



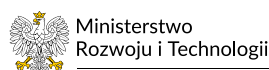
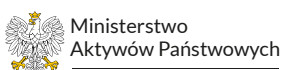
PARTNER RAPORTU



RAPORT:

BEZPIECZEŃSTWO ŁAŃCUCHÓW DOSTAW

w Polskim Przemysle Obronnym
w Czasie Pokoju



RAPORT:

BEZPIECZEŃSTWO ŁAŃCUCHÓW DOSTAW

w Polskim Przemysle Obronnym
w Czasie Pokoju

ZESPÓŁ REDAKCYJNY

Instytut Studiów Wschodnich

Zygmunt Berdychowski
Przewodniczący Rady Programowej
Forum Ekonomicznego,

dr Krzysztof Księżopolski
Instytut Badań nad Bezpieczeństwem, Energią i Klimatem
(ISECS) oraz Szkoła Główna Handlowa w Warszawie,
Kierownik Badawczo-Rozwojowy Projektu,
(cel raportu, przedmiot i obszar badań, metodyka badania,
roz. 5.4, 6.1, 6.3, 6.4, wnioski i rekomendacje)

Artur Nowak
Koordynator Raportu (cel raportu, przedmiot i obszar
badań, wnioski i rekomendacje)

Szkoła Główna Handlowa w Warszawie (roz. 2.2, 2.4, 3)

dr hab. Marzenna Cichosz, prof. SGH
Koordynator Zespołu
(cel raportu, przedmiot i obszar badań, roz. 2.2, 2.4, 3)

dr hab. Mariusz Jan Radło, prof. SGH

dr Mariusz Lipski

dr hab. Barbara Ocicka prof. SGH

dr hab. Wioletta Mierzejewska, prof. SGH

dr hab. Hanna Kinowska, prof. SGH

dr hab. Agata Lulewicz-Sas, prof. SGH

prof. dr hab. Bogumił Kamiński

dr Patryk Dziurski

dr Artur Tomeczek

Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego (roz. 2.1, 4.4, 5.2, 6.2)

płk rez. dr inż. Robert Woźniak
Koordynator Zespołu
(cel raportu, przedmiot i obszar badań, roz. 2.1)

płk rez. prof. dr hab. inż. Szymon Mitkow

płk rez. dr inż. Marek Kalwasiński

dr Paulina Zamelek

płk rez. dr inż. Ryszard Lewiński

płk rez. dr inż. Dariusz Nagrabski

płk rez. mgr inż. Piotr Górski

Politechnika Krakowska im. Tadeusza Kościuszki (roz. 4.1, 4.2, 5.3, 6.2)

dr inż. Daniel Kubek
Koordynator Zespołu
(cel raportu, przedmiot i obszar badań, roz. 4)

prof. dr hab. inż. Andrzej Szarata

dr inż. Augustyn Lorenc

dr inż. Paweł Więcek

dr inż. Sabina Puławska-Obiedowska

dr inż. Aleksandra Ciastoń-Ciulkin

dr inż. Jan Paszkowski

dr inż. Damian Grela

dr inż. Marcin Pawlik

mgr inż. Mariusz Soboń

mgr inż. Jacek Kasz

Uniwersytet Jagielloński (roz. 1.1, 1.2, 1.3)

Prof. dr hab. Krzysztof Oplustil
Koordynator Zespołu (roz. 1.4)

dr hab. Tomasz Długosz, prof. UJ

dr Mateusz Winiarz

dr Sylwia Bąk

dr hab. Sławomir Wyciślak

Uniwersytet Warszawski (roz. 5.1, 5.2)

dr hab. Tomasz Michalak, prof. UW

Akademia Górniczo-Hutnicza im. Stanisława Staszica (roz. 2.3, 4.3, 5.2)

r. pr. Magdalena Ostasz
Koordynator Zespołu

prof. dr hab. inż. Waldemar Skomudek

dr hab. inż. Stanisław Tokarski, prof. GIG

dr inż. Tomasz Siostrzonek

dr hab. inż. Arkadiusz Kustra, prof. AGH

dr inż. Artur Halbina

dr inż. Sylwia Lorenc-Szot

dr inż. Marta Podobińska-Staniec

dr inż. Anna Wiktor-Sułkowska

dr inż. Wojciech Roszczyński

mgr Jakub Izak

SPIS TREŚCI

WSTĘP	10
Cel raportu	10
Przedmiot i obszar badań	10
Metodyka badania	11
KONTEKST FUNKCJONOWANIA ŁAŃCUCHÓW DOSTAW W POLSKIM PRZEMYSŁE OBRONNYM	14
1.1. Rola i znaczenie łańcucha dostaw w obronności	14
1.2. Analiza potencjału regulacyjnego	16
1.3. Analiza wsparcia administracji państwowej	24
1.4. Wnioski i rekomendacje	30
MAPA ŁAŃCUCHÓW DOSTAW DLA WYBRANEGO SPRZĘTU WOJSKOWEGO I ŚRODKÓW BOJOWYCH	32
2.1. Analiza przedmiotowa polskiego przemysłu obronnego	32
2.2. Analiza podmiotowa potencjału polskiego przemysłu	46
2.3. Analiza surowcowa	60
2.4. Wnioski i rekomendacje	63
3. IDENTYFIKACJA I OCENA RYZYKA W ŁAŃCUCHACH DOSTAW W POLSKIM PRZEMYSŁE OBRONNYM	66
3.1. Modele łańcuchów dostaw a profil ryzyka w polskim przemyśle obronnym	67
3.2. Metodyka identyfikacji i oceny ryzyka	68
3.3. Kluczowe obszary ryzyka	69
3.4. Ocena prawdopodobieństwa i wpływu ryzyka na poziomie branży	72
3.5. Ocena znaczenia ryzyka dla wybranych kategorii sprzętu wojskowego	73
3.6. Zarządzanie ryzykiem	76
3.7. Rekomendacje	77
4. ANALIZA BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ	79
W CELU ZAPEWNIENIA CIĄGŁOŚCI DOSTAW DO PRODUKCJI I DYSTRYBUCJI SPRZĘTU WOJSKOWEGO I ŚRODKÓW BOJOWYCH	79
4.1. Infrastruktura transportowa (drogowa, kolejowa, lotnicza)	79
4.2. Infrastruktura logistyczna	86
4.3. Krytyczna infrastruktura elektroenergetyczna	91
4.4. Infrastruktura informatyczna	99
4.5. Wnioski i rekomendacje	104
5. SZTUCZNA INTELIGENCJA W BEZPIECZEŃSTWIE ŁAŃCUCHÓW DOSTAW	108
5.1. Zastosowanie AI i analiza danych w zarządzaniu ryzykiem dostaw – kierunki rozwoju	108
5.2. Cyberbezpieczeństwo w łańcuchach dostaw zasadniczego SpW, ŚB, ŚM dla Sił Zbrojnych RP	114
5.3. Ocena współzależności infrastruktury fizycznej i cyfrowej	123
5.4. Wnioski i rekomendacje	127
6. ANALIZA POTENCJAŁU POLONIZACJI ŁAŃCUCHÓW DOSTAW	131
DLA KLUCZOWEGO SPRZĘTU WOJSKOWEGO I ŚRODKÓW BOJOWYCH	131
6.1. Określenie możliwości produkcji podstawowego sprzętu wojskowego przez polski potencjał przemysłowy	131
6.2. Ocena potencjału i możliwości zaangażowania uczelni na rzecz rozwoju polskiego przemysłu obronnego	137
6.3. Analiza ryzyka polonizacji łańcucha dostaw	141
6.4. Wnioski i rekomendacje	146
WNIOSKI KOŃCOWE I KLUCZOWE REKOMENDACJE	152
Bibliografia	159
Wykaz skrótów i oznaczeń	164

Energia jutra
zaczyna się dziś



Morskie farmy wiatrowe, nowe elektrownie gazowe, zakupy nowoczesnego taboru: za każdą z tych inwestycji stoją polscy partnerzy, rodzime kompetencje i tysiące nowych miejsc pracy. To local content, czyli strategia, w której nasza energia napędza lokalny wzrost.

