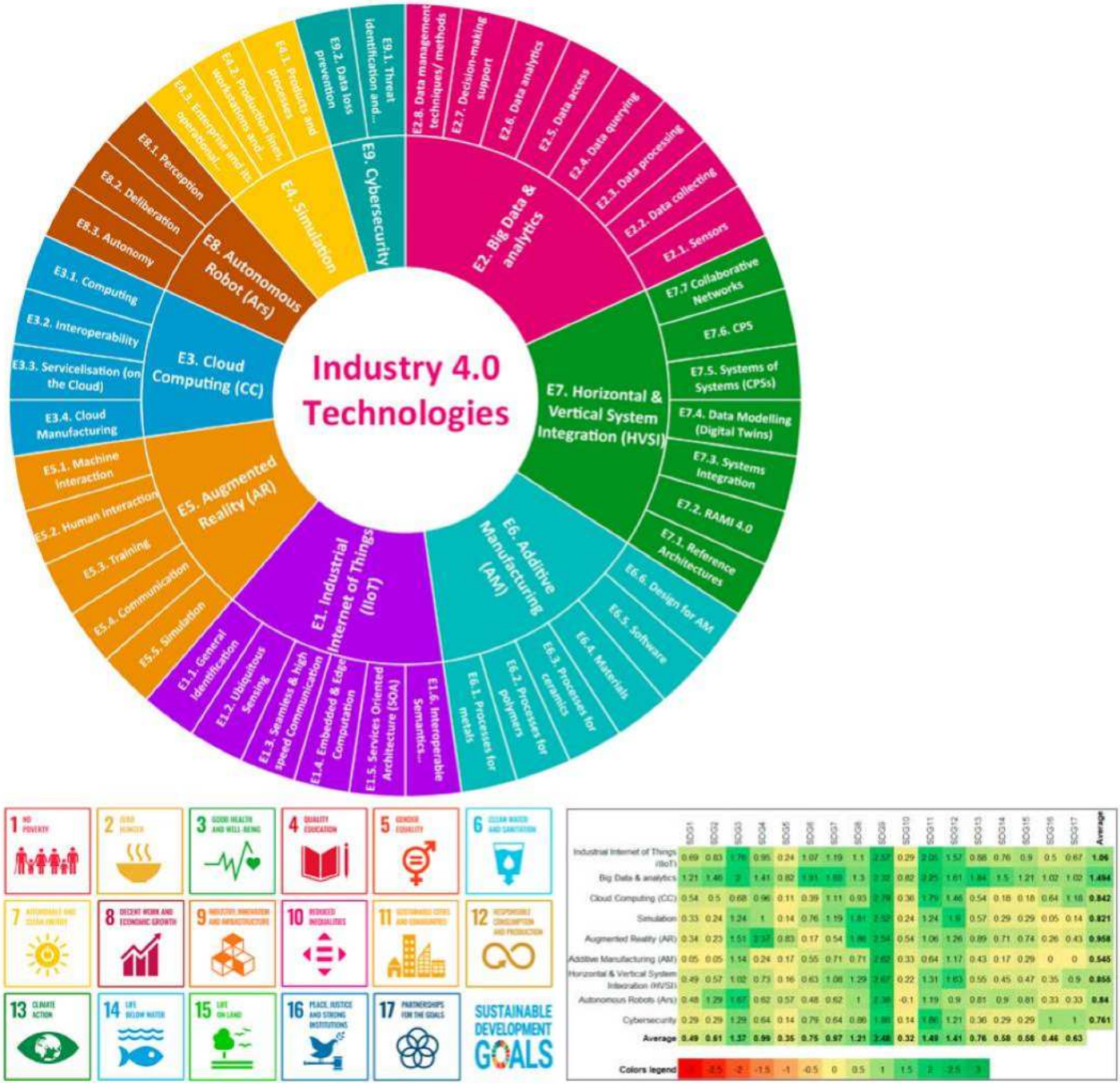
Przyjęta w tej pracy metodyka mapowania została opisana bardzo szczegółowo. Efektem pracy jest wniosek, w myśl którego to analiza dużych zbiorów danych (Big Data), Przemysłowy Internet Rzeczy (IIoT) oraz rozszerzona rzeczywistość (AR) mają największy wpływ na realizację celów zrównoważonego rozwoju w najbliższym czasie.

W niniejszym opracowaniu powiązano kluczowe technologie istotne z perspektywy wdrożenia ich w praktyce przemysłowej MŚP oraz minimalizacji wpływu luki cyfrowej na potencjał konkurencyjny/kompetencyjny przedsiębiorstwa z przyjętym na poziomie europejskim modelem ADMA. Podejście to w przekonaniu autorów ma znacznie bardziej praktyczny wymiar aniżeli podejście autorów pracy [20].

---

3 Model ADMA (Advanced Manufacturing) – opracowany na zlecenie Agencji EASME Komisji Europejskiej w ramach umowy GRO-SME-17-C-063 [44]. Wersja polska opracowania modelu transformacji ADMA dostępna jest na stronach Fundacji Platforma Przemysłu Przyszłości pod adresem: https://przemyslprzyszlosci.gov.pl/skaner-adma-opis/.

4 Clarivate Web of Science Core Collection https://www.webofscience.com/wos/woscc/basic-search.



Rysunek 8. Technologie oraz ich elementy składowe, wspierające I4.0.

Źródło: „Mapping Industry 4.0 Enabling Technologies into United Nations Sustainability Development Goals" https://doi.org/10.3390/su13052560 [20].

W kolejnych podrozdziałach zostaną omówione zidentyfikowane w siedmiu obszarach transformacji szanse i zagrożenia związane z wprowadzaniem technologii cyfrowych w MŚP.

3.1.1. Zaawansowane technologie produkcyjne

Na podstawie analizy artykułów udostępnionych w ramach Web of Science (ang. WoS) w latach 2022-2023 można stwierdzić, że zagadnieniom kluczowych (w tym przełomowych) technologii dla Przemysłu 4.0 poświęcono łącznie blisko 600 prac, w tym zaawan-

sowanej produkcji (99), tzw. uczącym fabrykom (19), fabrykom przyszłości (77), monitorowaniu produkcji w czasie rzeczywistym (157), technologiom przyrostowym (112). Transformacja 1 modelu ADMA związana jest z tym, jak potencjał zaawansowanych technologii produkcyjnych, odpowiednio ukierunkowany oraz zarządzany pod względem wdrażania w przedsiębiorstwie produkcyjnym może powiększać jego potencjał konkurencyjny. Kluczowe w tym obszarze jest zdefiniowanie i konsekwentna realizacja przyjętej strategii rozwoju potencjału cyfryzacji. Powiązanie strategii wdrażania technologii (Internetu Rzeczy, Internetu nowej generacji, Obliczeń chmurowych, Sztucznej inteligencji w tym uczenia maszynowego, Analizy dużych i bardzo dużych zbiorów danych, zastosowania Autonomicznych i zrobotyzowanych systemów produkcyjnych) z przyjętymi w firmie kluczowymi wskaźnikami jakości i produktywności świadczy z całą pewnością o wysokiej zdolności konkurencyjnej przedsiębiorstwa. W transformacji 1 ważne jest budowanie wiedzy przedsiębiorstwa na temat technologii i skutków ich wdrażania, prowadzenie działań uświadamiających w zakresie technologii produkcyjnych oraz sposobów ich wprowadzania do firmy. Z pewnością dużą szansę na rozwój mają te przedsiębiorstwa, które swoje hale produkcyjne są w stanie przygotować pod względem przepływu pracy oraz estetyki, by stały się również narzędziem pozytywnego marketingu. Jest to związane z bardzo ważnymi współcześnie ścieżkami kompetencyjnymi rozwoju, które można rozwijać nie tylko u swoich pracowników, ale również tworzyć na tej podstawie nowe modele biznesowe.

Najistotniejszymi szansami dla przedsiębiorstw sektora MŚP, związanymi z wdrażaniem zaawansowanych technologii produkcyjnej, są: zwiększenie produktywności oraz obniżenie kosztów produkcji, osiągane głównie dzięki standaryzacji wdrażanych w firmie technologii.

Często związana jest z tym konieczność zmiany ugruntowanego w firmie sposobu pozyskiwania informacji o nowoczesnych technologiach z rynku. Konieczność planowania a przede wszystkim komunikowania długofalowych działań inwestycyjnych może stanowić zagrożenie dla działania MŚP. Niniejszy obszar transformacji dla MŚP wiąże się głównie z opracowaniem strategii wdrażania nowych technologii oraz sposobu komunikowania tego zarówno wewnątrz jak i na zewnątrz organizacji. Firmy z reguły w sposób nieuporządkowany pozyskują wiedzę na temat nowych technologii, ma to charakter zdarzeniowy, nie stanowiąc elementu długofalowej strategii.

3.1.2. Cyfrowa fabryka

Przedmiotem Transformacji 2 (Cyfrowa fabryka) są wyzwania technologiczne oraz poszukiwanie sposobów realizacji procesu cyfryzacji przedsiębiorstwa. W ponad 900 pracach, które podaje baza WoS w latach 2022-2023, najczęściej przewijające się hasła to: cyfrowa transformacja (1916), przetwarzanie języka naturalnego (1832; to dość specyficzne zastosowanie metod sztucznej inteligencji do rozpoznawania ludzkiej mowy oraz tekstów swobodnie pisanych przez człowieka, np. do opisywania historycznych zdarzeń oraz podejmowanych decyzji podczas wdrażania systemów informatycznych [21], cyfrowy bliźniak/Asset Administration Shell (1344), e-commerce (858), Przemysłowy Internet Rzeczy (765).

W przypadku transformacji 2 modelu ADMA wiele uwagi przywiązuje się do kompletności przepływu danych (zwykle bardzo dużych zbiorów danych) między wszystkimi urządzaniami na hali produkcyjnej oraz wymiany danych z klientami, z dostawcami, czy wreszcie cyfryzacji konfiguracji produktów. Koncepcja tzw. pojedynczego źródła prawdy leży u podstaw projektowania cyfrowych systemów produkcyjnych – jej główne założenie opiera się na tezie, w myśl której wszyscy widzą te same dane, wprowadzane do systemu w określonym czasie, dostępne w taki sam sposób.

Kluczowym wyzwaniem w obszarze cyfryzacji MŚP jest zapewnienie odpowiedniego poziomu cyberbezpieczeństwa.

W ramach transformacji cyfrowej fabryki w literaturze pojawia się wiele angielskojęzycznych nazw systemów informatycznych: Production Management Systems (670), Business Intelligence (494), Computer Aided Manufacturing (314), Manufacturing Process Software (138), Cloud/Edge computing (130), Robotic Process Automation (65), Manufacturing Execution System (23). Terminy te odnoszą się zwykle do grup/typów programów komputerowych, wykorzystywanych do rozwiązywania różnych problemów biznesowych. Zakres ich użycia wynika z konkretnego obszaru i zakresu działalności MŚP.

Niezaprzeczalnym zagrożeniem w przypadku tej transformacji jest niewłaściwe podejmowanie decyzji inwestycyjnych w zakresie wdrażania rozwiązań cyfrowych w firmie (sprzęt i oprogramowanie). Wiele uwagi należy przywiązywać do systemowego wdrażania strategii cyfrowej transformacji. Konieczne jest również zapewnienie cyberbezpieczeństwa, odpowiadającego na potrzeby wynikające z rozwoju firmy.

Szansą dla MŚP w przypadku podjęcia wyzwania cyfryzacji i wdrożenia dobrze dobranych do celów firmy technologii cyfrowych jest stabilny wzrost i minimalizacja luki cyfrowej.

3.1.3. Fabryka ekologiczna

Współcześnie przywiązuje się dużą wagę nie tylko do zagadnień związanych z cyfrową, ale również z zieloną transformacją zgodnie z podejściem opisanym w ramach Europejskiego Zielonego Ładu [22]. Transformacje te są ze sobą ściśle powiązane, głównie z uwagi na złożoność zielonej transformacji, która bez odpowiedniego poziomu cyfryzacji może stać się jedynie przyczynkiem do braku spójności pomiędzy celami MŚP w zakresie usprawniania gospodarki zarządzania zasobami i odpadami.

Ma to swoje odzwierciedlenie w pracach indeksowanych w przywołanej tutaj bazie Web of Science. Pośród ponad 4000 prac poświęconych zagadnieniom ekologicznych rozwiązań na potrzeby produkcji blisko 3800 porusza problematykę odnawialnych źródeł energii: fotowoltaika (1000), ogólnych problemów odnawialnych źródeł energii (905), inteligentnych sieci energetycznych (861), alternatywnych paliw (518), ogniw wodorowych (355) oraz rosnących w ostatnich miesiącach na znaczeniu zagadnień morskiej energetyki wiatrowej (158).

Technologie cyfrowe, w tym oprogramowanie związane z zarządzaniem Gospodarką Obiegu Zamkniętego (148) i Analizą Cyklu Życia (ang. LifeCycle Assessment – LCA, 21)

stanowią przedmiot mniejszej liczby prac. Oprogramowanie wspierające całościowo analizy LCA staje się jednak coraz bardziej popularne na rynku[5]. Dzięki tego typu narzędziom już niedługo wyznaczenie wpływu działalności na środowisko, dotychczas trudne lub wręcz niemożliwe stanie się, dzięki analizie dużych zbiorów danych oraz odpowiednio zaprojektowanym wskaźnikom, codziennością – na dodatek już nie tak kosztowną jak jeszcze kilka lat temu.

Upowszechnienie oprogramowania wspierającego analizę LCA jest to bardzo dużą szansą dla MŚP. Dzięki technologiom takim jak obliczenia chmurowe czy sztuczna inteligencja możliwe będzie zmniejszenie negatywnego wpływu procesu produkcji oraz samego produktu na środowisko. Dzięki technologii Przemysłowego Internetu Rzeczy można zapewnić stały dostęp do informacji na temat zużycia energii (wielu jej parametrów, nie tylko zużytej energii) oraz zarządzać odpadami w kierunku ich minimalizacji.

Dużym zagrożeniem w tym obszarze jest błędne zdefiniowanie wskaźników, na podstawie których dane przedsiębiorstwo będzie budować swoją strategię transformacji w kierunku fabryki ekologicznej. Fabryka ekologiczna to bowiem nie tylko odnawialne źródła energii, ale aktywność całego łańcucha wartości, w ramach którego MŚP funkcjonuje.

Transformacja zielona może się nie udać, bez uprzedniej minimalizacji luki cyfrowej. To istotne zagrożenie i pokazuje, jaką kolejność należy przyjąć transformując swoje przedsiębiorstwo.

3.1.4. Kompleksowa inżynieria zorientowana na Klienta

Najważniejszym jak dotychczas dokumentem związanym z cyfryzacją, odnoszącym się do niniejszego obszaru transformacji przedsiębiorstwa produkcyjnego jest standard VDI/VDE 2206 „Development of mechatronic and cyber-physical systems" [23]. Kolejnym kamieniem milowym jest przyjęcie na poziomie europejskim i wskazanie jako rekomendowanego przez Stadardization Council Industrie 4.0 referencyjnego modelu architektury systemów Przemysłu 4.0, zwanego RAMI 4.0 (Reference Architecture Model Industrie 4.0) [24]. Jedna z osi modelu RAMI 4.0 dotyczy tego, w jaki sposób nowe projekty i produkty przynoszą wartość firmie, która je realizuje (oś Life Cycle and Value Stream, zgodnie z normą IEC 62890).

W ostatnich latach coraz większą popularność wśród firm przemysłowych zyskuje oprogramowanie łączące koncepcję graficznego programowania oraz wirtualnej weryfikacji i walidacji, ugruntowane w przemyśle motoryzacyjnym. O tym, jak wdrażać w firmie podejście znane w literaturze jako Model-Based Design można przeczytać w pracy wieloletniego inżyniera Firmy Mathworks, Rogera Aarenstrupa [25]. W latach 2022-2023 w bazach Web of Science pojawiło się ponad 1100 prac poświęconych cyfryzacji procesów projektowania i tworzenia nowych lub ulepszonych produktów w oparciu o koncepcję tzw. systemów cyberfizycznych (638), z zastosowaniem narzędzi cyfrowego wsparcia projektowania (345). Branża motoryzacyjna oraz kosmiczna odcisnęły swoje piętno wprowadzając do słownika pojęcie Model-Based Systems Engineering (118) zaś ciągłe po-

5 Strona producenta oprogramowania OneClick LCA. https://www.oneclicklca.com/

prawianie procesów projektowania oprogramowania w złożonych systemach sprawia, że rośnie popularność narzędzi programowych, dzięki którym możliwe staje się dziedzinowe modelowanie i projektowanie, np. urządzeń medycznych czy też wspierających zdalną rehabilitację/monitorowanie pacjentów (42).

Szansą w przypadku wysokiego poziomu cyfryzacji procesów projektowania jest osiągnięcie 100% dopasowania produktu do rzeczywistych, wyartykułowanych, sparametryzowanych a następnie dobrze udokumentowanych i zarządzanych potrzeb klientów. Dzięki temu MŚP może szybko odpowiadać na potrzeby rynku oraz w krótkim czasie wprowadzać na rynek nowe lub ulepszone produkty. Systematyczne gromadzenie i analiza (parametryzacja) wymagań klientów zwykle prowadzi do modularyzacji oferowanych produktów zaś w dalszej perspektywie do obniżenia kosztu wytwarzania nowych wersji produktu.

Zdecydowanie dużym wyzwaniem i zagrożeniem dla tego obszaru jest wysoki próg kompetencji, niezbędnych do efektywnego użycia narzędzi cyfrowych wspomagających ten obszar działania MŚP. Koszt oprogramowania w tym obszarze jest również dość wysoki. Podobnie jak konieczność ustrukturyzowania procesów i narzędzi pracy zespołowej nad projektami w firmie.

3.1.5. Organizacja skupiona na człowieku

W latach 2018 – 2023 w projektach Europejskiego Funduszu Społecznego uznawano za priorytetowy rozwój kompetencji: cyfrowych, językowych, analitycznych (w tym umiejętności rozwiązywania problemów), komunikacyjnych (w tym umiejętności pracy w grupie) oraz w zakresie przedsiębiorczości. Pandemia COVID-19 sprawiła, że tempo rozwoju kompetencji cyfrowych, również w zakresie rozwoju kompetencji komunikacyjnych oraz pracy zespołowej, było niekiedy ponad siły i percepcję pracowników firm. Konieczna była interwencyjna aktywność doradców zawodowych oraz wsparcie psychologiczne.

Pandemia koronawirusa uderzyła w firmy nie tylko w wymiarze produkcyjnym, ale również ludzkim. Z drugiej zaś strony pojawiły się liczne wyzwania związane z systemowym podejściem do rozwoju kompetencji pracowników.

Obecna perspektywa finansowania projektów, związanych z rozwojem kompetencji wskazuje dwa obszary priorytetowe: kompetencje cyfrowe oraz kompetencje na rzecz zielonej transformacji [26]. Jak już wskazano w rozdziale poświęconym transformacji MŚP w kierunku fabryki ekologicznej, niezbędne jest najpierw zbudowanie odpowiedniego poziomu kompetencji cyfrowych. Poniżej przytoczono przykładowe kompetencje cyfrowe, zdaniem autorów niezbędne do efektywnego wdrażania technologii w firmach sektora MŚP, przy czym przez kompetencje cyfrowe rozumiemy tutaj: **umiejętność efektywnej współpracy cyfrowej, opanowanie narzędzi, technologii i umiejętności interpersonalnych wymaganych do współpracy cyfrowej.**

Do najistotniejszych kompetencji cyfrowych zaliczamy:

1. kompetencje i zaawansowane umiejętności korzystania z narzędzi cyfrowych i Internetu – umiejętność prawidłowego korzystania z zaawansowanych technologii cyfrowych w pracy;

2. ogólna wiedza o operacjach informatycznych – ogólna wiedza i zrozumienie działania istniejących narzędzi cyfrowych (sprzętu i oprogramowania). Podstawowa umiejętność wdrażania wymagań technicznych organizacji (od konserwacji po programowanie);
3. komunikacja cyfrowa – tworzenie i dystrybucja treści cyfrowych w celu budowania rozpoznawalności w Internecie;
4. zarządzanie danymi – efektywne zarządzanie danymi, ich strategiczne wykorzystanie, zapewnienie bezpieczeństwa i zgodności z przepisami;
5. bezpieczeństwo cyfrowe – zrozumienie wyzwań związanych z bezpieczeństwem informatycznym. Ocena i zarządzanie ryzykiem. Organizowanie zapobiegania naruszeniom i zapewnienie poufności, integralności oraz dostępności informacji cyfrowych;
6. włączenie cyfrowe – zrozumienie kwestii i barier związanych z dostępem do technologii cyfrowych i korzystaniem z nich przez różnych użytkowników. Uwzględnianie tych barier podczas projektowania narzędzi cyfrowych;
7. zarządzanie zmianą – umiejętność planowania, wdrażania i skutecznego zarządzania zmianami związanymi z transformacją cyfrową. Promowanie akceptacji, adaptacji i sukcesu nowych inicjatyw (skuteczna komunikacja, przywództwo, zarządzanie oporem itp. związane ze zmianami);
8. kompetencje w zakresie programowania – umiejętność prawidłowego projektowania, wytwarzania, testowania oraz dokumentowania oprogramowania w wybranych językach;
9. kompetencje w zakresie Big-Data i Data-Science – umiejętność przygotowania danych do wyciągania wniosków z dużych zbiorów danych. Umiejętność projektowania o wytwarzania oprogramowania, służącego do tego celu. Umiejętność krytycznego wyciągania wniosków oraz projektowania systemów automatycznego podejmowania decyzji na podstawie gromadzonych w czasie rzeczywistym danych;
10. kompetencje w zakresie wizualizacji danych – umiejętność gromadzenia wymagań wobec celu wizualizacji danych. Znajomość współczesnych narzędzi przetwarzania i wizualizacji danych, zarządzania udostępnianiem i raportowaniem w systemach klasy *Business Intelligence*.

O tym, jak ważny jest uporządkowany, systemowy rozwój kompetencji cyfrowych niech poświadczą liczne dostępne w Internecie dokumenty strategiczne [27] oraz serwisy poświęcone DESI (*Digital Economy and Society Index* [28]). Eksperci Fundacji Platforma Przemysłu Przyszłości opracowali narzędzie – Weryfikator kompetencji cyfrowych, wspomagające metodyczny rozwój trzech ostatnich wskazanych na powyższej liście kompetencji [29].

W bazie Web of Science znajdujemy w latach 2022-2023 blisko 3000 prac, poświęconych transformacji kompetencyjnej firm, wdrażających technologie Przemysłu 4.0. Co ciekawe, autorzy tych prac rzadko skupiają się na kompetencjach miękkich (7) czy modelach kompetencyjnych (37, modele kompetencji dla Przemysłu 4.0 – 51 prac), a znacznie bardziej na konkretnych kompetencjach cyfrowych (364) oraz narzędziach (z reguły cyfrowych, co nie dziwi), dzięki którym kompetencje cyfrowe mogą zostać w krótkim czasie wzmocnione. Kursom typu MOOC (Massive Open Online Courses)

poświęcono 263 prace. Metodyki pracy nad rozwojem kompetencji jak blended learning (886) oraz Problem-Based Learning (446) wskazywane są najczęściej jako te, które w powiązaniu z innowacyjnymi narzędziami (727), w tym wirtualną i rozszerzoną rzeczywistością, edukacyjnymi zestawami do druku 3D oraz programami do symulacji zjawisk fizycznych (systemów cyber-fizycznych), zapewniają najszybszy wzrost kompetencji cyfrowych.

Pokazuje to w jasny sposób, jak duża jest luka cyfrowa w wymiarze kompetencyjnym i jak wiele jest do zrobienia w tym obszarze. Modele rozwoju kompetencji są już opracowane, sposoby pomiaru i planowania rozwoju również – czas podjąć działanie, zmierzające do rozwoju kompetencji cyfrowych w MŚP do poziomu, który w zauważalny sposób będzie przeciwdziałać luce cyfrowej oraz postępującemu wykluczeniu cyfrowemu części społeczeństwa.

Szansą dla rozwoju MŚP dzięki stabilnemu przyrostowi kompetencji cyfrowych jest zwiększenie ogólnej produktywności firmy, poprawa komunikacji wewnętrznej i zewnętrznej oraz istotnie większa odporność na zmiany. Pracownicy o wyższych kompetencjach zapewniają lepszą atmosferę i ogólnie samopoczucie swoje i otoczenia. Najbardziej doświadczeni pracownicy mogą stać się mentorami dla mniej doświadczonych członków zespołów.

Do najważniejszych zagrożeń zaliczyć tutaj należy realizację rozwoju kompetencji cyfrowych bez jasnej korelacji z celami organizacji. Może do tego doprowadzić bardzo duża liczba dostępnych na rynku materiałów e-learningowych niskiej jakości. Inwestycje w rozwój kadry powinny mieć przełożenie na obszar aktywności pracowników, powinni również czuć swój sprawczy wpływ w zakresie kierunków rozwoju i tempa przyrostu kompetencji cyfrowych. W tym obszarze bardzo łatwo

o potknięcie, które może kosztować firmę utratę wartościowej kadry.

3.1.6. Inteligentna produkcja

Jednym z kluczowych obszarów działalności MŚP produkcyjnych pod względem zastosowania metod sztucznej inteligencji jest tzw. inteligentna produkcja. Nie polega ona na produkowaniu inteligentnych produktów, tylko na inteligentnym podejściu do optymalizacji procesów produkcyjnych oraz tzw. odchudzania produkcji, skutkującego zazwyczaj podniesieniem ogólnej produktywności.

Baza Web of Science zawiera ponad 1400 prac z lat 2022-2023, związanych z optymalizacją produkcji (157), jej planowaniem (495) oraz z uwzględnieniem zastosowania elastycznych systemów produkcyjnych (195). Najwięcej uwagi autorzy poświęcają zagadnieniom predykcyjnego utrzymania ruchu, również z zastosowaniem metod sztucznej inteligencji, w tym głównie uczenia maszynowego (553).

Ten obszar transformacji MŚP koncentruje się na ciągłej poprawie procesów oraz zwiększaniu produktywności, na początek przez eliminowanie strat. Cechą charakterystyczną zastosowania technologii cyfrowych jest m.in. utylitarny charakter użycia metod sztucznej inteligencji do skrócenia czasu przezbrojenia linii produkcyjnych podczas zmiany wytwarzanego produktu. Poza specjalistycznym oprogramowaniem,

podobnie jak w przypadku transformacji 1 (Zaawansowane technologie produkcyjne tak i tutaj ważne jest zdefiniowanie wskaźników, na podstawie których MŚP podejmie decyzję o inwestycji w rozwiązania poprawiające produktywność.

Zastosowanie technologii Przemysłowego Internetu Rzeczy w powiązaniu z rozwiązaniami typu Business Intelligence i metodami sztucznej inteligencji dają szansę na lepszy dostęp i zarządzanie danymi w produkcji, szybką rekonfigurację nawet całych linii produkcyjnych, zapewniając tym samym możliwość bieżącego dostosowania produkcji do zapotrzebowania.

W obszarze inteligentnej produkcji dużym zagrożeniem wydaje się przede wszystkim niska dostępność kadry o wysokich kompetencjach, umożliwiających dobór narzędzi i metod do potrzeb firmy w zakresie transformacji związanej z inteligentną produkcją. Kosztem własnym MŚP wdrażającego rozwiązania cyfrowe jest konieczność uporządkowania i ustandaryzowania procesów przed podjęciem wyzwania cyfryzacji.

3.1.7. Otwarta fabryka skoncentrowana na łańcuchu wartości

Ostatnim obszarem transformacji zgodnie z modelem ADMA jest transformacja związana z szeroko rozumianą współpracą wewnętrzną oraz z otoczeniem. Nie dziwi tym samym liczba prac związanych z tematyką Customer Relationship Management (CRM, systemy cyfrowe wspomagające zarządzanie relacjami z klientami, 218 prac w latach 2022-2023), jakie znajdujemy w bazie Web of Science. Kolejnym trendem w tym obszarze jest tzw. kokreacja (203). Współtworzenie nowych produktów we współpracy z klientami jest możliwe wtedy, gdy MŚP charakteryzuje się wysokim poziomem gotowości/dojrzałości cyfrowej w obszarze transformacji 4 (Kompleksowa inżynieria zorientowana na Klienta).

Niewiele jest w ostatnim czasie prac nt. cyfrowych modeli biznesowych (20) oraz modeli transformacji firm (11). Wydaje się bowiem, że temat ten jest już na tyle ugruntowany, że należy czerpać z wytycznych i dobrych praktyk, które już są dostępne na rynku.