Morska energetyka wiatrowa
Współpraca z polskimi firmami przy budowie infrastruktury i łańcucha dostaw.

Elektrownie gazowe
Trzy nowe elektrownie budowane z udziałem polskich wykonawców i dostawców komponentów.

Tabor kolejowy
Nowoczesne lokomotywy od PESA Bydgoszcz. Największy tego typu kontrakt zawarty przez polskie firmy.



Local content to rozwój polskich firm i budowa dobrobytu dla kolejnych pokoleń

Energia jutra
zaczyna się lokalnie



PARTNER RAPORTU

ORLEN to multienergetyczny koncern, dostarczający paliwa i energię milionom odbiorców w Europie Środkowej. Firma działa w całym łańcuchu energetycznym – od wydobycia ropy i gazu, przez ich przetwórstwo i sprzedaż, po wytwarzanie oraz dystrybucję energii. Produkty spółki trafiają do klientów w ponad 100 krajach na sześciu kontynentach.

Strategia ORLEN 2035 zakłada rozwój niskoemisyjnych w rozumieniu Taksonomii UE źródeł energii. Kluczowe projekty z tego obszaru obejmują m.in. zwiększenie krajowego wydobycia gazu, budowę czterech morskich farm wiatrowych na Bałtyku, rozwój wielkoskalowych magazynów energii oraz uruchomienie co najmniej dwóch małych elektrowni jądrowych. Do 2035 roku koncern planuje przeznaczyć na realizację celów strategicznych od 350 do 380 mld zł.



Zygmunt Berdychowski

Przewodniczący Rady Programowej
Forum Ekonomicznego

Szanowni Państwo,

Współczesna architektura bezpieczeństwa międzynarodowego przechodzi obecnie najbardziej gwałtowną transformację od czasów zakończenia zimnej wojny. Pełnoskalowa agresja Federacji Rosyjskiej przeciwko Ukrainie, a także narastające napięcia geopolityczne w innych kluczowych regionach świata, poddały bezlitosnej weryfikacji dotychczasowe paradygmaty obronne państw demokratycznych. Obserwacja trwających konfliktów o wysokiej intensywności prowadzi do jednego, fundamentalnego wniosku: o zdolności państwa do przetrwania i skutecznej obrony decyduje nie tylko liczba wyszkolonych żołnierzy czy zakontraktowanych na rynkach zagranicznych nowoczesnych systemów uzbrojenia, ale w pierwszej kolejności – wydolność, elastyczność i autonomia narodowej bazy przemysłowo-technologicznej. Krwioobiegami tej bazy są łańcuchy dostaw.

Oddajemy w Państwa ręce unikalny w skali kraju, kompleksowy raport zatytułowany **„Bezpieczeństwo łańcuchów dostaw w polskim przemyśle obronnym w czasie pokoju”**. Jest to dokument o znaczeniu krytycznym i strategicznym, stanowiący odpowiedź na palącą potrzebę zdiagnozowania faktycznego stanu polskiego sektora zbrojeniowego w dobie bezprecedensowego wzrostu wydatków na obronność i masowych procesów modernizacyjnych Sił Zbrojnych RP. Jak wykazują analizy zawarte w niniejszym opracowaniu, bezpieczeństwa dostaw nie da się zbudować wyłącznie poprzez jednorazowe zwiększanie zakupów sprzętu wojskowego z zagranicy. Konieczna jest długofalowa, przemyślana polityka przemysłowo-obronna, która zagwarantuje kontrolę nad technologiami krytycznymi, umożliwi selektywną polonizację kluczowych komponentów oraz zapewni przejście od doraźnych procesów zakupowych do ciągłego zarządzania cyklem życia sprzętu wojskowego w oparciu o krajowe zdolności serwisowe i produkcyjne.

Waga niniejszego projektu polega na jego holistycznym podejściu. Zidentyfikowano w nim nie tylko klasyczne luki w zaopatrzeniu, ale również przeanalizowano potencjał regulacyjny, wsparcie administracji państwowej, trendy technologiczne oraz wyzwania surowcowe, w tym niezwykle istotny wpływ europejskiej polityki klimatycznej na energochłonny sektor obronny. To pierwsze opracowanie, które w tak przekrojowy sposób mapuje podmiotowy i przedmiotowy potencjał polskiego przemysłu w odniesieniu do wybranego asortymentu sprzętu wojskowego i środków bojowych, wskazując jednocześnie obszary najwyższego ryzyka zakłóceń – od sabotażu i cyberataków po utratę kluczowych dostawców i przerwanie szla-

ków transportowych. Analiza bezpieczeństwa łańcuchów dostaw wymagała zintegrowanego podejścia i wsparcia Ministerstwa Obrony Narodowej, Ministerstwa Aktywów Państwowych oraz Ministerstwa Rozwoju i Technologii, które to podmioty od samego początku były zaangażowane w to znaczące przedsięwzięcie.

Realizacja tak zaawansowanego zadania analitycznego nie byłaby możliwa bez połączenia sił i synergii kompetencji wiodących polskich ośrodków akademickich. Projekt ten jest doskonałym przykładem tego, jak kluczowe dla obronności państwa są dialog i ścisła współpraca na linii nauka – przemysł – administracja. Skonsolidowane wysiłki badawcze pozwoliły na stworzenie opracowania, które łączy twardą inżynierię, ekonomię, nauki prawne i zarządzanie kryzysowe. W tym miejscu pragniemy wyrazić najwyższe uznanie dla uczelni oraz kilkudziesięciu naukowców współtworzących ten raport. W prace te zaangażowane były: **Uniwersytet Warszawski, Uniwersytet Jagielloński, Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Akademia Górniczo-Hutnicza im. Stanisława Staszica, Szkoła Główna Handlowa w Warszawie, Politechnika Krakowska im. Tadeusza Kościuszki**.

Efektem tej bezprecedensowej współpracy uczelni jest zbiór konkretnych rekomendacji, skierowanych zarówno do administracji publicznej, jak i zarządów spółek. Jak podnosimy w raporcie: administracja publiczna musi wziąć na siebie rolę kreatora stabilnych warunków systemowych poprzez przewidywalne zamówienia i wsparcie procesów B+R (Badania i Rozwój). Z kolei przedsiębiorstwa muszą przyspieszyć cyfrową transformację, mapować swoich dostawców, dywersyfikować źródła zaopatrzenia i w sposób bezwzględny chronić własne technologie.

Wyrażamy głęboką nadzieję, że oddawany w Państwa ręce dokument stanie się nie tylko literaturą przedmiotu, ale przede wszystkim operacyjnym kompendium i bodźcem do odważnych decyzji zarządczych oraz politycznych. Zabezpieczenie polskich łańcuchów dostaw to dzisiaj racja stanu, od której zależą suwerenność i bezpieczna przyszłość Rzeczypospolitej Polskiej. Składamy serdeczne podziękowania wszystkim Zespołom Badawczym za ich trud, wiedzę i ogromne zaangażowanie w powstanie tego przełomowego opracowania.