Cechą charakterystyczną firm sektora MŚP, które podejmują działania związane z niniejszą transformacją jest chęć otwarcia się na innowacje pochodzące zarówno z wnętrza organizacji, od pracowników budujących potencjał konkurencyjny każdego dnia jak również z zewnątrz: od podmiotów takich jak uczelnie, ośrodki badawczo-rozwojowe, klastry branżowe, stowarzyszenia branżowe/sektorowe.

Dużą szansą dla sektora MŚP w tym obszarze jest możliwość budowania lub udziału w partnerstwach badawczo-rozwojowych z jednostkami badawczo-rozwojowymi i uczelniami technicznymi, dostęp do bardzo rozległej wiedzy zewnętrznej. Skutkiem wysokiego poziomu transformacji w tym obszarze jest również elastyczność łańcucha dostaw i możliwości w zakresie bezpieczeństwa dostaw.

Firma, która chce zwiększyć swoją otwartość na otoczenie musi nastawić się na zdefiniowanie w ramach swoich struktur nowych ról związanych z cyfrowymi modelami biznesowymi. Na początku drogi można posiłkować się ekspertami zewnętrznymi, jednakże często okazuje się, że lepszym rozwiązaniem jest budowanie potencjału konkurencyjnego i minimalizowanie wpływu luki cyfrowej w tym obszarze, bazując na własnych zasobach.

3.1.8. Podsumowanie

W ramach niniejszego rozdziału dokonano identyfikacji szans i zagrożeń/wyzwań związanych z wdrażaniem technologii w 7 obszarach transformacji MŚP, zgodnie z modelem ADMA. Rozważania te podsumowano w poniższej tabeli (Tabela 2).

Tabela 2. Identyfikacja szans i zagrożeń/wyzwań związanych z wdrażaniem technologii w 7 obszarach transformacji MŚP, zgodnie z modelem ADMA

Obszar transformacji ADMA	Szanse	Wyzwania
T1. Zaawansowane technologie produkcyjne	1. Obniżenie kosztów produkcji dzięki standaryzacji 2. Zwiększenie produktywności MŚP dzięki świadomemu wykorzystaniu technologii	1. Konieczność zmiany sposobu gromadzenia informacji o nowych technologiach 2. Konieczność opracowania strategii inwestycji w nowe technologie
T2. Cyfrowa fabryka	1. Obniżenie wykluczenia cyfrowego 2. Stabilny rozwój MŚP w różnych obszarach	1. Konieczność zapewnienia wysokiego poziomu cyberbezpieczeństwa 2. Konieczność opracowania strategii inwestycji w nowe technologie cyfrowe
T3. Fabryka ekologiczna	1. Świadoma gospodarka zasobami i odpadami 2. Zwiększenie poziomu optymalności produktu	1. Konieczność zdefiniowania wskaźników dla wdrażania rozwiązań proekologicznych 2. Konieczność opracowania strategii wdrażania założeń zielonej transformacji z zastosowaniem technologii cyfrowych
T4. Kompleksowa inżynieria zorientowana na Klienta	1. Skrócenie czasu wprowadzania na rynek produktów, bardzo dobrze odpowiadających na potrzeby klientów	1. Konieczność opracowania strategii inwestycji w oprogramowanie 2. Konieczność podniesienia kompetencji pracowników w działach B+R
T5. Organizacja skupiona na człowieku	1. Zwiększenie ogólnej produktywności firmy 2. Poprawa komunikacji wewnętrznej i zewnętrznej 3. Większa odporność na zmiany otoczenia	1. Konieczność opracowania strategii rozwoju i ogólnie zarządzania zasobami ludzkimi 2. Konieczność zdefiniowania nowych ról dla organizacji
T6. Inteligentna produkcja	1. Lepszy dostęp i zarządzanie danymi w produkcji 2. Szybka rekonfiguracja nawet całych linii produkcyjnych 3. Zapewnienie możliwości bieżącego dostosowania produkcji do zapotrzebowania klientów	1. Konieczność uporządkowania i ustandaryzowania procesów przed podjęciem wyzwania cyfryzacji 2. Niska dostępność kadry o wysokich kompetencjach, umożliwiających dobór narzędzi i metod do potrzeb firmy
T7. Otwarta fabryka skoncentrowana na łańcuchu wartości	1. Możliwość budowania lub udziału w partnerstwach badawczo-rozwojowych z jednostkami badawcz-rozwojowymi i uczelniami technicznymi 2. Dostęp do bardzo rozległej wiedzy zewnętrznej 3. Elastyczność łańcucha dostaw i możliwości w zakresie bezpieczeństwa dostaw	1. Konieczność zdefiniowania w firmie nowych ról związanych z cyfrowymi modelami biznesowymi 2. Konieczność otwarcia się na współpracę i rezygnacji ze *status quo* w obszarach współpracy

Źródło: opracowanie własne.

To, co łączy wszystkie obszary transformacji MŚP w drodze do Przemysłu Przyszłości, to zapewnienie firmie bezpieczeństwa:

- świadomego dostępu do najnowocześniejszych technologii,
- bezpieczeństwa wytwarzania i przetwarzania danych,
- w zakresie dostępności zasobów oraz wypełniania norm w zakresie powstających podczas produkcji odpadów,
- myśli technologicznej wytwarzanej w działach projektowych, również w ramach współpracy z otoczeniem,
- dokumentacji i innych wytworów pracy rąk zatrudnionych w firmie zarówno inżynierów jak i pracowników administracji.

W kolejnym rozdziale skupimy się na rozpoznaniu luki cyfrowej, charakteryzującej funkcjonowanie polskich MŚP.

3.2. Identyfikacja luki cyfrowej

Zgodnie z siatkę pojęciową zaproponowaną w punkcie 2 luka/różnica cyfrowa (LC) stanowi w proponowanym tutaj ujęciu pewien składnik luki/różnicy konkurencyjnej. Akceptacja tej konstatacji oznacza, że uzasadnione jest skonkretyzowanie trzech zaproponowanych wymiarów luki/różnicy konkurencyjnej, a mianowicie potencjału konkurencyjnego, strategii konkurencyjnej i pozycji konkurencyjnej. Operacjonalizacja tych trzech zagadnień jest przedmiotem tej części opracowania.

Obecna pozycja cyfrowa rozpatrywania w jakimś momencie odniesionym do danego przedsiębiorstwa to wynik procesu konkurowania zachodzącego w okresie poprzedzającym moment, dla którego staramy się ustalić aktualną pozycję cyfrową. Obecna pozycja cyfrowa to inaczej pozycja konkurencyjna firmy odniesiona do sfery cyfryzacji, rozpatrywana z punktu widzenia różnic (przewag/mocnych stron oraz luk/deficytów/słabych stron) widzianych jako rezultat procesu konkurowania w przeszłości. Tak rozumiana pozycja cyfrowa może być opisana przez następujące zmienne:

- rentowność (relatywna, tzn. w porównaniu z konkurentami z branży) działań podejmowanych w ramach procesu cyfryzacji (stosunek osiągniętych wyników i poniesionych nakładów w związku z cyfryzacją),
- skala nakładów na cyfryzację w relacji do nakładów najważniejszych konkurentów,
- poziom kosztów cyfryzacji (relatywny w zestawieniu z głównymi konkurentami),
- cechy stosowanych technologii cyfrowych w porównaniu z cechami technologii używanych przez konkurentów,
- znajomość osiągnięć firmy i jej osiągnięć w zakresie cyfryzacji na rynku oraz związane z tym postrzeganie firmy przez otoczenie.

Obecny potencjał cyfrowy obejmuje zestaw czynników związanych z zasobami, jakimi dysponuje firma w procesie cyfryzacji działalności, ale też zawiera w sobie szerszą listę zmiennych. W tym szerszym znaczeniu potencjał cyfryzacji przedsiębiorstwa obejmuje następujące elementy:

- jego zasoby (szeroko rozumiane) wykorzystywane w procesie cyfryzacji,
- kultura przedsiębiorstwa odnosząca się do cyfryzacji,
- ujęcie kwestii cyfryzacji w strukturze organizacyjnej przedsiębiorstwa,
- miejsce cyfryzacji w wizji strategicznej przedsiębiorstwa,
- właściwy dla przedsiębiorstwa sposób zachowania się (proces tworzenia strategii) w zakresie cyfryzacji.

Zasoby przedsiębiorstwa wyznaczają mu pole manewru w otoczeniu gospodarczym i społecznym, w tym wypadku w zakresie cyfryzacji. Ich ilość ogranicza skalę działania firmy w tym zakresie. Ich elastyczność i mobilność wpływają na możliwości zmiany pozycji przedsiębiorstwa w otoczeniu na bardziej korzystną. Szeroko rozumiane zasoby przedsiębiorstwa obejmują zasoby kadrowe, technologiczne, materiałowe/sprzętowe, finansowe oraz zasoby niematerialne (np. reputację). Zasoby kadrowe w zakresie cyfryzacji to pracownicy, którzy są zaangażowani w procesy digitalizacji działań przedsiębiorstwa, ale też pozostałe kadry, które mogą wnieść do tych procesów jakiś wkład. Zasoby technologiczne sprowadzają się do dysponowania przez przedsiębiorstwo zestawem metod i narzędzi, które są wykorzystywane w podejmowaniu działań cyfrowych. Kolejny element stanowią sprzęt i stosowne materiały niezbędne w procesach digitalizacji. Wymienione składniki zasobów przedsiębiorstwa łącznie prowadzą do pojęcia kompetencji czy umiejętności cyfrowych firmy. Zasoby finansowe stanowią natomiast źródło finanso-wania dla tychże składników. Dostępne przedsiębiorstwu zasoby redukują zbiór zachowań potencjalnych/możliwych (w danych warunkach otoczenia) do zbioru zachowań wykonal-nych. Warto podkreślić, że ilość, jakość, charakter i alokacja zasobów przedsiębiorstwa wykorzystywanych w sferze cyfryzacji wpływają na możliwości budowania/uzyskania różnicy cyfrowej (przewagi albo luki konkurencyjnej w sferze cyfrowej). Z powyższego rozumowania wynika jednoznaczny wniosek, że zasoby przedsiębiorstwa istotne z punktu widzenia występowania i „zasypywania" ewentualnej luki cyfrowej wcale nie ograniczają się wyłącznie do zagadnień technologicznych opisanych w metodyce ADMA.

Kultura przedsiębiorstwa określa, które sposoby zachowania się gospodarczego są preferowane przez właścicieli, kierowników i pracowników firmy. W jednych przedsiębiorstwach priorytet zyskują zachowania nowatorskie, w innych przewagę mają zachowania zachowawcze. W jednych przedsiębiorstwach ryzyko podejmowane jest chętnie, inne przedsiębiorstwa wykazują awersję w stosunku do ryzyka. Ogólnie rzecz biorąc, jedne przedsiębiorstwa mogą wykazywać kulturę sprzyjającą zachowaniom konkurencyjnym (np. przedsiębiorczym), podczas gdy inne takiej kultury nie posiadają. Ogólne cechy kultury przedsiębiorstwa stanowią trudne do przecenienia uwarunkowanie cyfryzacji i budowania różnicy konkurencyjnej w tej sferze. Wydaje się, że cyfryzacji sprzyjają takie okoliczności jak nastawienie przedsiębiorcze skłonności do zachowań nowatorskich oraz akceptacja relatywnie wysokiego poziomu ryzyka.

Organizacja przedsiębiorstwa określa, czyje preferencje w przedsiębiorstwie będą miały większe, a czyje mniejsze znaczenie. Na strukturę organizacyjną przedsiębiorstwa składają się: podział władzy, podział pracy i sieć łączności. Można więc rozważać usytuowanie w strukturze organizacyjnej pracowników odpowiedzialnych za cyfryzację, ich zakresy kompetencji oraz umiejscowienie w sieci łączności.

Na rzeczywiste zachowanie się przedsiębiorstwa w sferze cyfryzacji wpływa też istniejąca wizja strategiczna (niekiedy formalny plan strategiczny), określająca jego domenę celową, czyli w uproszczeniu przedmiot działalności, misję i sposób zachowania się. Znaczenie istniejącej wizji w zakresie cyfryzacji (zakładamy, że wizja w zakresie cyfryzacji jest immanentnym składnikiem wizji całego przedsiębiorstwa) zależy od jej klarowności, zakresu jej poparcia (przez ośrodki władzy, wewnątrz i na zewnątrz przedsiębiorstwa), dotychczasowych doświadczeń w jej realizacji oraz możliwości wprowadzenia jej w życie.

Strategia przedsiębiorstwa w obszarze cyfryzacji wyłania się z procesu tworzenia strategii cyfryzacji. Składają się nań dwa subprocesy – proces formułowania wizji (planu) strategicznej w zakresie cyfryzacji oraz proces wdrażania wizji/planu cyfryzacji w życie. Poszczególne przedsiębiorstwa dysponują wypracowanymi rutynami poszukiwawczymi, planistycznymi i realizacyjnymi, między innymi w zakresie cyfryzacji. Czynniki zewnętrzne i wewnętrzne powodują, że przedsiębiorstwa są mniej lub bardziej skłonne do zmiany stosowanego zestawu rutyn w tym obszarze. W niektórych takie rutyny wręcz jeszcze nie zdążyły się wyraźnie ukształtować. Czynniki zewnętrzne i wewnętrzne powodują też, że zachowanie się przedsiębiorstwa bardziej zbliża się do planowanego kursu (skutecznego wdrażania klarownej wizji strategicznej w zakresie cyfryzacji) albo też do dryfu strategicznego (wynikającego albo z braku jasnej wizji strategicznej cyfryzacji) albo z niemożności wprowadzenia jej w życie). Z powyższych uwag wyłania się wniosek, że strategia przedsiębiorstwa (zdolność jej tworzenia i wdrożenia) w zakresie cyfryzacji może też być traktowana jako swego rodzaju zasób, czyli element potencjału konkurencyjnego cyfryzacji.

Pożądana/proponowana pozycja cyfrowa to inaczej konkurencyjność *ex ante* rozumiana jako przyszła (prospektywna) pozycja konkurencyjna w zakresie cyfryzacji. Jest ona określona między innymi przez relatywną (odniesioną do umiejętności rywali) zdolność firmy do konkurowania w przyszłości w zakresie cyfryzacji, czyli przez jego cyfrowy potencjał konkurencyjny. Innymi słowy jest to konkurencyjność atrybutowa (rezultatowa) możliwa do zrealizowania w przyszłości.

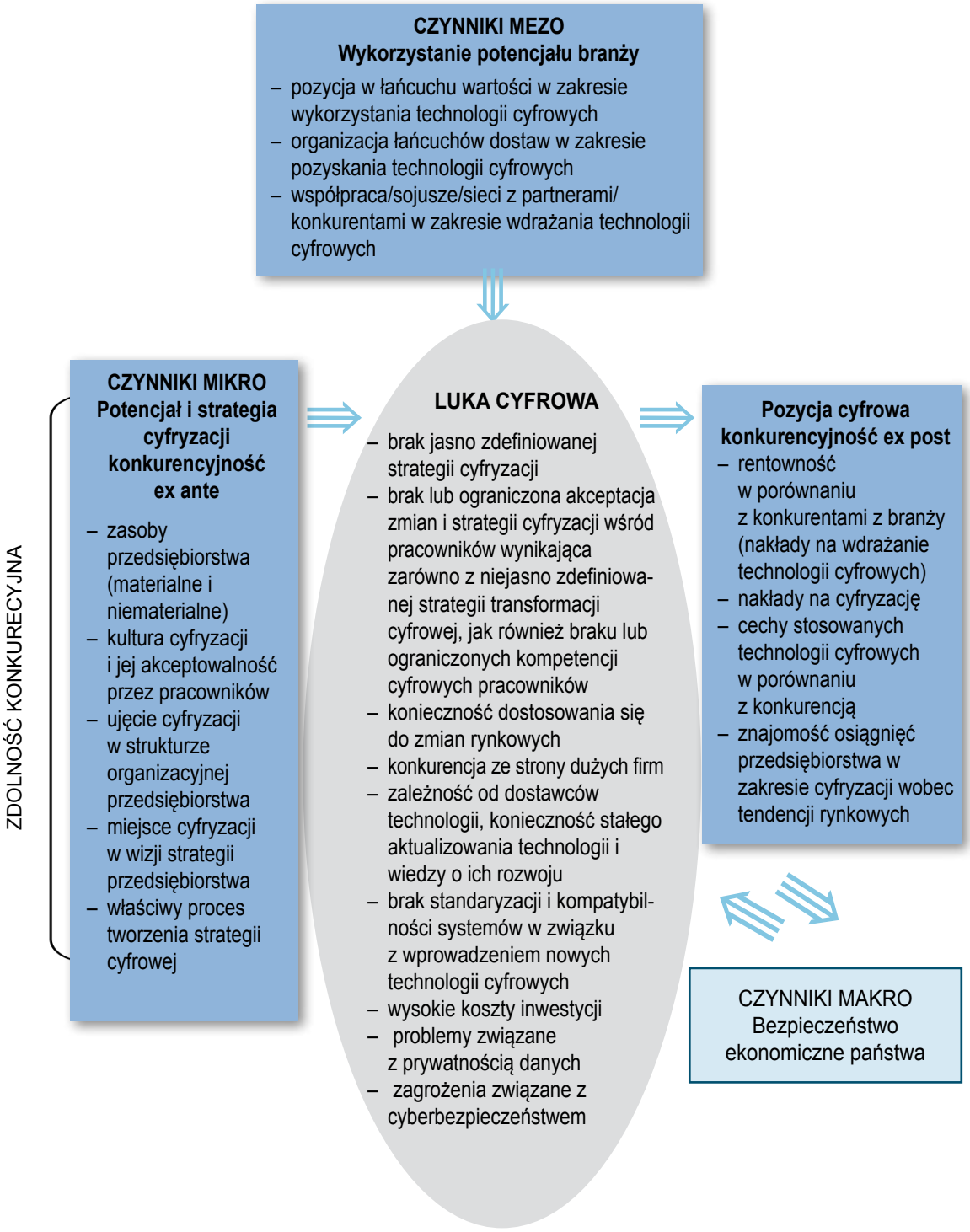
Proponowana strategia cyfrowa jest ogniwem pośrednim łączącym osiągniętą pozycję konkurencyjną w zakresie cyfryzacji z zamierzoną w przyszłości pozycją konkurencyjną, z wykorzystaniem potencjału konkurencyjnego w obszarze cyfryzacji. Budowę, a następnie wykorzystanie potencjału konkurencyjnego cyfryzacji opisuje planowana lub zamierzona strategia konkurencyjna w zakresie cyfryzacji. Strategia konkurencyjna obiektu uczestniczącego w procesie konkurowania w obszarze cyfryzacji jest więc kategorią analityczną umożliwiającą przejście od potencjału konkurencyjnego, czyli konkurencyjności potencjalnej (*ex ante*) do konkurencyjności rzeczywistej, czyli zrealizowanej (*ex post*). Strategie konkurowania są stosowane po to, aby konkurujący obiekt mógł zająć jak najlepszą pozycję konkurencyjną w zakresie cyfryzacji. Osiągnięcie pożądanej pozycji konkurencyjnej, czyli przewagi konkurencyjnej w sensie zajmowanej pozycji uwarun-

kowane jest posiadaniem przewagi konkurencyjnej w zakresie potencjału konkurencyjnego i/lub strategii konkurencyjnej odnoszących się do cyfryzacji. Innymi słowy posiadanie przewagi konkurencyjnej w zakresie potencjału i/lub strategii jest warunkiem koniecznym dla zajęcia dobrej pozycji konkurencyjnej. Różnica/przewaga/luka w zakresie pozycji konkurencyjnej jest efektem zastosowania zbioru instrumentów konkurowania w obrębie cyfryzacji, które są składnikami strategii konkurowania w obszarze digitalizacji. Zestaw instrumentów konkurowania składających się na strategię cyfryzacji może obejmować, takie składniki jak: kompatybilność rozwiązań w zakresie cyfryzacji z potrzebami dostawców i klientów oraz konsumentów, elastyczność dostosowywania w czasie rozwiązań cyfrowych do potrzeb odbiorców, podnoszenie poziomu nowoczesności wykorzystywanych technologii cyfrowych, zapewnienie potencjalnym kooperantom dobrego dostępu do wykorzystywanych rozwiązań cyfrowych (informacji itp.), szerokość asortymentu stosowanych narzędzi cyfryzacji dopasowana do potrzeb rynku, reklama i promocja kompetencji cyfrowych stosowanych przez przedsiębiorstwo, zakres świadczonych usług okołosprzedażnych (w tym szkoleniowych) w zakresie cyfryzacji oraz ceny tychże usług, warunki płatności za świadczone usługi cyfrowe, rozbudzanie nieznanych dotychczas potrzeb odbiorców (kreowanie potrzeb) w zakresie świadczonych usług cyfrowych.

Biorąc pod uwagę czynniki wpływające na wielkość potencjału cyfrowego przedsiębiorstwa zarówno wynikającego z zasobów wewnętrznych, jak i otoczenia konkurencyjnego możliwe jest określenie luki cyfrowej MŚP. Rozmiar i wymiary luki cyfrowej oraz zdolności przedsiębiorstw do jej „zasypania" determinują długoterminową, permanentną i trudną do skopiowania pozycję cyfrową MŚP (Rysunek 9).

Wymiary i rozmiar luki cyfrowej MŚP uzależnione są od potencjału cyfrowego (zarówno wewnętrznego, jak i wynikającego z zasobów otoczenia) i obejmują między innymi następujące czynniki:

1. Brak jasno zdefiniowanej strategii cyfryzacji przedsiębiorstwa;
2. Brak lub ograniczona akceptacja zmian i strategii cyfryzacji wśród pracowników wynikająca zarówno z niejasno zdefiniowanej strategii transformacji cyfrowej, jak również braku lub ograniczonych kompetencji cyfrowych pracowników;
3. Konieczność dostosowania się do zmian rynkowych;
4. Konkurencja ze strony dużych firm – np.: udział w łańcuchach dostaw;
5. Zależność od dostawców technologii, konieczność stałego aktualizowania technologii i wiedzy o ich rozwoju;
6. Brak lub ograniczona standaryzacja i kompatybilność systemów w związku z wprowadzeniem nowych technologii cyfrowych;
7. Wysokie koszty inwestycji – zakup oprogramowania i wdrażania technologii cyfrowych we wszystkich obszarach ADMA. Koszty wdrażania nowych technologii mogą być wyższe niż zakładano, co może być rezultatem braku integracji systemów;
8. Problemy związane z prywatnością danych;
9. Zagrożenia związane z cyberbezpieczeństwem.



Rysunek 9. Rozpoznanie luki cyfrowej MŚP

Źródło: opracowanie własne.

Powyższe założenia potwierdzają badania przeprowadzone w 2023 roku przez Ministerstwo Cyfryzacji wśród MŚP na temat gotowości wdrożenia, poziomu wiedzy i wykorzystania nowych technologii cyfrowych. Zgodnie z uzyskanymi rezultatami 56% badanych MŚP wskazuje na wysokie koszty inwestycji związanych z wdrażaniem technologii cyfrowych, 30% na brak wykwalifikowanej kadry i brak świadomości zysku/zwrotu

z zastosowania technologii cyfrowych. Aż 70% firm wskazało na brak szkoleń z zakresu cyfryzacji. W najbliższej przyszłości inwestycje w technologie cyfrowe podejmowane przez polskie MŚP obejmą zapewnienie dostępności rozwiązań cyfrowych w codziennych zadaniach zawodowych i zakupie podstawowego wyposażenia (np. komputery, kserokopiarki, skanery). Również stosowanie sztucznej inteligencji nie jest powszechnie wśród polskich MŚP. Wykorzystuje ją tylko 5,6% badanych. Więcej, bo 22,5% MŚP wdrożyło rozwiązania Internetu rzeczy. Najczęściej polskie MŚP wskazują na wykorzystywanie e-usług do komunikacji pomiędzy daną firmą a urzędami oraz firmą a jej klientami zewnętrznymi – 67% badanych [16].

W zakończeniu tego rozdziału warto zauważyć, że proponowane rozumienie luki cyfrowej ma charakter całościowy i wywodzi się z ugruntowanych koncepcji zarządzania strategicznego. Zastosowane podejście prowadzi do wniosku, że w rozpatrywaniu istoty luki cyfrowej nie należy ograniczać się do wąsko rozumianych uwarunkowań technologicznych. Są one ważne, ale nie są jedyne. Podobnie błędem byłoby ograniczenie rozważań wyłącznie do w zawężony sposób ujmowanego aspektu zasobowego. Ważnymi elementami kontekstu występowania luki cyfrowej rozpatrywanego przez pryzmat zasobów, jakimi dysponuje lub może dysponować przedsiębiorstwo są także kultura przedsiębiorstwa (kultura cyfryzacji), organizacja przedsiębiorstwa (lokalizacja zagadnień cyfryzacji w strukturze organizacyjnej), wizja przedsiębiorstwa (umiejscowienie zagadnień cyfryzacji w wizji firmy; w tym plany cyfryzacji) oraz sam sposób realizacji czy wdrażania strategii (np. rzeczywiste znaczenie przywiązywane do cyfryzacji przez kierownictwo).

4 Wpływ technologii cyfrowych na bezpieczeństwo ekonomiczne państwa

Już w tytule niniejszego raportu zasygnalizowano, że chodzi w nim nie tylko o identyfikację zagrożeń związanych z wprowadzaniem nowych technologii cyfrowych w przedsiębiorstwach, ale także o uwzględnienie perspektywy bezpieczeństwa państwa. Jest więc oczywiste, że konieczne jest jednoczesne uwzględnienie i pogodzenie dwóch punktów widzenia. Pierwszy to szczebel mikroekonomiczny, odnoszący się do poszczególnych indywidualnych jednostek gospodarczych, jakie stanowią przedsiębiorstwa stawia akcent na przetrwaniu i prosperowaniu w wymagającym otoczeniu konkurencyjnym dzięki umiejętnościom wykazywanym na polu rywalizacji rynkowej z konkurentami. Jak wiadomo jednak funkcjonowanie gospodarki narodowej, czyli de facto państwa w wymiarze gospodarczym nie jest prostą sumą działań zatomizowanych indywidualnych przedsiębiorstw, ale może tutaj wystąpić zarówno pozytywny efekt synergii, jak i negatywny efekt synergii, który zależy od tego, co dzieje się na poziomie wyższym, czyli na poziomie całej gospodarki. Państwo jest z kolei ważnym komponentem tego wyższego szczebla i dlatego problematyka jego bezpieczeństwa pojawia się jako istotny kontekst procesów konkurowania zachodzących na poziomie przedsiębiorstw i branż, które one konstytuują.

4.1. Podstawy bezpieczeństwa państwa i jego fundamentów gospodarczych

Bezpieczeństwo to obszerny i wielowymiarowy koncept, który odnosi się do ochrony przed różnymi zagrożeniami, ryzykiem i niebezpieczeństwami. Podstawowy dylemat pojęciowy przy definiowaniu bezpieczeństwa ma charakter bardziej semantyczny niż merytoryczny. Używa się takich pojęć jak „bezpieczeństwo państwa" lub „bezpieczeństwo narodowe". Terminy te często są używane zamiennie, ale mogą mieć nieco różne znaczenia w zależności od kontekstu i kraju. Dywagacje na ten temat znacznie przekroczyłyby ramy niniejszego opracowania. Dlatego przytoczono jedynie najważniejsze kwestie.

Ogólnie rzecz biorąc, różnica między nimi może być taka, że bezpieczeństwo państwa skupia się na bezpieczeństwie samego państwa jako instytucji oraz jego zdolności do sprawowania władzy i kontrolowania terytorium. Może to dotyczyć kwestii wewnętrznych, takich jak stabilność rządu, utrzymanie prawa i porządku, zwalczanie terroryzmu, zarządzanie kryzysami wewnętrznymi itp. Może również uwzględniać ochronę granic, terytorium oraz suwerenności państwa [30][6].

Natomiast bezpieczeństwo narodowe obejmuje szeroki zakres zagadnień, które wpływają na bezpieczeństwo całego narodu, w tym obywateli, instytucje państwowe,

6 W Konstytucji RP np. używa się ogólnego terminu bezpieczeństwo lub bezpieczeństwo państwa, Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.

gospodarkę i inne aspekty życia narodowego. Koncentruje się na ochronie interesów narodowych danego kraju w kontekście międzynarodowym. Dotyczy też relacji między państwami i dążenia do utrzymania lub zwiększenia wpływów, suwerenności i stabilności kraju na arenie międzynarodowej. Może uwzględniać aspekty takie jak polityka zagraniczna, obrona narodowa, dyplomacja, gospodarka, surowce energetyczne, itp.

W praktyce terminy te są często używane zamiennie, a ich znaczenie może się różnić w zależności od kontekstu i języka używanego w danym kraju. Ostatecznie oba te pojęcia odnoszą się do ochrony interesów i bezpieczeństwa państwa oraz jego obywateli, ale „bezpieczeństwo narodowe" może bardziej akcentować wymiar międzynarodowy, podczas gdy „bezpieczeństwo państwa" może bardziej koncentrować się na kwestiach wewnętrznych [31].