Zygmunt Berdychowski

Przewodniczący Rady Programowej
Forum Ekonomicznego

NAJWAŻNIEJSZE WNIOSKI I REKOMENDACJE

Polska znajduje się obecnie w sytuacji, w której skala zakupów uzbrojenia rośnie szybciej niż zdolność państwa do zapewnienia bezpieczeństwa i ciągłości dostaw. Fundamentalnym problemem nie jest brak środków finansowych, lecz brak zintegrowanego systemu identyfikowania, oceny i ograniczenia zależności technologicznych, materiałowych, infrastrukturalnych i kadrowych. Polska może kupować coraz więcej nowoczesnego uzbrojenia, a jednocześnie pozostawać zależna od pojedynczych zagranicznych dostawców kluczowych komponentów czy usług serwisowych. Oznacza to, że **wzrost potencjału wojskowego nie jest automatycznie równoznaczny ze wzrostem bezpieczeństwa państwa.**

Najważniejszym wnioskiem raportu jest konieczność konsekwentnego przechodzenia od modelu „kupowania sprzętu” do modelu „budowania i utrzymywania zdolności”, w którym pozyskanie uzbrojenia jest elementem szerszego, ciągłego procesu zapewniania bezpieczeństwa – obejmującego rozwój, produkcję, utrzymanie, modernizację i odtwarzanie zdolności, w kraju oraz we współpracy z partnerami zagranicznymi. Każdy strategiczny kontrakt powinien obejmować nie tylko dostawę produktu, lecz również ciągłość dostaw i serwisu, dostęp do części zamiennych, dokumentacji i technologii, transfer kompetencji oraz możliwość szybkiego zwiększenia produkcji. Szczęólnego znaczenia nabiera zabezpieczenie dostaw komponentów krytycznych w górze **łańcucha dostaw**, obejmujące m.in. materiały specjalne, chemię, półprzewodniki, elektronikę. Sama produkcja końcowa lub montaż w Polsce nie jest zatem równoznaczna z suwerennością technologiczną.

Pierwszą rekomendacją powinno być stworzenie jednej centralnej „mapy bezpieczeństwa polskiej obronności”. Powinna ona obejmować krytycznych dostawców, poziomy P1–P3, surowce, technologie, infrastrukturę, zależności cyfrowe i serwisowe oraz zdolności do odtworzenia produkcji. Dla każdej strategicznej zdolności państwo powinno znać odpowiedź na pięć pytań: **od czego**

zależy dana zdolność, kto jest jedynym dostawcą, jak długo można funkcjonować bez dostaw, czy istnieje zamiennik oraz jak szybko można odtworzyć utraconą zdolność.

Drugą rekomendacją jest dalsza ewolucja roli MON w procesie pozyskiwania Sprzętu Wojskowego (SpW), a w szczególności **Agencji Uzbrojenia**. Dotyczy to kwestii administrowania kontraktami, zapewnienia zdolności operacyjnej w całym cyklu życia SpW – od decyzji zakupowej, poprzez produkcję, dostawę, eksploatację, po śledzenie potrzeb rozwoju sprzętu. Kompetencje te nie mogą dublować uprawnień, które obecnie posiada już Inspektorat Wsparcia Sił Zbrojnych w zakresie: napraw, obsługi, eksploatacji, modernizacji, remontów i odtworzenia zdolności SpW. Konieczne jest również wyeliminowanie silosowości informacyjnej pomiędzy MON, przemysłem państwowym i prywatnym oraz instytucjami odpowiedzialnymi za infrastrukturę, logistykę i finansowanie.

Trzeci priorytet to **budowa odporności, a nie pełna autarkia**. Nie wszystko musi być produkowane w Polsce, ale wszystko, co jest krytyczne dla funkcjonowania Sił Zbrojnych RP, musi być zabezpieczone poprzez dywersyfikację dostawców, strategiczne zapasy, długoterminowe umowy, dostęp do rynku sojuszniczego lub – w przypadku najważniejszych aktywów – udział kapitałowy. Szczęólniej ochrony wymagają mikroelektronika, półprzewodniki, materiały energetyczne, chemia specjalistyczna oraz technologie cyfrowe. Równocześnie odporność łańcucha musi obejmować energetykę, transport, telekomunikację oraz infrastrukturę cyfrową. Dla każdego strategicznego programu należy wskazać podmiot odpowiedzialny za koordynację całego przepływu – od źródła zaopatrzenia, przez produkcję, magazynowanie i transport, po dostawę oraz odtworzenie sprawności sprzętu. System ten powinien

obejmować przygotowane warianty zastępcze, wymagania dotyczące odporności energetycznej i informacyjnej oraz regularne testy działania po wystąpieniu zakłócenia.

Czwarty priorytet stanowi amunicja, w szczególności kalibru 120 i 155 mm. Rozwój tej zdolności powinien być traktowany jako strategiczny program przemysłowo-obronny, obejmujący cały łańcuch – od surowców, chemii i materiałów energetycznych, przez komponenty i zapalniki, po elaborację, kontrolę jakości, magazynowanie i transport. Budowa jedynie zakładu produkcji końcowej nie zapewni bezpieczeństwa, jeżeli krytyczne elementy P2 i P3 pozostaną zależne od dostawców zagranicznych.

Piąty priorytet to kadry i wiedza. Utrata kilku ekspertów może oznaczać utratę zdolności technologicznej, której odbudowa zajmie wiele lat. Należy stworzyć system identyfikacji kompetencji krytycznych, programy sukcesji, rozwój reskillingu i upskillingu oraz trwałą współpracę przemysłu z uczelniami i szkołami zawodowymi. W przedsiębiorstwach strategicznych należy rozważyć utworzenie **Korpusu Menedżerów** odpowiedzialnego za realizację kluczowych projektów, z obiektywnymi kryteriami oceny, stabilnym systemem zatrudnienia i ochroną profesjonalnego zarządzania przed bieżącymi zmianami politycznymi.

Szósty priorytet to zapewnienie konkurencyjności podmiotów, skuteczny wywiad gospodarczy, kontrwywiad i szybkość działania. Monopol państwowy nie jest synonimem bezpieczeństwa.

Tam, gdzie jest to możliwe, należy zwiększać konkurencję technologiczną i przemysłową, oceniając wykonawców nie tylko pod kątem ceny, lecz również zdolności produkcyjnych, innowacyjności, poziomu polonizacji i bezpieczeństwa dostaw. Jednocześnie wywiad gospodarczy i kontrwywiad powinny stać się stałym elementem ochrony strategicznych łańcuchów dostaw. Konieczne jest także skrócenie przewlekłych postępowań zakupowych i certyfikacyjnych, ponieważ **czas jest dziś parametrem bezpieczeństwa.**

Całość zmian powinna opierać się na pięciu zasadach: **bezpieczeństwo łańcucha dostaw jako podstawowe kryterium pozyskiwania sprzętu i usług** (*security by procurement*), **konkurencja jako element projektowania procesu i warunków zamówienia** (*competition by design*), **analiza wywiadowcza jako stały element procesu decyzyjnego** (*intelligence by default*), **czas jako parametr bezpieczeństwa** (*time is security*) oraz **kompetencje ludzi jako integralny element zdolności obronnych państwa** (*people are capability*).

Ostatecznym celem nie powinno być więc pytanie, **ile uzbrojenia Polska kupi, lecz czy będzie w stanie je produkować, naprawiać, modernizować i uzupełniać wtedy, gdy będzie to najbardziej potrzebne.** Państwo, które nie zna swoich zależności, nie zarządza bezpieczeństwem. Państwo, które je zna, ale ich nie zabezpiecza, jedynie zna swoje ryzyko. **Bezpieczeństwo zaczyna się dopiero wtedy, gdy państwo potrafi tym ryzykiem skutecznie zarządzać.**

WSTĘP

Cel raportu

Raport dotyczy bezpieczeństwa łańcuchów dostaw w polskim przemyśle obronnym w czasie pokoju, rozumianego jako zdolność państwa, Sił Zbrojnych Rzeczypospolitej Polskiej, przemysłu i współpracujących podmiotów do zapewnienia ciągłego, przewidywalnego i kontrolowanego przepływu surowców, komponentów, części zamiennych, usług, danych oraz wyrobów gotowych w wymaganym czasie, jakości, ilości i reżimie bezpieczeństwa — mimo zakłóceń technicznych, organizacyjnych, rynkowych, regulacyjnych, cybernetycznych lub geopolitycznych w czasie pokoju. Istotnym czynnikiem analizy jest optymalizacja kosztów. Analiza koncentruje się na przygotowaniu systemu w czasie pokoju do ograniczania skutków zakłóceń w obszarach produkcji, zaopatrzenia, zarządzania kapitałem ludzkim, finansów, transportu i logistyki, technologii oraz regulacji, a nie na operacyjnym zarządzaniu logistyką w czasie wojny.

Raport został przygotowany przez sześć uczelni (Szkołę Główną Handlową w Warszawie, Wojskową Akademię Techniczną im. Jarosława Dąbrowskiego, Politechnikę Krakowską im. Tadeusza Kościuszki, Akademię Górniczo-Hutniczą im. Stanisława Staszica, Uniwersytet Jagielloński oraz Uniwersytet Warszawski) we współpracy z Ministerstwem Obrony Narodowej, Ministerstwem Aktywów Państwowych oraz Ministerstwem Rozwoju i Technologii. Jego głównym odbiorcą jest Minister Obrony Narodowej, jednak ze wzglę-

du na systemowy charakter bezpieczeństwa łańcuchów dostaw oraz konieczność współdziałania wielu podmiotów raport jest adresowany również do szerokiego grona interesariuszy, w szczególności przedsiębiorstw przemysłu obronnego i ich dostawców, przedstawicieli administracji publicznej, Sił Zbrojnych Rzeczypospolitej Polskiej, instytucji odpowiedzialnych za rozwój gospodarczy i technologiczny oraz środowiska naukowego. Opracowanie opiera się wyłącznie na jawnych źródłach informacji, obejmujących literaturę przedmiotu, dokumenty strategiczne i programowe, akty prawne, raporty oraz ogólnodostępne dane statystyczne i branżowe. Zespół autorów dokonał krytycznej analizy i syntezy zgromadzonych materiałów, uzupełniając je o wnioski wynikające z własnego doświadczenia badawczego i eksperckiego. Efektem tych prac jest zestaw rekomendacji, których celem jest wsparcie działań służących zwiększeniu bezpieczeństwa, odporności i zdolności adaptacyjnych łańcuchów dostaw w polskim przemyśle obronnym oraz stworzenie podstaw do bardziej świadomego kształtowania polityk publicznych i decyzji zarządczych w tym obszarze.

W raporcie wskazano potencjalne ryzyka, oszacowano ich poziomy i prawdopodobieństwo wystąpienia oraz wpływ na bezpieczeństwo funkcjonowania łańcuchów dostaw w polskim przemyśle obronnym, które mogą mieć znaczenie dla zapewnienia ciągłości dostaw dla Sił Zbrojnych RP.

Przedmiot i obszar badań

Z uwagi na obszerny zakres przedmiotowy badania Ministerstwo Obrony Narodowej (MON) zdecydowało o zawężeniu analizy bezpieczeństwa łańcuchów dostaw do pię-

ciu rodzajów sprzętu: amunicja artyleryjska 155 mm, BWP BORSUK, system WARMATE, AHS KRAB oraz AHS K9.

W ujęciu przedmiotowym badanie rezygnuje z podejścia jednowymiarowego na rzecz wielopoziomowej analizy strukturalnej, śledzącej przepływy materiałowe, kapitałowe, informacyjne i technologiczne. Przedmiotem badań są nie tylko gotowe wyroby, ale cały łańcuch wartości: od surowców strategicznych i metali krytycznych, poprzez półprodukty, podzespoły elektroniczne, układy optoelektroniczne, aż po zaawansowane systemy sterowania i oprogramowanie bojowe.

Wielopoziomowa i złożona struktura łańcuchów dostaw wymagała ograniczenia obszaru badań i skoncentrowania się na krajowych integratorach systemów oraz wybranych kluczowych podmiotach polskiego przemysłu obronnego. W konsekwencji badaniem objęto zarówno państwowe podmioty – skonsolidowane w strukturach holdingu Polska Grupa Zbrojeniowa (PGZ S.A. jako integrator administracyjny i holdingowy), jak i wiodące podmioty prywatne, ze szczególnym uwzględnieniem Grupy WB (jako integratora technologicznego). Takie zbalansowane podejście pozwala na obiektywne zidentyfikowanie synergii, barier kooperacyjnych oraz dysproporcji potencjałów pomiędzy państwowym a prywatnym segmentem krajowego przemysłu obronnego.

Badaniem objęto sieć powiązań kompetencyjnych pomiędzy kluczowymi organami administracji publicznej (MON, MAP, MSWiA) a agencjami wykonawczymi i instytucjami finansowymi, takimi jak Rządowa Agencja Rezerw Strategicznych (RARS), Agencja Mienia Wojskowego (AMW) oraz Bank Gospodarstwa Krajowego (BGK). Raport analizuje

przepływ informacji planistycznych między tymi podmiotami w celu eliminacji zjawiska silosowości informacyjnej.

Obszar badań został ograniczony pod względem czasowym i operacyjnym do warunków funkcjonowania przemysłu **w czasie pokoju**. Perspektywa ta celowo pomija operacyjne zarządzanie logistyką w fazie wojny kinetycznej, skupiając się na kluczowym dla odporności państwa procesie przygotowania struktur gospodarczych, tworzenia rezerw i procedur. Horyzont prognostyczny i planistyczny raportu został zsynchronizowany ze średniookresową perspektywą wdrożeniową Centralnych Planów Rzeczowych MON, w tym niejawnego „Programu Rozwoju Sił Zbrojnych RP na lata 2025–2039” oraz powiązanych z nim planów modernizacji technicznej i zakupu środków materiałowych. Obszar badawczy raportu osadzony jest w złożonej, wielopoziomowej architekturze prawno-instytucjonalnej, łączącej reżimy krajowe z regulacjami międzynarodowymi (Unii Europejskiej oraz NATO). Analiza obejmuje badanie spójności, komplementarności oraz potencjalnych luk prawnych w stosowaniu kluczowych aktów normatywnych.

Obszar badań obejmuje również ocenę odporności otoczenia infrastrukturalnego i technologicznego, w którym funkcjonują łańcuchy dostaw. Wymiar ten został podzielony na trzy komplementarne obszary obejmujące odporność infrastruktury i systemu energetycznego, kondycję finansową i ryzyka płynnościowe, integralność cyfrową i cyberbezpieczeństwo.

Metodyka badania

Badanie zostało przeprowadzone z wykorzystaniem podejścia integrującego metody jakościowe i elementy analizy danych ilościowych. Przyjęte podejście wynikało ze złożoności badanego problemu, którego nie można wiarygodnie analizować wyłącznie z perspektywy ekonomicznej, bezpieczeństwa, logistyki czy prawa. Bezpieczeństwo łańcuchów dostaw w przemyśle obronnym stanowi bowiem rezultat współoddziaływania czynników technologicznych, organiza-

cyjnych, infrastrukturalnych, regulacyjnych, finansowych oraz geostrategicznych, dlatego proces badawczy wymagał połączenia różnych metod analizy oraz wzajemnej weryfikacji uzyskanych wyników. Podstawowym założeniem metodologicznym było odejście od jednowymiarowego postrzegania bezpieczeństwa dostaw na rzecz systemowej oceny odporności całego ekosystemu przemysłowo-obronnego.

Badanie podporządkowano odpowiedzi na pytanie, w jakim stopniu polski przemysł obronny jest zdolny zapewnić ciągłość dostaw sprzętu wojskowego i środków bojowych w warunkach zakłóceń występujących w czasie pokoju oraz jakie czynniki ograniczają lub wzmacniają odporność analizowanych łańcuchów dostaw. W szczególności analizowano, które ogniwa wykazują największą podatność na zakłócenia, jakie znaczenie mają uwarunkowania regulacyjne, technologiczne i organizacyjne dla utrzymania ciągłości produkcji oraz w jakim zakresie możliwe jest ograniczenie ryzyka poprzez rozwój krajowych zdolności przemysłowych, dywersyfikację dostaw lub proces polonizacji wybranych komponentów i usług.