Dla celów niniejszego opracowania warto przytoczyć definicję bezpieczeństwa przemysłowego, gdyż takie m.in. bezpieczeństwo jest niezbędne do utrzymania stabilności fundamentów gospodarczych państwa. „*Bezpieczeństwo przemysłowe to wszelkie działania związane z zapewnieniem ochrony informacji niejawnych udostępnianych przedsiębiorcy w związku z realizacją umowy związanej z dostępem do informacji niejawnych lub zadań wynikających z przepisów prawa*". [32]

Fundamenty gospodarcze państwa stanowią podstawę dla funkcjonowania gospodarki narodowej, wpływają na stabilność i rozwój gospodarczy danego kraju i również mogą różnić się w zależności od kraju i jego specyficznych warunków. Można do nich zaliczyć m.in. politykę gospodarczą, infrastrukturę, kapitał ludzki i finansowy, rynek pracy, prawo i instytucje rządowe, innowacje i badania naukowe, rynek konsumencki, handel zagraniczny, zasoby naturalne. Fundamenty gospodarcze państwa tworzą podstawę dla jego zdolności do generowania dochodów, tworzenia miejsc pracy, rozwoju przedsiębiorczości i poprawy jakości życia obywateli. Nie trzeba nikogo przekonywać, że bezpieczeństwo państwa ma istotny wpływ na jego fundamenty gospodarcze, a te z kolei kształtują bezpieczne państwo. Również i w tym przypadku rozważaniom na powyższe tematy można by poświecić osobne opracowanie.

4.2. Definicje dotyczące bezpieczeństwa narodowego, w tym bezpieczeństwa cyfrowego

Bezpieczeństwo narodowe odnosi się do stanu ochrony i bezpieczeństwa państwa oraz jego obywateli przed różnymi zagrożeniami i ryzykami. Obejmuje szeroki zakres obszarów i dziedzin, z których najważniejsze to [33, 34, 35, 36]:

- suwerenność, a więc prawo do samodzielnego zarządzania przez państwo swoimi sprawami i niezależność od innych państw,
- obrona narodowa, czyli działania, siły i środki służące ochronie terytorium, granic i obywateli przed zagrożeniami militarnymi,
- bezpieczeństwo wewnętrzne polegające na utrzymaniu porządku i bezpieczeństwa wewnątrz państwa, walki z przestępczością, terroryzmem oraz innymi zagrożeniami dla spokoju publicznego,

- bezpieczeństwo ekonomiczne rozumiane jako ochrona gospodarki państwa przed zagrożeniami, takimi jak recesje, inflacja, bezrobocie i inne czynniki, które mogą wpływać na stabilność ekonomiczną,
- cyberbezpieczeństwo zapewniające ochronę przed atakami i zagrożeniami związanymi z cyberprzestępczością oraz bezpieczeństwem infrastruktury krytycznej,
- energia, która zapewnia dostęp do wystarczającej jej ilości, a także zabezpieczenie strategicznych źródeł i infrastruktury energetycznej,
- żywność i woda, czyli ochrona dostępu do żywności i czystej wody, a także zapewnienie bezpieczeństwa żywnościowego w przypadku kryzysów,
- bezpieczeństwo zdrowotne w tym, zapobieganie i zarządzanie zagrożeniami zdrowotnymi, takimi jak pandemie, epidemie i bioterroryzm,
- polityka zagraniczna i dyplomacja określające strategię i relacje państwa z innymi krajami oraz organizacjami międzynarodowymi w celu zapewnienia bezpieczeństwa narodowego, będące narzędziem do rozwiązywania konfliktów międzynarodowych, negocjowania umów i umacniania pozycji państwa na arenie międzynarodowej,
- wywiad i kontrwywiad, czyli działania wywiadu i kontrwywiadu mające na celu zbieranie informacji i rozpoznawanie zagrożeń dla państwa,
- zasoby ludzkie obejmujące zarządzanie personelem i zdolnością państwa do mobilizacji ludzi w sytuacjach kryzysowych,
- kultura narodowa i tożsamość, a więc ochrona i zachowanie dziedzictwa kulturowego oraz budowanie jedności narodowej.

Ten dość szeroki (ale zapewne niewyczerpany) wachlarz stanowi fundament bezpieczeństwa narodowego, ale istnieje wiele innych czynników i zagadnień, które mogą mieć wpływ na bezpieczeństwo państwa i jego obywateli. Strategia bezpieczeństwa narodowego jest dostosowywana do konkretnych wyzwań i sytuacji, z którymi państwo ma do czynienia [37].

W kontekście obszaru tematycznego opracowania, na szczególną uwagę zasługują te elementy bezpieczeństwa, które bezpośrednio lub pośrednio wiążą się z nowymi technologiami. Priorytetową kwestią jest tu bezpieczeństwo cyfrowe państwa, gdyż obecnie wiele aspektów funkcjonowania państwa i życia obywateli opiera się na technologii i systemach cyfrowych [38]. Cyfrowe podstawy bezpieczeństwa państwa i jego fundamentów gospodarczych są newralgiczne dla zachowania stabilności i rozwoju kraju w erze cyfrowej.

Do kluczowych pojęć z zakresu cyfrowego bezpieczeństwa państwa można zaliczyć:

- cyberbezpieczeństwo jako ogólny termin obejmujący wszystkie środki i działania mające na celu ochronę systemów komputerowych, sieci oraz danych przed atakami, zagrożeniami i incydentami cybernetycznymi,
- cyberataki**,** czyli próby nieautoryzowanego dostępu do systemów komputerowych lub sieci w celu zakłócenia ich działania, kradzieży danych lub szkodzenia infrastrukturze,

- incydenty cybernetyczne, w tym wszelkiego rodzaju zdarzenia, które mogą stanowić zagrożenie lub prowadzić do naruszenia bezpieczeństwa cyfrowego. Mogą to być ataki, awarie, włamania, wycieki danych, itp.,
- obrona cybernetyczna, a więc zbiór działań, procedur i technologii mających na celu zapobieganie, wykrywanie i odpieranie cyberataków,
- szkolenia i świadomość cyfrowa, które są ważnym elementem edukacji obywateli i pracowników w zakresie bezpieczeństwa cyfrowego, aby zminimalizować ryzyko ludzkiego błędu,
- plan zarządzania incydentami cybernetycznymi, które obejmują tworzenie przez państwo i różne instytucje i organy planów i procedur zarządzania incydentami, aby skutecznie reagować na ataki i awarie,
- regulacje prawne o cyberbezpieczeństwie, funkcjonujące w wielu krajach jako specjalne ustawy i przepisy regulujące dziedzinę cyberbezpieczeństwa oraz określające obowiązki i odpowiedzialność instytucji i przedsiębiorstw w tym zakresie [39][7],
- zarządzanie ryzykiem cyfrowym w ramach którego państwa, instytucje i przedsię-biorstwa muszą oceniać ryzyko związanego z cyberzagrożeniami i podejmować odpowiednie kroki w celu jego zminimalizowania lub zarządzania nim,
- narodowa infrastruktura krytyczna jako kluczowe sektory i systemy (np. energia, transport, opieka zdrowotna), których zakłócenie lub zniszczenie mogłoby mieć poważne konsekwencje dla państwa,
- współpraca międzynarodowa między państwami i organizacjami międzynarodowymi, gdyż zagrożenia te nie znają granic, a wymiana informacji o zagrożeniach, wspólne działanie przeciwko cyberprzestępczości oraz ustalenia standardów bezpieczeństwa jest szczególnie istotne.

Te pojęcia stanowią jedynie początek zrozumienia kompleksowej dziedziny cyfrowego bezpieczeństwa państwa. Bezpieczeństwo cybernetyczne jest stale rozwijającą się dziedziną, a państwa muszą być na bieżąco w dziedzinie strategii, technologii i praktyk, aby chronić swoje interesy i obywateli w erze cyfrowej.

Duże znaczenie ma tu prawidłowe funkcjonowanie przedsiębiorstw, które są podstawą funkcjonowania gospodarki. Aby się rozwijać, muszą one wprowadzać nowe technologie, które wpływają na tempo, dynamikę i skalę postępu, jednak niewłaściwie wdrożone mogą stanowić zagrożenie dla ich przyszłości, co z kolei przekłada się na ich bezpieczeństwo, a co za tym idzie, bezpieczeństwo ekonomiczne państwa.

7 Por. Ustawa o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. definiuje zadania i strukturę Krajowego Systemu Cyberbezpieczeństwa oraz określa, jakie podmioty są zobowiązane do raportowania incydentów związanych z cyberbezpieczeństwem (Dz. U. 2023.913 t.j.).

4.3. Wybrane zagrożenia dla przedsiębiorstw

Nowe technologie przynoszą wiele korzyści i możliwości [40], ale jednocześnie mogą stanowić potencjalne zagrożenia dla bezpieczeństwa państwa. Również dla MŚP nowe technologie stanowią zarówno szanse, jak i zagrożenia. Jakie zatem mogą być zagrożenia dla bezpieczeństwa państwa ze strony nowych technologii?

W nawiązaniu do zagrożeń dla MŚP w sferze cyfryzacji zidentyfikowanych w poprzednich punktach tego raportu, warto w tym miejscu dokonać enumeracji tych zagrożeń z przyjęciem jako dominującej perspektywy bezpieczeństwa państwa. Do głównych zagrożeń, z jakimi MŚP (i nie tylko one) mogą się spotkać w związku z nowymi technologiami, można zaliczyć m.in.:

- cyberzagrożenia, na które MŚP są często bardziej podatne niż duże korporacje, ponieważ mogą nie posiadać tak rozbudowanych systemów obronnych. Hakerzy i cyberprzestępcy mogą próbować włamać się do systemów MŚP, kradnąc dane, szantażować, czy nawet przerywać dostęp do usług [41][8],
- brak zasobów na zapewnienie cyberbezpieczeństwa w MŚP, gdyż często dysponują one ograniczonymi (w przeciwieństwie do dużych przedsiębiorstw) środkami na inwestycje w cyberbezpieczeństwo, co sprawia, że są bardziej narażone na ataki. Brak odpowiednich zabezpieczeń i edukacji pracowników może prowadzić do ryzyka utraty danych lub finansowych strat,
- naruszenie prywatności polegające na zbieraniu i przetwarzaniu danych klientów oraz pracowników za pomocą nowych technologii [42]. Firmy muszą przestrzegać przepisów o ochronie danych, w przeciwnym razie mogą grozić im kary i utrata zaufania klientów [43, 44, 45],
- automatyzacja procesów biznesowych (a w konsekwencji utrata miejsc pracy) za pomocą nowych technologii może prowadzić do zmniejszenia zapotrzebowania na pracowników, zwłaszcza w niektórych sektorach. To może mieć wpływ na zatrudnienie w MŚP,
- konkurencja online - rozwój Internetu i e-commerce może zwiększyć konkurencję dla MŚP. Konkurencja z firmami działającymi online może być wyjątkowo trudna, zwłaszcza jeśli MŚP szybko nie dostosują się do tych zmian,
- zmieniające się oczekiwania klientów wynikające z nowych technologii. Klienci mogą oczekiwać szybszych, bardziej efektywnych i bardziej dostosowanych do swoich potrzeb usług. MŚP muszą być elastyczne i gotowe do dostosowywania się do tych zmian,
- złożoność i koszty utrzymania technologii. Nowoczesne technologie, takie jak chmura obliczeniowa czy sztuczna inteligencja, mogą być skomplikowane i kosztowne w utrzymaniu. MŚP mogą mieć trudności z zarządzaniem i dostosowywaniem się do tych nowości, bo koszty ich utrzymania mogą przekroczyć ich potencjalne korzyści,

8 Por. DoD Dictionary of Military and Associated Terms, hasło: cyberspace attack, DoD, 2021, s. 55 (dostęp 09 września 2023).

- zależność od dostawców technologii, co może prowadzić do zwiększonego ryzyka, jeśli dostawcy doświadczą awarii lub incydentów bezpieczeństwa.

Również i ten katalog nie jest wyczerpany i będzie się on w dalszym ciągu rozwijał stosownie do rozwoju technologii.

Wśród wyżej wymienionych zagrożeń pominięto na przykład zamachy na infrastrukturę krytyczną. Oczywiście nowe technologie mogą uczynić infrastrukturę krytyczną, taką jak elektrownie, systemy wodociągowe, systemy transportowe i telekomunikacyjne [46] bardziej podatnymi na ataki. Awarie lub ataki na te systemy mogą mieć poważne skutki dla bezpieczeństwa państwa. Działalność MŚP może być również prowadzona w oparciu o infrastrukturę krytyczną.

Oprócz tego sztuczna inteligencja i jej rozwój może wprowadzić niebezpieczeństwo w przypadku utraty kontroli lub decyzji opartych jedynie na algorytmach. Niewątpliwie rosnąca zależność od zaawansowanych technologii może sprawić, że różne systemy i organizacje staną się bardziej podatne na awarie lub ataki na nie same i na różnorodne technologie.

Aby skutecznie zarządzać tymi zagrożeniami, MŚP powinny inwestować w odpowiednie zabezpieczenia cybernetyczne, przestrzegać różnorodnych przepisów, w tym o ochronie danych, monitorować zmiany na rynku i dostosowywać się do nich oraz doskonalić swoje umiejętności i wiedzę w zakresie nowych technologii.

4.4. Budowanie odporności przedsiębiorstw

Wdrażanie nowoczesnych technologii w MŚP to proces, który wymaga starannego planowania, ciągłego zarządzania i elastyczności w dostosowywaniu się do zmian [47]. To kluczowy krok w zapewnieniu konkurencyjności i efektywności działalności firmy. Konieczne jest zbudowanie swoistego sposobu postępowania – *modus operandi*, który uodporni MŚP przed negatywnym wpływem wprowadzania nowych technologii.

Eliminacja zagrożeń to trudne, ale niezbędne zadanie. Istotna będzie tu identyfikacja wiadomych i potencjalnych zagrożeń związanych z nowoczesnymi technologiami w firmie, a więc ustalenie, czy mogą to być awarie systemów, problemy z ochroną danych, czy inne ryzyka. Dlatego też dokładna ocena ryzyka związana z każdym zidentyfikowanym zagrożeniem winna określić, jakie mogą być konsekwencje każdego zagrożenia dla działalności i klientów. W tym celu konieczne może być opracowanie planu działań, konkretnych kroków do podjęcia mających na celu eliminację lub minimalizację zidentyfikowanych zagrożeń [48].