Jednostkę analizy stanowiły łańcuchy dostaw wybranych systemów uzbrojenia wraz z ich komponentami materiałowymi, technologicznymi, organizacyjnymi, logistycznymi, cyfrowymi oraz regulacyjnymi. Dobór sprzętu miał charakter celowy i został uzgodniony z Ministerstwem Obrony Narodowej. Analizą objęto amunicję artyleryjską kalibru 155 mm, bojowy wóz piechoty Borsuk, system amunicji krążącej Warmate, armatohaubicę samobieżną Krab oraz armatohaubicę K9 w kontekście rozwoju krajowych zdolności serwisowo-produkcyjnych. Wybrane systemy reprezentują odmienne modele organizacji łańcuchów dostaw – od rozwiązań o wysokim stopniu krajowej autonomii technologicznej po systemy silnie uzależnione od zagranicznych dostawców – co umożliwiło porównanie różnych modeli funkcjonowania przemysłu obronnego oraz identyfikację wspólnych mechanizmów ryzyka.

Proces badawczy miał charakter sekwencyjny i został zrealizowany w pięciu wzajemnie powiązanych etapach. Pierwszy etap obejmował analizę źródeł wtórnych, w ramach której dokonano krytycznego przeglądu krajowej i zagranicznej literatury przedmiotu, dokumentów strategicznych, aktów prawnych, raportów instytucji publicznych, dokumentów programowych NATO i Unii Europejskiej oraz ogólnodostępnych danych statystycznych i branżowych. Celem tego etapu było zidentyfikowanie uwarunkowań funkcjonowania krajowego przemysłu obronnego oraz określenie formalnych ram bezpieczeństwa łańcuchów dostaw.

Kolejny etap polegał na mapowaniu analizowanych łańcuchów dostaw. Analiza została przeprowadzona równolegle w dwóch wymiarach. W ujęciu podmiotowym zidentyfikowano integratorów systemów uzbrojenia, dostawców komponentów funkcjonujących na poziomach P 1, P 2 i P 3 oraz dostawców surowców i materiałów strategicznych. W ujęciu przedmiotowym przeanalizowano przepływy materiałów, komponentów, technologii, usług serwisowych, praw własności intelektualnej oraz zależności cyfrowych występujących pomiędzy poszczególnymi uczestnikami analizowanych łańcuchów. Pozwoliło to na identyfikację punktów koncentracji ryzyka oraz potencjalnych wąskich gardeł ograniczających ciągłość produkcji i utrzymania sprzętu wojskowego.

Na podstawie przygotowanych map przeprowadzono ocenę podatności analizowanych struktur na zakłócenia. W badaniu przyjęto, że ryzyko stanowi funkcję czterech wzajemnie powiązanych elementów: krytyczności danego komponentu lub usługi dla ciągłości funkcjonowania systemu uzbrojenia, prawdopodobieństwa wystąpienia zakłócenia, potencjalnych skutków jego wystąpienia oraz możliwości odtworzenia zdolności poprzez zastosowanie alternatywnych dostawców, krajowej produkcji, zapasów strategicznych, zamienników lub innych mechanizmów ograniczających podatność łańcucha dostaw.

Operacjonalizacja tych założeń została przeprowadzona z wykorzystaniem autorskiego modelu analizy wektorowej obejmującego sześć podstawowych obszarów funkcjonowania łańcuchów dostaw: bezpieczeństwo dostaw surowców i materiałów, krajowe zdolności produkcyjne, infrastrukturę transportową, logistykę magazynową, bezpieczeństwo energetyczne oraz odporność i cyberbezpieczeństwo systemów teleinformatycznych. Takie podejście umożliwiło ocenę nie pojedynczych przedsiębiorstw, lecz odporności całego systemu przemysłowego.

Integralnym elementem badania była również analiza potencjału technologicznego krajowego przemysłu obronnego. Wykorzystano kwerendy prowadzone w krajowych i międzynarodowych bazach patentowych

(UPRP, Espacenet i PATENTSCOPE), analizę projektów badawczo-rozwojowych realizowanych przez przedsiębiorstwa, uczelnie oraz instytuty badawcze, a także informacje dotyczące poziomów gotowości technologicznej (TRL). Analiza ta miała charakter pomocniczy i nie była traktowana jako dowód posiadania zdolności produkcyjnych. Jej celem było wskazanie kierunków koncentracji kompetencji technologicznych oraz identyfikacja obszarów, w których istnieje potencjał rozwoju krajowych zdolności przemysłowych.

Istotnym elementem metodyki była analiza otoczenia prawno-instytucjonalnego. W tej części zastosowano metodę dogmatyczno-prawną, uzupełnioną o analizę funkcjonalną. Przedmiotem badania była identyfikacja instrumentów prawnych mogących oddziaływać na odporność łańcuchów dostaw, obejmujących planowanie obronne, system rezerw strategicznych, ochronę infrastruktury krytycznej, cyberbezpieczeństwo, zamówienia publiczne, kontrolę obrotu towarami strategicznymi oraz instrumenty polityki przemysłowej Unii Europejskiej. Celem analizy nie była ocena skuteczności stosowania tych instrumentów przez administrację publiczną, lecz określenie ich potencjalnego wpływu na bezpieczeństwo analizowanych łańcuchów dostaw.

Dla zwiększenia wiarygodności wyników zastosowano strategię triangulacji metod, polegającą na wzajemnym porównywaniu rezultatów uzyskanych z różnych źródeł informacji. Wyniki analiz dokumentów, danych rejestrowych, analiz patentowych i mapowania łańcuchów dostaw zostały skonfrontowane z rezultatami ustrukturyzowanych warsztatów eksperckich z udziałem przedstawicieli administracji publicznej, przedsiębiorstw przemysłu obronnego, środowiska naukowego oraz specjalistów z zakresu logistyki, produkcji i bezpieczeństwa. Opinie ekspertów nie stanowiły samodzielnego źródła ustaleń badawczych, lecz służyły walidacji rezultatów uzyskanych w toku analiz empirycznych oraz identyfikacji obszarów wymagających pogłębionej interpretacji. Takie rozwiązanie ograniczyło wpływ subiektywnych ocen oraz zwiększyło wiarygodność procesu badawczego, odpowiadając na potrzebę wyraźnego rozróżnienia między wynikami

analiz a ocenami eksperckimi. Badanie oparto na danych pochodzących z wielu niezależnych źródeł, obejmujących akty prawne, dokumenty strategiczne, raporty przedsiębiorstw, dane statystyczne, rejestry patentowe, bazy projektów badawczo-rozwojowych, informacje o infrastrukturze krytycznej oraz materiały pozyskane podczas warsztatów eksperckich. Zastosowanie zróżnicowanych źródeł danych umożliwiło ograniczenie ryzyka błędów wynikających z wykorzystania pojedynczego źródła informacji oraz zwiększyło możliwość wzajemnej weryfikacji uzyskanych rezultatów.

Należy jednocześnie podkreślić, że badanie ma jednak pewne ograniczenia. Wynikają one przede wszystkim z jawnego charakteru wykorzystanych źródeł, a więc braku dostępu do informacji niejawnych, szczegółowych danych kontraktowych, dokumentacji technicznej, szczegółowych danych dotyczących poddostawców niższych poziomów oraz informacji objętych tajemnicą przedsiębiorstwa. Ograniczeniem jest również dynamiczny charakter analizowanych łańcuchów dostaw, które podlegają zmianom wynikającym z procesów modernizacji technicznej Sił Zbrojnych RP, zmian regulacyjnych, sytuacji geostrategicznej oraz przesunięcia czasowego dostępnych danych. Z tego względu przedstawione wyniki należy traktować jako ekspercką diagnozę wspierającą proces podejmowania decyzji strategicznych oraz identyfikację priorytetowych kierunków dalszych analiz, a nie jako pełny audyt przemysłowy krajowego sektora obronnego.

KONTEKST FUNKCJONOWANIA ŁAŃCUCHÓW DOSTAW W POLSKIM PRZEMYSŁE OBRONNYM

1.1. Rola i znaczenie łańcucha dostaw w obronności

Sposób rozumienia pojęcia „łańcuch dostaw” jest uzależniony od kilku czynników, do których zalicza się m.in.: złożoność produktu finalnego, jego przeznaczenie, zasięg przestrzenny działania podmiotów zaangażowanych we współpracę, przyjęte strategie zaopatrzenia czy dystrybucji¹. Szczególną rolę łańcuchy dostaw odgrywają w zabezpieczeniu potrzeb obronnych państwa². W tym sektorze łańcuch dostaw stanowi fundament równowagi sił zbrojnych pomiędzy efektywnością w czasie pokoju, a możliwością skalowania produkcji oraz operacji logistycznych w czasie wojny³. Bezpieczeństwo łańcuchów dostaw w przemyśle zbrojeniowym uznaje się więc za jeden z czynników determinujących skuteczność systemu obrony narodowej.

Zastosowanie teorii zarządzania łańcuchami dostaw w przemyśle zbrojeniowym wnosi nowe perspektywy problemowe ze względu na specyficzne wymogi operacyjne i ograniczenia instytucjonalne: 1) teoria kosztów transakcyjnych nabiera znaczenia w kontekście decyzji dotyczących wyboru własnej produkcji uzbrojenia lub outsourcingu do prywatnych kontrahentów, gdzie asymetria informacji i specyficzność aktywów są kluczowe⁴, 2) podejście zasobowe znajduje zastosowanie w analizie strategicznych zdolności obronnych oraz w zarządzaniu krytycznymi łańcuchami dostaw broni i technologii wojskowych⁵, 3) teoria interesariuszy wymaga rozszerzenia o specyficzne grupy interesów, takie jak: sojusznicy strategiczni, społeczność międzynarodowa oraz obywatele [Elvemo, 2025], 4) teoria sieciowa pomaga w zrozu-

-
- 1 Kos, B. (2013). Znaczenie łańcuchów dostaw we współczesnej gospodarce. Zeszyty Naukowe Uniwersytetu Szczecińskiego, Problemy Zarządzania, Finansów i Marketingu, 29(751), 73–88.
 - 2 Antai, I., Hellberg, R. (2024). Identifying total defense logistics concepts: A comparative study of the Swedish pandemic response. Journal of Humanitarian Logistics and Supply Chain Management, 14(2), 208–222.
 - 3 Kovács, G., and P. Tatham. 2009. "Responding to Disruptions in the Supply Network – from Dormant to Action." Journal of Business Logistics 30 (2): 215–229. <https://doi.org/10.1002/j.2158-1592.2009.tb00121.x>.
 - 4 Kovács, G., and P. Tatham. 2009. "Responding to Disruptions in the Supply Network – from Dormant to Action." Journal of Business Logistics 30 (2): 215–229. <https://doi.org/10.1002/j.2158-1592.2009.tb00121.x>.
 - 5 Loska, D., Hazen, B., Rich, N., Genchev, S., Malik, T. (2025). Military Supply Chain Logistics and Dynamic Capabilities: A Literature Review and Synthesis. Transportation Journal, 64(2), e70002. <https://doi.org/10.1002/tjo3.70002>

mieniu złożonych relacji między różnymi rodzajami sił zbrojnych, agencjami rządowymi i kontrahentami obronnymi w ramach wielonarodowych sojuszy wojskowych⁶, 5) podejście systemowe w kontekście wojskowym umożliwia analizę wpływu zakłóceń w jednym elemencie systemu łańcucha dostaw na całokształt zdolności operacyjnych, co jest kluczowe dla zapewnienia ciągłości funkcjonowania w warunkach konfliktu zbrojnego⁷.

W zarządzaniu łańcuchami dostaw, również w przemyśle zbrojeniowym, istotny jest właściwy dobór długofalowych planów działania. Tym co wyróżnia strategię obronnych łańcuchów dostaw na tle łańcuchów dostaw z innych sektorów, to ich specyficzne wymagania, które powinny być uwzględniane w czasie kryzysów i konfliktów. Do potrzeb tych należą: redukcja buforowych zapasów kluczowych surowców i produktów, skrócenie czasu dostaw (just-in-time)⁸ oraz koncentracja na ciągłości wymiany w łańcuchu pomimo zakłóceń, które mogą bezpośrednio wpływać na gotowość operacyjną⁹. Istotnym wymiarem zarządzania łańcuchami dostaw realizującymi cele obrony narodowej są także adekwatne mechanizmy koordynacyjne. Integracja i koordynacja w tych łańcuchach charakteryzuje się specyficznymi wymogami wynikającymi z natury operacji wojskowych oraz struktury organizacyjnej sił zbrojnych. W ich przypadku synchronizacja logistyczna nabiera krytycznego znaczenia, ponieważ opóźnienia dostaw mogą mieć bezpośredni wpływ na bezpieczeństwo i sukces misji. Wymiana informacji w sektorze wojskowym musi uwzględniać aspekty bezpieczeństwa oraz klasyfikację danych, co wymaga specjalistycznych systemów łączności i protokołów bezpieczeństwa. Mechanizmy koordynacji charakteryzują się więc wysokim poziomem formalizacji wynikającym z hierarchicznej

struktury organizacyjnej oraz rygorystycznych procedur operacyjnych, jednocześnie wykorzystując nieformalne sieci współpracy między dowódcami różnych szczebli w ramach sojuszy międzynarodowych¹⁰.

Wspomniane mechanizmy koordynacyjne, obecnie przejawiają się również w postaci szerokiego zastosowania technologii, oprogramowania i towarów podwójnego zastosowania, które mogą być wykorzystywane symultanicznie zarówno w sektorze, cywilnym, jak i wojskowym, co stanowi o silnym powiązaniu organizacyjno-technologicznym między nimi. Technologie podwójnego zastosowania wymagają najczęściej współpracy pomiędzy sektorem obronnym, a uczelniami, instytutami badawczymi czy startupami technologicznymi. Obecnie efektami tego typu współpracy są najczęściej nowe narzędzia sztucznej inteligencji, technologie kosmiczne, autonomiczne systemy, zaawansowane materiały oraz nowe narzędzia wykorzystywane w obszarze cyberbezpieczeństwa.

Podejście do specyficznych ryzyk związanych z funkcjonowaniem łańcuchów dostaw w przemyśle zbrojeniowym jest kolejnym ważnym elementem zarządzania nimi, zarówno z perspektywy centralnej, jak i operacyjnej. Zarządzanie ryzykiem w tych łańcuchach dostaw cechują unikalne wyzwania wynikające z operowania w środowisku potencjalnej lub rzeczywistej wrogości oraz krytycznego wpływu na bezpieczeństwo narodowe. Współczesne wyzwania w zakresie zarządzania zakłóceniami w łańcuchach dostaw obronnych podkreślają potrzebę przejścia od reaktywnego do proaktywnego podejścia w identyfikacji i mitygacji ryzyka systemowego, szczególnie w kontekście rosnących napięć geopolitycznych i złożono-

6 Ekström, T. (2025). Supply Chain Resilience – An Empirical Exploration of Barriers and Enablers in Military Settings. *Scandinavian Journal of Military Studies*. <https://doi.org/10.31374/sjms.350>

Antai, I., Hellberg, R. (2024). Identifying total defense logistics concepts: A comparative study of the Swedish pandemic response. *Journal of Humanitarian Logistics and Supply Chain Management*, 14(2), 208–222. <https://doi.org/10.1108/JHLSCM-07-2022-0084>

7 Ekström, T. (2025). Supply Chain Resilience – An Empirical Exploration of Barriers and Enablers in Military Settings. *Scandinavian Journal of Military Studies*. <https://doi.org/10.31374/sjms.350>

8 Hellberg, R. (2023). Swedish Public Procurement and the Defence Industry: Obstacles and Opportunities. *Journal of Defense Analytics and Logistics* 7(2), s. 103–137.

9 Korkmaz, G. (2024). Supply Chain Risks and Management Strategies in the Defence Industry. *Journal of Defense Resources Management*, 15(1), s. 35–60.