Konsekwentnie, celowe będzie wdrażanie środków zaradczych zgodnie z opracowanym planem działania, obejmujące instalowanie oprogramowania zabezpieczającego, konfigurowanie zapór (firewall), przeprowadzanie testów lub szkolenie pracowników [49]. Nieuniknione też jest regularne monitorowanie skuteczności podjętych działań i ocena czy ryzyko zostało zredukowane, co pozwoli zidentyfikować ewentualne luki w środkach zaradczych i dostosować strategię. Regularne przeglądy i aktualizacje środków zaradczych oraz planów działania jest ważne, gdyż technologie

i zagrożenia ewoluują. Temu samemu celowi służyć mogą szkolenia pracowników nie tylko w zakresie bezpieczeństwa cybernetycznego i postępowania w przypadku potencjalnych zagrożeń, ale wprowadzanych w danej formie innowacji i nowych technologii oraz konsekwencji z tego wynikających.

Wszystkie osoby (nie tylko funkcyjne) winny wiedzieć, jak się zachować w przypadku incydentu, a więc opracowanie planu zarządzania incydentami, który będzie zawierać procedury reagowania na sytuacje awaryjne będzie priorytetowe, a także raportowanie wszelkich podejrzanych aktywności. Można też, w razie potrzeby, skorzystać z usług ekspertów w dziedzinie bezpieczeństwa cybernetycznego lub technologii, którzy pomogą w identyfikacji i eliminacji zagrożeń, ale też zapewnią wsparcie i doradztwo w tych kwestiach.

Opracowanie strategii działań prewencyjnych, które pomogą unikać potencjalnych zagrożeń związanych z nowoczesnymi technologiami musi być systematyczne i świadome, aby chronić działalność firmy i jej interesy. Ważne, aby unikać rutyny, która może okazać się zgubna w skutkach.

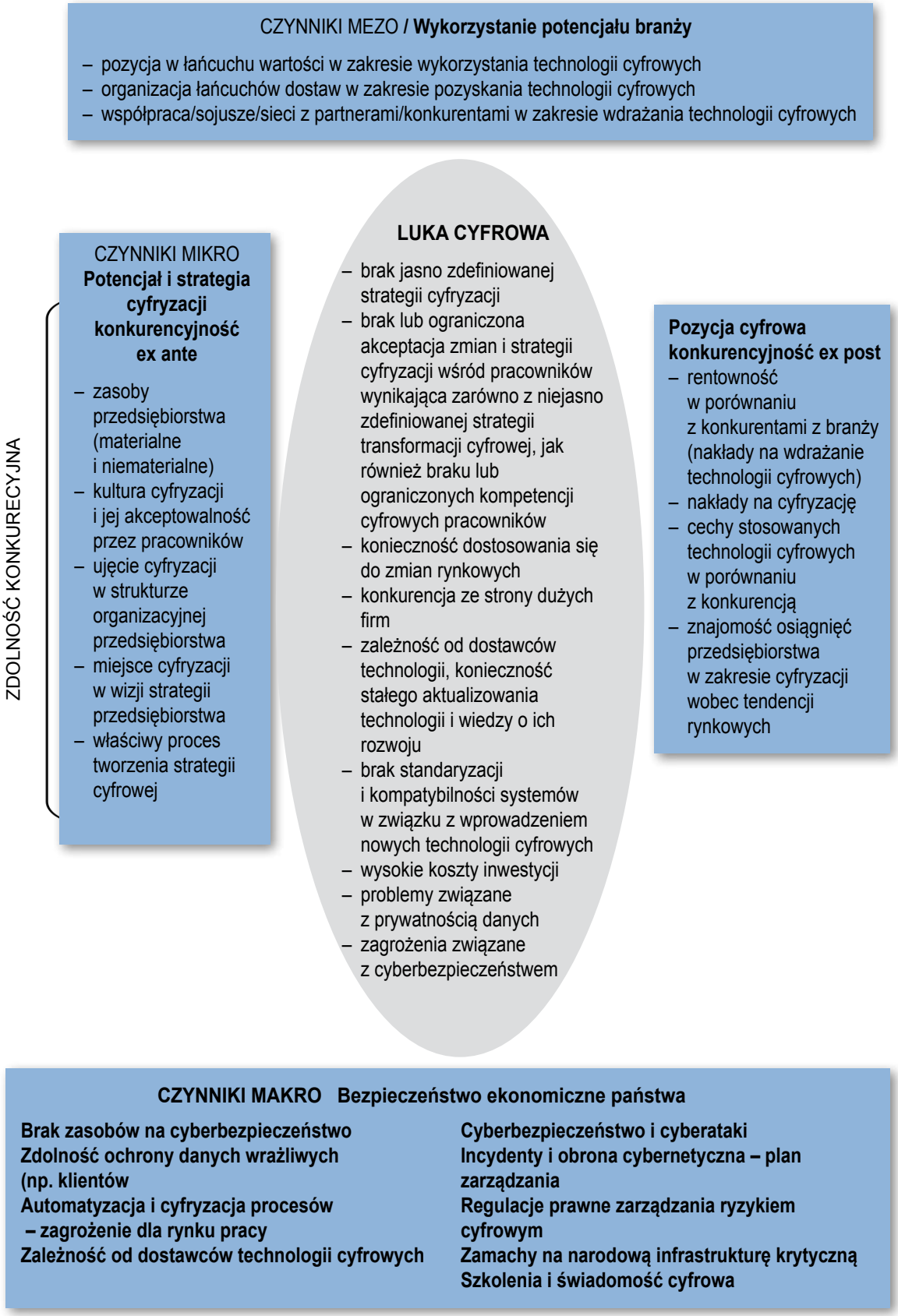
Dlatego budowanie odporności małych i średnich przedsiębiorstw (MŚP) na zagrożenia związane z wprowadzaniem nowoczesnych technologii jest tak istotne w dzisiejszym dynamicznym i cyfrowym środowisku biznesowym.

Aby udaremnić przyszłą złośliwą aktywność wynikającą z nowych technologii należy wdrożyć architekturę Zero Trust (zero zaufania) i powiązane z nimi technologie cyberbezpieczeństwa, a także zmodernizować algorytmy postępowania, zabezpieczenia w systemach, łączach danych i sieciach [50].

Dokładanie wszelkich starań w kierunku zniwelowania zagrożenia ze strony zagrożeń związanych z utrzymaniem bezpieczeństwa narodowego w konsekwencji wdrażania technologii cyfrowych w skali globalnej jest ważnym działaniem wpływającym na rozmiar luki cyfrowej MŚP. Jednocześnie rozmiar i różne wymiary luki cyfrowej MŚP oddziaływają na utrzymanie bezpieczeństwa cyfrowego i gospodarczego na poziomie kraju (Rysunek 9).

Budowanie odporności przedsiębiorstw i eliminacja zagrożeń związanych z nowoczesnymi technologiami w MŚP to proces długotrwały (nieprzerwany), wielokierunkowy, a więc w naturalny sposób skomplikowany, jednakże konieczny i wymagający stałej uwagi.

Zdecydowanie warto budować odporność na możliwe obecne i przyszłe, nieznane zagrożenia, zaczynając od najniższego segmentu gospodarki. Aby zapewnić bezpieczeństwo przedsiębiorstw, konieczne jest ciągłe monitorowanie i dostosowywanie działań do zmieniającego się krajobrazu technologicznego oraz inwestowanie w środki ochrony i cyberbezpieczeństwo. Współpraca między przedsiębiorstwami, oczywiście na tyle, na ile pozwala konkurencja rynkowa, jest w tym zakresie koniecznością.



Rysunek 10. Związek pomiędzy luką cyfrową na poziomie przedsiębiorstwa a bezpieczeństwem ekonomicznym państwa

Źródło: opracowanie własne.

5 Wiodące ośrodki naukowe zajmujące się badaniem technologii cyfrowych

Ośrodki badawcze zajmujące się technologiami cyfrowymi istotnymi dla MŚP odgrywają kluczową rolę w rozwoju i wsparciu tych przedsiębiorstw. Prowadzą badania nad nowymi technologiami cyfrowymi, które pozwalają małym podmiotom budować przewagi konkurencyjne i utrzymać permanentną pozycję konkurencyjną. Umożliwiają łatwiejsze dostosowanie się MŚP do zmieniających się trendów technologicznych, biorą udział w monitorowaniu trendów rynkowych i dostarczają MŚP informacji na temat tego, jakie technologie i rozwiązania są dla nich istotne.

Ponadto wspierają przedsiębiorstwa w procesie innowacji identyfikując nowe możliwości wykorzystania technologii cyfrowych w procesach biznesowych. Oferują nierzadko profesjonalne doradztwo techniczne w celu doboru odpowiednich rozwiązań dostosowanych do potrzeb danego podmiotu. Rozwiązują również problemy związane z technologią cyfrową, testowaniem prototypów i formułowaniem koncepcji przed wdrożeniem ich na szeroką skalę.

Niewątpliwie do jednych z najważniejszych zadań ośrodków badania technologii cyfrowych zaliczyć należy pomoc w uzyskaniu zewnętrznego dofinansowania projektów związanych z technologią cyfrową oraz organizacji szkoleń i warsztatów pozwalających na podniesienie kompetencji cyfrowych pracowników. Daje to ewidentne szanse na zmniejszenie luki cyfrowej polskich MŚP. Ośrodki spełniają również funkcję platformy kontaktów i sieciowania MŚP z inwestorami, ekspertami i instytucjami publicznymi, co może stanowić również wsparcie w dostępie do rynków międzynarodowych.

Istnieje wiele międzynarodowych i krajowych ośrodków badawczych zajmujących się badaniami nad technologiami cyfrowymi istotnymi dla MŚP. Wiodące ośrodki międzynarodowe przedstawiono w tabeli 3.

Wyraźnie dominują wśród nich ośrodki uniwersyteckie i ośrodki wspierane przez instytucje publiczne.

Tabela 3. Wiodące międzynarodowe ośrodki badawcze zajmujące się badaniami nad technologiami cyfrowymi istotnymi dla MŚP

Międzynarodowe ośrodki badawcze	Kluczowe raporty i publikacje dotyczące cyfryzacji
1	2
MIT Initiative on the Digital Economy (IDE) MIT Sloan School of Management Massachusetts Institute of Technology	**2022 MIT IDE Annual Report** https://www.yumpu.com/en/document/view/67549920/2022-mit-ide-annual-report
Center for Information Systems Research (CISR) MIT Sloan School of Management Massachusetts Institute of Technology	Szeroka gama publikacji naukowych i raportów: https://cisr.mit.edu/research-library
Oxford Internet Institute (OII) University of Oxford	Raporty, rozdziały w monografiach, raporty, artykuły: https://www.oii.ox.ac.uk/research/publications/#symplectic-report
Harvard Business School's Digital Initiative Digital Data Design Institute	HBS Digital Transformation Task Force Report https://www.alumni.hbs.edu/Documents/bulletin/HBS-Digital-Transformation-Task-Force-Report.pdf
Digital Europe Komisja Europejska plus **Enterprise Europe Network**	Komisja Europejska, 2020, Kształtowanie cyfrowej przyszłości Europy. COM(2020) 67 final. Bruksela. Komisja Europejska (2021), Cyfrowy kompas na 2030: europejska droga w cyfrowej dekadzie, COM (2021) 118 final, Bruksela. Komisja Europejska (2023), 2030 Digital Decade, Report on the state of the Digital Decade 2023, https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade
The European Digital SME Alliance największa sieć MŚP z sektora ICB w Europie, reprezentująca łącznie ponad 45 000 przedsiębiorstw. Sojusz jest wspólnym wysiłkiem 30 krajowych i regionalnych stowarzyszeń MŚP z państw członkowskich UE i krajów sąsiednich	Lista publikacji i raportów: https://www.digitalsme.eu/policy/
The Copenhagen Institute for Future Studies (CIFS)	Scenario Reports FARSIGHT https://cifs.dk/shop/
Cambridge Digital Innovation (CDI) **University of Cambridge**	Lista publikacji i raportów: https://www.cambridgedigitalinnovation.org/publications
UW Interactive Data Lab University of Washington projektowanie nowych interaktywnych systemów do wizualizacji i analizy danych	Lista publikacji: https://idl.cs.washington.edu/
Digital Switzerland inicjatywa promująca cyfryzację w Szwajcarii	Annual Report https://digitalswitzerland.com/annual-report-2022/

1	2
Technion – Izrael Institute of Technology	Raporty i projekty badawcze https://www.technion.ac.il/wp-content/uploads/2014/07/INDUSTRY-GUIDE-TO-TECHNION_L.pdf
Silicon Roundabout Londyński HUB technologiczny	Raporty https://www.ft.com/silicon-roundabout
Karlsruhe Institute of Technology	https://www.kit.edu/english/index.php
Berlin Center for Digital Transformation Fraunhofer Institutes	Projekty i raporty https://www.digitale-vernetzung.org/de/projekte.html
National IT Industry Promotion Agency Korea Południowa	https://www.nipa.kr/eng/index
IBM Research jeden z największych ośrodków badawczych na świecie w zakresie badań nad sztuczną inteligencją, komputacją kwantową i innymi technologiami cyfrowymi	https://research.ibm.com/publications
Google Research prowadzi badania w dziedzinie analizy danych, uczenia maszynowego i innych technologii cyfrowych	Lista publikacji i raportów: https://research.google/pubs/
IBM Quantum Network	Raport “The Quantum Decade. A playbook for achieving awareness,readiness, and advantage. Third edition” https://www. ibm.com/thought-leadership/institute-business-value/report/quantum-decade
Uniwersytet Techniczny w Monachium (TUM) Munich Quantum Valley	https://www.munich-quantum-valley.de/
Gartner trendy w rozwoju kluczowych strategicznych technologii w tym technologii cyfrowych prezentuje firma doradcza	Raport “Top 10 Strategic Technology Trends for 2023” (https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2023)
McKinsey	Raport “McKinsey Technology Trends Outlook 2023” (https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#new-and-notable)
TEKsystems	Raport “State Of Digital Transformation. Optimizing the Journey Forward” (https://www.teksystems.com/en/insights/state-of-digital-transformation-2023)

Źródło: opracowanie własne.

Wiodące krajowe ośrodki badawcze zajmujące się badaniami nad technologiami cyfrowymi istotnymi dla MŚP zaprezentowano natomiast w tabeli 4.

Tabela 4. Wiodące krajowe ośrodki badawcze zajmujące się badaniami nad technologiami cyfrowymi istotnymi dla firm sektora MŚP

Krajowe ośrodki badawcze	Kluczowe raporty dotyczące cyfryzacji
1	2
Grupy robocze Ministerstwa Cyfryzacji: – ds. Sztucznej Inteligencji (GRAI) – ds. strategicznych kierunków zarządzania danymi (grupaZD) – ds. rejestrów rozproszonych i blockchain – ds. Internetu Rzeczy – ds. Ochrony Danych Osobowych – ds. Cyberbezpieczeństwa	Raporty: „Cyfryzacja polskich przedsiębiorstw" „W drodze ku doskonałości cyfrowej. Raport końcowy z badania rynku na temat gotowości wdrożenia, poziomu wiedzy i wykorzystania nowych technologii cyfrowych w Małych i Średnich Przedsiębiorstwach" „Internet Rzeczy - Polska Przyszłości" „Wdrażanie technologii w samorządach"
Polska Agencja Rozwoju Przedsiębiorczości Grupa PFR	– Raport „Monitoring innowacyjności polskich przedsiębiorstw. Wskaźnik dojrzałości innowacyjnej" – Raport „Monitoring innowacyjności polskich przedsiębiorstw - Kluczowe wnioski" https://www.parp.gov.pl/component/site/site/monitoring-innowacyjnosci-polskich-przedsiebiorstw – Raport „Jak zwiększyć poziom cyfryzacji w firmie? Poradnik dla MŚP" https://poir.parp.gov.pl/publikacje/publication/jak-zwiekszyc-poziom-cyfryzacji-w-firmie-poradnik-dla-msp
Główny Urząd Statystyczny	Digital Economy and Society Index (DESI) (https://digital-strategy.ec.europa.eu/pl/policies/desi) GUS – społeczeństwo informacyjne
Fundacja Platforma Przemysłu Przyszłości	Raporty: „Przegląd międzynarodowy metodyk benchmarkingu klastrów w zakresie cyfryzacji" „Poradnik dotyczący cyfryzacji łańcuchów wartości w klastrach" „Modele cyfryzacji łańcucha wartości w klastrach" Cyfryzacja: https://przemyslprzyszlosci.gov.pl/tag/cyfryzacja/page/2/
Fundacja Digital Poland	Raporty: „Technologia w służbie społeczeństwu. Czy Polacy zostaną społeczeństwem 5.0? Edycja 2023" „Czas na cyfrową gospodarkę!" https://digitalpoland.org/publikacje
Deloitte	Raport „Trendy Technologiczne 2023"
SpotData platforma wizualizacji i analizy danych ekonomicznych	Raport „Cyfryzacja to więcej niż technologia. Jak polskie firmy zaczynają nadrabiać zaległości w cyfryzacji i jaką rolę odgrywają w tym procesie fundusze private equity"
KPMG	Raport „Monitor Transformacji Cyfrowej Biznesu"

1	2
NASK	Raporty: „E-transformacja i bezpieczeństwo cyfrowe w polskich przedsiębiorstwach” „Krajobraz bezpieczeństwa polskiego Internetu. Roczny raport z działalności CERT 2022”
IDEAS NCBR ośrodek badawczo-rozwojowy działający w obszarze sztucznej inteligencji	https://ideas-ncbr.pl/en/institutions-and-researchers/research-and-groups/

Źródło: opracowanie własne.

Ponadto w Polsce funkcjonuje wiele instytucji, konsorcjów i sieci, które prowadzą badania związane z wdrażaniem technologii cyfrowych szczególnie ważnych dla MŚP:

1. Europejskie Huby Innowacji Cyfrowych (EDIH)– ich główną misją jest budowanie potencjału cyfrowego MŚP i organizacji sektora publicznego w całej Unii Europejskiej. Aby przyspieszyć transformację cyfrową, sieć EDIH koncentruje się na budowaniu potencjału i wykorzystywaniu najnowocześniejszych technologii w kluczowych sektorach [51]:
   - WAMA EDIH – WaMa Innovation Hub (Warmia-Mazury – HUB innowacyjny),
   - h4i – hub4industry Kraków,
   - WRO4digITal European Digital Innovation Hub Wroclaw,
   - (CyberSec) National Centre of Secure Digital Transformation (Instytut Chemii Bioorganicznej PAN Poznańskie Centrum Superkomputerowo-Sieciowe),
   - Pomeranian Digital Innovation Hub,
   - European Digital Innovation Hub of Mazovia,
   - The Regional Digital Innovation Hub Silesia Smart Systems (EDIH-SILESIA),
   - Technopark Kielce DIH (TKDIH),
   - FinTech Copernicus Hub (FTCH) (Uniwersytet Mikołaja Kopernika – Toruń),
   - HPC4Poland European Digital Innovation Hub, Poznań, Szczecin, Zielona Góra,
   - re_d: rethink digital – Central Poland Digitalisation Hub, Łódź,
   - LUBDIGHUB, Lublin,
   - The Smart Secure Cities – Creating Smart Secure Cities for EU citizens, Warszawa,
   - European Digital Innovation Hub for North - Central Poland – 1, Toruń.

2. Polska Akademia Nauk, uniwersytety i uniwersytety techniczne – jest to jedna z liczniejszych grup ośrodków prowadzących kluczowe badania technologii cyfrowych kluczowych dla MŚP. Przykładowe ośrodki to:
   - Laboratorium Rzeczywistości Wirtualnej i Psychofizjologii PAN (https://psych.pan.pl/struktura/laboratoria/laboratorium-rzeczywistosci-wirtualnej-i-psychofizjologii/)

- Instytut Informatyki Teoretycznej i Stosowanej PAN (https://www.iitis.pl/pl),
- Instytut Podstaw Informatyki PAN (https://ipipan.waw.pl/),
- Centrum Inteligentnych Technologii Wydział Zarządzania Uniwersytet Łódzki (https://www.wz.uni.lodz.pl/centrum-inteligentnych-technologii),
- Wydział Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej,
- Wydział Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego,
- Wydział Informatyki i Zarządzania Politechniki Wrocławskiej,
- Wydział Informatyki Uniwersytetu Jagiellońskiego,
- Wydział Informatyki i Telekomunikacji Politechniki Poznańskiej,

3. Parki technologiczne i inkubatory – zlokalizowane są w różnych miastach w Polsce, promują na szeroką skalę innowacje i badania w dziedzinie technologii cyfrowych, przykładowe ośrodki to:
   - Warsaw Spire,
   - Gdański Park Naukowo-Technologiczny,
   - Pomorski Park Naukowo-Technologiczny (Gdynia),
   - Krakowski Park Technologiczny,
   - Poznański Park Naukowo-Technologiczny,
   - Wrocławski Park Naukowo-Technologiczny.

4. Przemysłowe ośrodki badawcze – skupiają badania podejmowane przez przedsiębiorstwa i instytucje badawcze z sektora prywatnego. Prowadzą badania w zakresie technologii cyfrowych w obszarach oprogramowanie, elektronika, telekomunikacja i automatyka. W licznej grupie tychże ośrodków przykładami mogą być:
   - Nokia Solutions and Networks – technologie telekomunikacyjne, w tym sieci 5G, Internetu rzeczy (IoT) (https://www.nokia.com/networks/),
   - ABB Corporate Research Center Poland - rozwijanie technologii związanych z au-tomatyzacją, robotyką, systemami sterowania i energetyką (https://global.abb/group/en/technology/corporate-research-centers/poland),
   - Samsung R&D Institute Poland – oprogramowanie, technologia mobilna, Internet rzeczy (IoT) i innowacje w dziedzinie urządzeń elektronicznych (https://samsungrd. pl/obszary-kompetencji).

5. Konsorcja i inicjatywy badawcze – angażują podmioty w międzynarodowe projekty badawcze związane z technologiami cyfrowymi. Wśród licznych powiązań przykładami mogą być następujące porozumienia:
   - Level 4.0 – konsorcjum we Wrocławiu zrzeszające firmy, specjalistów i naukowców promocja idei Przemysłu 4.0. tj: algorytmy uczące się, chmura obliczeniowa, cyberbezpieczeństwo, Internet rzeczy, automatyka i robotyka, wirtualna i rozszerzona rzeczywistość (https://www.level4dih.pl/),

- Polski klaster AI o IoT Sinotaic – badania i rozwijanie technologii związanych ze sztuczną inteligencją i Internetem Rzeczy, w tym urządzeniami inteligentnymi, komunikacją maszynową i analizą danych (https://sinotaic.com/o-klastrze/),
- Polska Chmura – związek polskich dostawców usług chmurowych (https://polska--chmura.pl/),
- Polskie Stowarzyszenie Blockchain - wspiera wymianę wiedzy i doświadczeń w obszarze technologii blockchain, zrzesza ekspertów blockchain oraz osoby zainteresowane tą technologią, reprezentujące różne środowiska (IT, prawnicze, marketingowe, sprzedażowe) (https://blockchain-polska.org/),
- Data Science PL – platforma skupiająca wszystkich zainteresowanych analizą dużych zbiorów danych (Big Data) i ich wizualizacją (elementy Business Intelligence). Liderem jest Politechnika Wrocławska (https://www.facebook.com/groups/datasciencepl).

Ośrodki badawcze technologii cyfrowych prowadząc badania i jednocześnie wspierając transformację cyfrową MŚP posługują się różnorodnymi metodykami i narzędziami charakterystycznymi dla tego typu działalności. Ze względu na badania związane z technologiami cyfrowymi dominują analizy danych oraz dużych zbiorów danych (Big Data), które ułatwiają zrozumienie trendów związanych z wdrażaniem technologii cyfrowych. Przykładowe ośrodki polskie i międzynarodowe to: Data Science PL, MIT Initiative on the Digital Economy (IDE), TUM Uniwersytet w Monachium, IBM Quantum Network, IBM Research, Google Research czy UW Interactive Data Lab.

Często przeprowadzane są również badania ankietowe i wywiady, które pozwalają na monitorowanie potrzeb, wyzwań, korzyści i zagrożeń związanych z wdrażaniem technologii cyfrowych. Opracowywane są również studia przypadków, które na podstawie doświadczeń innych podmiotów ułatwiają zaplanowanie i wdrożenie rozwiązań cyfrowych w przedsiębiorstwie. Wykorzystywane są także badania eksperymentalne pozwalająca na testowanie nowych rozwiązań technologicznych oraz pomiar ich wpływu na MŚP. Takie narzędzia i metody są powszechnie aplikowane przez wiodące ośrodki krajowe i międzynarodowe, do których można zaliczyć: NASK, Eurostat, PARP, Ministerstwo Cyfryzacji, SpotData, Deloitte, KPMG, McKinsey, TEKsystems czy MIT Sloan School of Management.

Kluczowe miejsce wśród narzędzi i metod badawczych zajmują metody popularne w zarządzaniu strategicznym tj. mapy myśli – pozwalające na wizualizację koncepcji i zależności między różnymi aspektami technologii cyfrowych (UW Interactive Data Lab), metody badania rynku (np.: analiza trendu, punktowa ocena atrakcyjności sektora) (FPPP, PARP, Ministerstwo Cyfryzacji, Eurostat, Deloitte, Digital Switzerland, The Copenhagen Institute for Future Studies (CIFS), MIT Initiative on the Digital Economy (IDE)), metoda benchmarkingu pozwalająca na wyłonienie najlepszych praktyk (FPPP, PARP, Deloitte) czy analiza SWOT pozwalająca na ocenę pozycji konkurencyjnej MŚP w procesie transformacji cyfrowej (Digital Europe, Sinotaic).

Istotne jest również modelowanie matematyczne, statystyczne i ekonometryczne. Pozwala bowiem na przewidywanie skutków oraz modelowanie predykcyjne. Wykorzystywane jest przez wszystkie wiodące ośrodki uniwersyteckie i naukowo-badawcze zarówno w Polsce, jak i świecie.

Warto również podkreślić, iż jednoznaczne przypisanie danej metodyki do danego ośrodka badawczego technologii cyfrowych jest praktycznie niemożliwe. W szerokim spektrum oferowanych przez nie opracowań i studiów aplikowane są różne narzędzia i metody wskazane powyżej. Wszystkie wymienione powyżej, jak również szereg innych narzędzi i metod badawczych znajduje zastosowanie w szerokich opracowaniach naukowych oraz badaniach wiodących uniwersytetów i innych jednostek badawczo-naukowych.

Zakończenie

W warunkach silnej labilności otoczenia biznesowego, transformacja cyfrowa MŚP jest wielką szansą mogącą prowadzić do zwiększenia wydajności, produktywności i efektywności ich działań, a tym samym przyczynić się do uzyskania trwałej pozycji konkurencyjnej. Z drugiej jednak strony wiąże się również z ryzykiem utraty przewagi konkurencyjnej na skutek niewłaściwego wykorzystania potencjału konkurencyjnego oraz potencjału wynikającego z przewag otoczenia biznesowego. Wykorzystując koncepcję konkurencyjności przedsiębiorstwa można analogicznie odnieść ją do transformacji cyfrowej i określić jej trzy wymiary: potencjał cyfryzacji (jako ekwiwalent potencjału konkurencyjnego), pozycja w procesie cyfryzacji (jak odpowiednik pozycji konkurencyjnej) oraz instrumenty cyfryzacji (jako odpowiednik instrumentów konkurowania), składające się na strategię cyfryzacji, czyli wykorzystania technologii cyfrowych w MŚP. Określenie wymiaru i rozmiaru luki cyfrowej pozwoliło autorom na zidentyfikowanie potencjalnych działań zmierzających do jej „zasypania". Warto w tym miejscu podkreślić, iż negatywne skutki cyfryzacji w MŚP wynikające w głównej mierze z powodu nieprawidłowo sformułowanej strategii cyfryzacji oraz braku wykwalifikowanych pracowników mogą być potęgowane przez wiele innych czynników m.in. brak standaryzacji i kompatybilności systemów, co prowadzi do wyższych kosztów inwestycji. Dodatkowo, konieczność dostosowania się do zmian rynkowych i konkurencja ze strony dużych firm stawiają przed MŚP dodatkowe wyzwania.

Jak wiadomo funkcjonowanie gospodarki narodowej, czyli de facto państwa w wymiarze gospodarczym nie jest prostą sumą działań indywidualnych przedsiębiorstw. Może tu wystąpić zarówno pozytywny jak i negatywny efekt synergii, który zależy od tego, co dzieje się na poziomie wyższym (w otoczeniu dalszym), czyli na poziomie całej gospodarki. Państwo jest ważnym komponentem tego wyższego poziomu, stąd problematyka jego bezpieczeństwa pojawia się jako istotny kontekst procesów konkurowania zachodzących na poziomie przedsiębiorstw i branż. Państwo odgrywa kluczową rolę w zarządzaniu zagrożeniami związanymi z cyberbezpieczeństwem i ochroną infrastruktury krytycznej. Regulacje prawne, szkolenia, podnoszenie świadomości cyfrowej oraz monitorowanie zagrożeń dla rynku pracy stają się kluczowymi elementami strategii państwa w obliczu automatyzacji i cyfryzacji procesów.