10 Loska, D., Hazen, B., Rich, N., Genchev, S., Malik, T. (2025). Military Supply Chain Logistics and Dynamic Capabilities: A Literature Review and Synthesis. *Transportation Journal*, 64(2), e70002. <https://doi.org/10.1002/tjo.370002>

ści technologicznej systemów uzbrojenia¹¹. Zarządzanie ryzykiem w wojskowych łańcuchach dostaw wymaga więc specjalistycznych strategii uwzględniających te unikalne zagrożenia i wyzwania oraz wymogi bezpieczeństwa narodowego. Jedną z takich strategii jest łagodzenie ryzyka, które w kontekście wojskowym powinno koncentrować się na budowaniu niezależnych zdolności produkcyjnych oraz strategicznych rezerw krytycznych materiałów, co często przeważa nad optymalizacją kosztową¹². Kolejną możliwą strategią jest transfer ryzyka, który w sektorze obronnym jest ograniczony ze względu na kwestie bezpieczeństwa narodowego oraz klasyfikację informacji, co wymusza większą zależność od mechanizmów łagodzenia ryzyka. Strategie wojskowe muszą również uwzględniać ryzyka wynikające z działań wojennych przeciwnika, co wymaga implementacji redundantnych systemów oraz procedur bezpieczeństwa operacyjnego znacznie przekraczających standardy komercyjne¹³.

Naturalną konsekwencją realizowanych procedur zarządzania ryzykiem w obronnych

łańcuchach dostaw jest ciągle wzmacnianie ich odporności. Szczególne znaczenie w tym przypadku mają uwarunkowania logistyki wojskowej, takie jak: złożone systemy adaptacyjne, dynamiczne zdolności związane z dowodzeniem i kontrolą oraz dedykowane narzędzia zarządzania ryzykiem i zarządzania kryzysowego specjalnie dostosowane do specyfiki funkcjonowania podmiotów pełniących funkcje obronne oraz ich partnerów współpracujących w łańcuchu dostaw¹⁴. Zwiększaniu poziomu odporności łańcuchów dostaw wykorzystywanych w systemach bezpieczeństwa narodowego, mogą służyć takie działania organizowane centralnie jak: szkolenia i zgłębianie wiedzy na temat logistyki wojskowej wśród podmiotów uczestniczących we współpracy łańcucha dostaw, koncentracja na działaniach służących utrzymaniu efektywności operacyjnej i siły bojowej w każdych (szczególnie kryzysowych) warunkach oraz wzmacnianie umiejętności służących szybkiemu odzyskiwaniu pełnej funkcjonalności i przepustowości łańcucha po sytuacji kryzysowej¹⁵.

1.2. Analiza potencjału regulacyjnego

Główne cele polityki państwa w zakresie bezpieczeństwa narodowego i obronności określa Strategia Bezpieczeństwa Narodowego RP z 2020 roku (dalej: SBN)¹⁶. W lipcu 2025 r. Rada Ministrów przyjęła nową SBN RP, która wymaga zatwierdzenia przez Prezydenta RP¹⁷ zgodnie z art. 24 ust. 1 pkt 2 ustawy z 11.03.2022 r. o obronie Ojczyzny¹⁸

(dalej: u.o.O.). Dokumentem planistycznym o fundamentalnym znaczeniu dla Sił Zbrojnych jest „Program Rozwoju Sił Zbrojnych RP na lata 2025–2039” wprowadzony w drodze zarządzenia Ministra Obrony Narodowej z 22.12.2025 r., będący dokumentem niejawnym¹⁹. Dokument jest aktualizowany co cztery lata na 15-letni okres planistyczny, zgodnie

11 Dolgui, A., Ivanov, D., Sokolov, B. (2018). Ripple effect in the supply chain: An analysis and recent literature. *International Journal of Production Research*, 56(1–2), 414–430. <https://doi.org/10.1080/00207543.2017.1387680>

12 Jüttner, U., Maklan, S. (2011). Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Management: An International Journal*, 16(4), 246–259. <https://doi.org/10.1108/13598541111139062>

13 Apte, A., Rendon, R., Salmeron, J. (2011). An optimization approach to strategic sourcing: A case study of the United States Air Force. *Journal of Purchasing and Supply Management*, 17. <https://doi.org/10.1016/j.pursup.2011.03.002>

14 Elvemo, L. (2025). Supply Chain Resilience in Military Operations: A Case Study Exploring Command and Control. *Scandinavian Journal of Military Studies*, 8(1), s. 178–199.

15 Elvemo, L. (2025). Supply Chain Resilience in Military Operations: A Case Study Exploring Command and Control. *Scandinavian Journal of Military Studies*, 8(1), s. 178–199.

16 Załącznik do postanowienia Prezydenta Rzeczypospolitej Polskiej z dnia 12 maja 2020 r. w sprawie zatwierdzenia „Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej” (M. P. z 2020 r. poz. 413); https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf

17 <https://www.gov.pl/web/premier/strategia-bezpieczenstwa-narodowego-rzeczypospolitej-polskiej>

18 Tj. Dz.U. z 2025 r., poz. 825.

19 Więcej na ten temat publikacja serwisu Prawo.pl pt. Docelowo pół miliona żołnierzy – wojsko wdraża nowy Program Rozwoju Sił Zbrojnych, wiadomość z 16.01.2026 r., dostępna na stronie: <https://www.prawo.pl/samorzad/nowy-program-rozwoju-sil-zbrojnych-liczebosc-wojska-nowe-jednostki,536802.html> (data dostępu: 29.04.2026 r.).

ze standardami NATO. Zgodnie z art. 37 ust. 2 u.o.O., Program ma określać w szczególności zamierzenia w zakresie gromadzenia i utrzymywania zapasów środków bojowych i materiałowych dla Sił Zbrojnych oraz rozwoju infrastruktury wojskowej. Dla realizacji tych zamierzeń istotne znaczenie ma zapewnienie bezpieczeństwa łańcuchów dostaw. Plan opiera się na dwóch niejawnych dokumentach nadrzędnych: „Głównych kierunkach rozwoju Sił Zbrojnych oraz ich przygotowań do obrony państwa” przyjętych przez Prezydenta RP oraz „Szczegółowych kierunkach przebudowy i modernizacji technicznej Sił Zbrojnych” zatwierdzonych uchwałą Rady Ministrów z 11.12.2024 r. Dokumentami pochodnymi są Centralne Plany Rzeczowe, w tym Plan Modernizacji Technicznej, Plan Zakupu Środków Materiałowych oraz krajowe i natowskie plany inwestycji budowlanych, w tym realizowane w ramach NATO *Security Investment Programme*.

1.2.1. Analiza prawnych ram i potencjału regulacyjnego łańcuchów dostaw w polskim przemyśle obronnym

Z punktu widzenia zabezpieczenia i organizacji łańcuchów dostaw na potrzeby obronne kluczowe znaczenie mają **przepisy działów XX–XXII** ustawy z dnia 11 marca 2022 r. **o obrocie Ojczyzny**²⁰ (dalej: u.o.O.), które podporządkowują rynkowe relacje przedsiębiorców systemowi sformalizowanych obowiązków administracyjnoprawnych, uzasadnionych potrzebami bezpieczeństwa i obronności państwa oraz potrzebami Sił Zbrojnych. Obowiązek realizacji zadań obronnych przez przedsiębiorców obejmuje w szczególności wykonywanie produkcji, napraw lub świadczenie usług w warunkach zagrożenia bezpieczeństwa państwa lub w czasie wojny, utrzymywanie w czasie pokoju niezbędnych mocy produkcyjnych, naprawczych lub usługowych, a także ochronę obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa. Obejmuje on również zabezpieczenie systemów łączności, transportu, energetyki, gazownictwa i sektora pa-

liwowego, zapewnienie logistycznego wsparcia, utrzymanie funkcjonowania systemów wodociągowych i kanalizacyjnych oraz wykonywanie prac wdrożeniowych i ekspertyz (art. 600 ust. 2 oraz art. 648 ust. 1 u.o.O.).