Nawiązując do powyższych spostrzeżeń, niezbędne jest opracowanie kompleksowych strategii zarządzania ryzykiem cyfrowym, wspieranie przedsiębiorstw w procesie cyfryzacji, a także ciągłe doskonalenie środków ochrony przed zagrożeniami cyfrowymi. Tylko w ten sposób możliwe będzie skorzystanie z potencjału rozwojowego, jaki niesie ze sobą cyfryzacja, jednocześnie minimalizując ryzyko negatywnych konsekwencji dla bezpieczeństwa państwa i konkurencyjności MŚP.

Bibliografia

[1] „Nowa strategia przemysłowa dla Europy," Komisja Europejska, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020DC0102&qid=1700319417191. [Data uzyskania dostępu: 18 Listopad 2023].

[2] „Strategia MŚP na rzecz zrównoważonej i cyfrowej Europy," Komisja Europejska, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020DC0103&qid=1700319534947. [Data uzyskania dostępu: 18 Listopad 2023].

[3] „Kształtowanie cyfrowej przyszłości Europy," Komisja Europejska, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020DC0067&qid=1700320178383. [Data uzyskania dostępu: 18 Listopad 2023].

[4] J. Kuczewska i J. Stefaniak, „Ewolucja jednolitego rynku wewnętrznego Unii Europejskiej - realizacja i nowe wyzwania," *Przegląd Zachodni,* tom 3, nr 380, pp. 161-176, 2021.

[5] „Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie," Komisja Europejska, 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021DC0118&qid=1700318511296. [Data uzyskania dostępu: 18 Listopad 2023].

[6] „Sprawozdanie na temat stanu cyfrowej dekady za 2023 r.," Komisja Europejska, 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/pl/library/2023-report-state-digital-decade. [Data uzyskania dostępu: 18 Listopad 2023].

[7] „Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY ustanawiające Platformę na rzecz technologii strategicznych dla Europy („STEP")," Komisja Europejska, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52023PC0335&qid=1700318852783. [Data uzyskania dostępu: 18 Listopad 2023].

[8] „Gartner Top 10 Strategic Technology Trends for 2023," Gartner, 2023. [Online]. Available: https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2023. [Data uzyskania dostępu: 18 Listopad 2023].

[9] „McKinsey Technology Trends Outlook 2023," McKinsey, 2023. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech. [Data uzyskania dostępu: 18 Listopad 2023].

[10] „Delloite Tech Trends 2023," 2023. [Online]. Available: https://www2.deloitte.com/content/dam/insights/articles/us175897_tech-trends-2023/DI_tech-trends-2023.pdf. [Data uzyskania dostępu: 18 Listopad 2023].

[11] K. Śledziewska i R. Włoch, Gospodarka cyfrowa. Jak nowe technologie zmieniają świat, Warszawa: Wydawnictwa Uniwersytetu Warszawskiego, 2020, p. 342.

[12] S. Quach, P. Thaichon, K. D. Martin, S. Weaven i R. W. Palmatler, „Digital technologies: tensions in privacy and data," tom 50, nr https://doi.org/10.1007/s11747-022-00845-y, pp. 1299-1323, 2022.

[13] M. Wynn i P. Jones, „Digital Technology Deployment and the Circular Economy," *Sustainability,* tom 14, nr https://doi.org/10.3390/su14159077, 2022.

[14] C. Chauhan, V. Parida i A. Dhir, „Linking circular economy and digitalisation technologies: A systematic literature review of past achievements and future promises," *Technological Forecasting and Social Change,* tom 177, nr https://doi.org/10.1016/j.techfore.2022.121508, 2022.

[15] D. Paschek, A. Mocan i A. Draghici, „Industry 5.0 – The Expected Impact Of Next Industrial Revolution," w *Thriving on Future Education, Industry, Business and Society; Proceedings of the MakeLearn and TIIM International Conference 2019*, 2019.

[16] „W drodze ku doskonałości cyfrowej Raport końcowy z badania rynku na temat gotowości wdrożenia, poziomu wiedzy i wykorzystania nowych technologii cyfrowych w Małych i Średnich Przedsiębiorstwach," Ministerstwo Cyfryzacji, 2023. [Online]. Available: https://www.gov.pl/attachment/4248f56b-7091-4096-83bc-b7abca1c36cf. [Data uzyskania dostępu: 18 Listopad 2023].

[17] „Decyzja nr 3/2022 Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji ws. utworzenia Zespołu zadaniowego do spraw technologii przełomowych," Ministerstwo Cyfryzacji, 2022. [Online]. Available: https://www.gov.pl/attachment/da2b797b-c58a-411a-92e2-9a6f838ddd45. [Data uzyskania dostępu: 18 Listopad 2023].

[18] M. Gorynia, Red., Luka konkurencyjna na poziomie przedsiębiorstwa a przystąpienie Polski do Unii Europejskiej, Wydawnictwo Akademii Ekonomicznej w Poznaniu, 2002.

[19] „The ADMA Methodology: a guide to create ADMA Transformation and Implementation plans," 2020. [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/other/call-doc-annexes/call-doc-annex_innosup-08-2020_en.pdf. [Data uzyskania dostępu: 18 Listopad 2023].

[20] M. M. Mabkhot, P. Ferreira, A. Maffei, P. Podržaj, M. Mądziel, D. Antonelli, M. Lanzetta, J. Barata, E. Boffa, M. Finžgar, Ł. Paśko, P. Minetola, R. Chelli, S. Nikghadam-Hojjati i W, „Mapping Industry 4.0 Enabling Technologies into United Nations Sustainability Development Goals," *Sustainability,* tom 13, nr https://doi.org/10.3390/su13052560, 2021.

[21] K. Grobler-Debska, B. Żak, J. Baranowski, E. Kucharska i A. Domagala, „Research on effective analysis and forecasting of demand in ERP systems - case studies," w *25th International Conference on Methods and Models in Automation and Robotics (MMAR)*, Międzyzdroje, Poland, 2021.

[22] Komisja Europejska, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52019DC0640. [Data uzyskania dostępu: 18 Listopad 2023].

[23] „Development of mechatronic and cyber-physical systems," Engl. VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik , 2021. [Online]. Available: https://www.vdi.de/en/home/vdi-standards/details/vdivde-2206-development-of-mechatronic-and-cyber-physical-systems. [Data uzyskania dostępu: 18 Listopada].

[24] „Standardization Council Industrie 4.0. RAMI 4.0," SCI 4.0, 2022. [Online]. Available: https://www.sci40.com/english/thematic-fields/rami4-0/. [Data uzyskania dostępu: 18 Listopad 2023].

[25] R. Aarenstrup, Managing Model-Based Design, Natick: The MathWorks, Inc., 2015, p. 94.

[26] „Strona internetowa programu Fundusze Europejskie dla Rozwoju Funduszu Społecznego," 2023. [Online]. Available: https://www.rozwojspoleczny.gov.pl/. [Data uzyskania dostępu: 18 Listopad 2023].

[27] „Strona Ministerstwa Cyfryzacji, poświęcona kompetencjom cyfrowym," Ministerstwo Cyfryzacji, 2023. [Online]. Available: https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe. [Data uzyskania dostępu: 18 Listopad 2023].

[28] „DESI 2023 dashboard for the Digital Decade," Komisja Europejska, 2023. [Online]. Available: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts. [Data uzyskania dostępu: 18 Listopad 2023].

[29] „Weryfikator kompetencji cyfrowych Fundacji Platforma Przemysłu Przyszłości," Fundacja Platforma Przemysłu Przyszłości, 2023. [Online]. Available: https://weryfikator-kompetencji.przemyslprzyszlosci.gov.pl/. [Data uzyskania dostępu: 18 Listopad 2023].

[30] „Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.," 1997. [Online]. Available: https://dziennikustaw.gov.pl/DU/1997/s/78/483.

[31] „Słownik terminów z zakresu bezpieczeństwa narodowego, Akademia Obrony Narodowej Wydział Strategiczno-Obronny, Wydanie szóste, Warszawa 2008, s.15," 2008. [Online]. Available: https://elk.wans.edu.pl/wp-content/uploads/2021/11/Slownik_terminow_-z_zakreu_bezpieczenstwa_narodoweg.pdf. [Data uzyskania dostępu: 2 września 2023].

[32] „Biuletyn Informacji Publicznej, Agencja Bezpieczeństwa Wewnętrznego," [Online]. Available: https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-przemys/148,BEZPIECZENSTWO-PRZEMYSLOWE.html. [Data uzyskania dostępu: 4 wrzesień 2023].

[33] „Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny," 2022. [Online]. Available: https://dziennikustaw.gov.pl/du/2022/2305.

[34] „Ustawa z dnia 26 stycznia 2023 r. o zmianie niektórych ustaw w związku z wprowadzeniem świadczenia za długoletnią służbę," 2023. [Online]. Available: https://dziennikustaw.gov.pl/du/2023/347.

[35] „Ustawa z dnia 9 marca 2023 r. o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw," 2023. [Online]. Available: https://dziennikustaw.gov.pl/du/2023/641.

[36] „Ustawa z dnia 28 lipca 2023 r. o zmianie ustawy – Kodeks cywilny oraz niektórych innych ustaw," 2023. [Online]. Available: https://dziennikustaw.gov.pl/du/2023/1615.

[37] „Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej," 2020. [Online]. Available: https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf. [Data uzyskania dostępu: 7 września 2020].

[38] „Vilnius Summit Communiqué Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023," 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_217320.htm. [Data uzyskania dostępu: 8 Wrzesień 2023].

[39] „Ustawa o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r.," 2023. [Online]. Available: https://dziennikustaw.gov.pl/du/2023/913.

[40] M. Banasik, „Znaczenie nowoczesnych technologii dla bezpieczeństwa," *Rocznik Bezpieczeństwa Międzynarodowego,* tom 12, nr 2, pp. 125-139, 2019.

[41] „DoD Dictionary of Military and Associated Terms," 2021. [Online]. Available: https://irp.fas.org/doddir/dod/dictionary.pdf. [Data uzyskania dostępu: 9 Wrzesień 2023].

[42] „Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych," 2019. [Online]. Available: https://dziennikustaw.gov.pl/du/2019/1781.

[43] „Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych," 2023. [Online]. Available: https://dziennikustaw.gov.pl/du/2023/756.

[44] „Ustawa z dnia 14 kwietnia 2023 r. o Państwowej Komisji do spraw badania wpływów rosyjskich na bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej w latach 2007–2022," 2023. [Online]. Available: https://dziennikustaw.gov.pl/du/2023/1030.

[45] „Ustawa z dnia 16 czerwca 2023 r. o zmianie ustawy o Państwowej Komisji do spraw badania wpływów rosyjskich na bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej w latach 2007–2022," 2023. [Online]. Available: https://dziennikustaw.gov.pl/du/2023/1532.

[46] „Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej," 2023. [Online]. Available: https://dziennikustaw.gov.pl/du/2023/1703.

[47] I. Albrycht, Ł. Gawron, M. Góra, M. Hampel, M. Krawczyk, S. Łazarek, K. Malesa i W. Skomra, „Systemowa odporność państwa w cyfrowej erze," Instytut Kościuszki, Kraków, 2022.

[48] „Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym," 2023. [Online]. Available: https://dziennikustaw.gov.pl/du/2023/122.

[49] „Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego," Departament Bezpieczeństwa KPRM, 2021. [Online]. Available: https://www.gov.pl/web/baza-wiedzy/podrecznik-postepowania-z-incydentami-naruszenia-bezpieczenstwa-komputerowego. [Data uzyskania dostępu: 14 Wrzesień 2023].

[50] „Summary 2023 Cyber Strategy of the Department of Defense U.S. Department of Defense," 2023. [Online]. Available: https://media.defense.gov/2023/Sep/12/2003299076/1/1/1/2023_DOD_Cyber_Strategy_Summary.PDF. [Data uzyskania dostępu: 15 Wrzesień 2023].

[51] "EDIH Catalogue, European Commission," Komisja Europejska, 2023. [Online]. Available: https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue. [Data uzyskania dostępu: 18 Listopad 2023].

[52] M. Gorynia, B. Jankowska, R. Owczarzak i M. Bartosik-Purgat, „Strategie firm polskich wobec ekspansji inwestorów zagranicznych," Organizacja i Kierowanie, tom 3, nr 121, pp. 9-26, 2005.

[53] M. Gorynia i B. Jankowska, Klastry a międzynarodowa konkurencyjność i internacjonalizacja przedsiębiorstwa, Warszawa: Difin, 2008, p. 228.

[54] M. Gorynia i E. Łaźniewska, Redaktorzy, Kompendium wiedzy o konkurencyjności, Warszawa: Wydawnictwo Naukowe PWN, 2009, p. 350.

[55] M. Gorynia i B. Jankowska, The influence of Polands accession to the euro zone on the international competitiveness and internationalisation of Polish companies, Warszawa: Difin, 2013, p. 240.

Spis rysunków, tabel

Spis rysunków

Spis tabel

Platforma Przemysłu Przyszłości

Raport dotyczący luki cyfrowej oraz zagrożeń związanych z technologiami cyfrowymi – to publikacja skierowana do tych wszystkich osób, które podejmują decyzje inwestycyjne i stoją przed dylematem dotyczącym wyboru technologii i jej wprowadzenia do kultury organizacyjnej. Publikacja poszerza i porządkuje wiedzę w zakresie wpływu zmian technologicznych na przedsiębiorstwo oraz przybliża ich skutki na jego działanie. Celem publikacji jest zwrócenie uwagi nie tylko na pozytywne efekty zmian, ale co najważniejsze pobudzenie refleksji na temat zagrożeń z punktu widzenia interesu publicznego i bezpieczeństwa narodowego.

Platforma Przemysłu Przyszłości – Fundacja powołana przez Ministerstwo Rozwoju i Technologii w celu wzmacniania kompetencji i konkurencyjności podmiotów prowadzących działalność na terytorium Polski – przedsiębiorców, koordynatorów klastrów, podmiotów działających na rzecz innowacyjnej gospodarki oraz partnerów społecznych i gospodarczych w zakresie cyfryzacji.

www.przemyslprzyszlosci.gov.pl