Całkowite podporządkowanie jednostek gospodarczych organom administracji publicznej lub Siłom Zbrojnym, prowadzące *de facto* do wyłączenia rynkowego charakteru relacji gospodarczych, następuje w ramach **militaryzacji** (art. 2 pkt 11 oraz art. 604 ust. 4 u.o.O.). Jej kluczowym elementem jest zmiana statusu prawnego personelu. Wobec osób posiadających przydziały organizacyjno-mobilizacyjne powstaje stosunek służbowy militaryzacji, który z mocy prawa zawiesza dotychczasowe stosunki pracy (art. 608 ust. 1 u.o.O.). Militaryzacja jednostek gospodarczych może zostać wprowadzona przez Radę Ministrów w przypadku ogłoszenia stanu wojennego, stanu wyjątkowego na całym terytorium Rzeczypospolitej Polskiej, mobilizacji oraz w czasie wojny i dotyczy jednostek przewidzianych do militaryzacji, na które nałożono obowiązek realizacji zadań szczególnie ważnych dla bezpieczeństwa lub obronności państwa (art. 600 ust. 1 u.o.O.). Prowadzony jest wykaz jednostek przewidzianych do militaryzacji (art. 600 ust. 5 u.o.O.), do którego wpisuje się jednostki organizacyjne oraz przedsiębiorców, na których nałożono, w drodze decyzji administracyjnej Ministra, obowiązek realizacji zadań szczególnie ważnych dla bezpieczeństwa lub obronności państwa. Na jednostkach przewidzianych do militaryzacji spoczywa obowiązek przygotowania do realizacji zadań (art. 603 u.o.O.). Zmilitaryzowane jednostki wykonują zadania określone przez właściwe organy, zgodnie z planami operacyjnymi (art. 2 pkt 15 oraz art. 604 ust. 4 u.o.O.). Zadania jednostek zmilitaryzowanych obejmują szeroki zakres procesów gospodarczych i logistycznych, w tym produkcję i naprawę uzbrojenia, zapewnienie ciągłości dostaw energii i paliw, ochronę obiektów oraz infrastruktury o znaczeniu strategicznym, a także szeroko rozumiane wsparcie realizacji zadań na rzecz bezpieczeństwa i obronności państwa (art. 600 ust. 2 u.o.O.).

²⁰ Dz. U. z 2025 r. poz. 825 ze zm.

Niezależnie od powyższego, zabezpieczenie ciągłości i odporności łańcuchów dostaw w u.o.O opiera się na dwóch komplementarnych mechanizmach ustawowych, tj. na instytucji świadczeń osobistych i rzeczowych na rzecz obrony (dział XXI u.o.O.) oraz na szczególnym reżimie zadań realizowanych przez przedsiębiorców na rzecz Sił Zbrojnych (dział XXII u.o.O.). Świadczenia osobiste w czasie pokoju polegają na wykonywaniu doraźnych prac przez osoby fizyczne, w tym osoby prowadzące działalność gospodarczą, na rzecz przygotowania obrony państwa. Świadczenia rzeczowe w czasie pokoju polegają natomiast na czasowym oddaniu do używania określonych zasobów, także przez przedsiębiorców, na potrzeby Sił Zbrojnych, jednostek przewidzianych do militaryzacji oraz innych podmiotów wykonujących zadania na rzecz obronności państwa. W warunkach pokoju świadczenia rzeczowe mogą służyć zabezpieczeniu ćwiczeń wojskowych, zapewniać doraźne wzmocnienie zasobów materialnych systemu logistycznego. Dalej idącą integrację zasobów cywilnych z potencjałem wojskowym zapewniają tzw. świadczenia szczególne, których celem jest – finansowane ze środków publicznych – dostosowanie infrastruktury, utrzymywanie zdolności produkcyjnych oraz gromadzenie i konserwacja składników majątkowych niezbędnych do realizacji zadań obronnych (art. 642 u.o.O.).

Dla utrzymania łańcuchów dostaw o charakterze przemysłowym znaczenie mają zadania realizowane przez przedsiębiorców na rzecz Sił Zbrojnych (dział XXII u.o.O.). Minister Obrony Narodowej nakłada na wybranych przedsiębiorców obowiązki obejmujące nie tylko przyszłą produkcję lub świadczenie usług w warunkach zagrożenia, lecz także utrzymywanie w czasie pokoju określonych mocy produkcyjnych, naprawczych lub usługowych. Mechanizm ten stanowi podstawę budowania tzw. nadmiarowości oraz zapewnienia ciągłości działania łańcuchów dostaw w przypadku zakłóceń (art. 648 ust. 1 pkt 1 i 2 u.o.O.). Realizacja tych obowiązków odbywa się w sformalizowanym reżimie opartym na decyzji administracyjnej oraz umowie (art. 648 ust. 2 i 6 u.o.O.). Całość systemu podlega nadzorowi i kontroli Ministra Obrony Na-

rodowej, co obejmuje weryfikację sposobu przygotowania przedsiębiorców do realizacji zadań oraz prawidłowości wykorzystania środków publicznych (art. 661 oraz art. 662 ust. 1 u.o.O.). Nadzór nad strukturą i drożnością łańcuchów dostaw wykonywany jest w oparciu o Plan zabezpieczenia potrzeb Sił Zbrojnych (art. 651 ust. 1 u.o.O.). Plan ten obejmuje m.in. szczegółowy wykaz kooperantów i podwykonawców – krajowych i zagranicznych – dostarczających surowce i komponenty niezbędne dla ciągłości produkcji obronnej (art. 651 ust. 2 pkt 3 u.o.O.). Zapewnia to wgląd w głęboką strukturę łańcucha wartości i umożliwia identyfikację ryzyk wynikających z uzależnienia od dostawców zewnętrznych. Plan sporządza się na okres pięciu lat, co najmniej na rok przed upływem okresu obowiązywania planu poprzedniego, co wyznacza horyzont analizy łańcuchów dostaw. Plan jest przygotowywany i zatwierdzany przez MON, a jego uruchomienie – w całości lub w części – następuje na wniosek tego ministra przez Prezesa RM w drodze rozporządzenia, w celu zabezpieczenia obrony państwa w warunkach zewnętrznego zagrożenia bezpieczeństwa. W przypadku uruchomienia planu przedsiębiorcy realizują zadania na rzecz Sił Zbrojnych z pierwszeństwem przed innymi zadaniami (art. 654 ust. 1 i 2 u.o.O.). Ryzyko strukturalne może wynikać z niedostatecznej jednoznacznego rozgraniczenia między przygotowaniem jednostek do militaryzacji, świadczeniami na rzecz obrony oraz zadaniami realizowanymi przez przedsiębiorców na rzecz Sił Zbrojnych w reżimach określonych w działach XXI i XXII ustawy o obronie Ojczyzny. Poszczególne mechanizmy regulacyjne dotyczą w istocie tych samych kategorii obowiązków, w szczególności utrzymywania mocy produkcyjnych, naprawczych i usługowych, co może powodować niepewność co do ich wzajemnego stosunku. niespójność ujawnia się również na poziomie finansowania, np. koszty przygotowań do militaryzacji ponoszą przedsiębiorcy (art. 603 ust. 2 u.o.O.), podczas gdy realizacja zadań na rzecz Sił Zbrojnych podlega mechanizmowi dotacyjnemu (art. 659 ust. 1 u.o.O.).

W czasie pokoju istotne znaczenie dla organizacji oraz zabezpieczenia łańcuchów dostaw na cele obronne ma ustawa z dnia 5

grudnia 2024 r. **o ochronie ludności i obro- nie cywilnej**²¹ (dalej: u.o.l.), która ustanawia ramy prawne dla dualnego systemu odporności, funkcjonującego zarówno w czasie pokoju, jak i na wypadek wojny. Przewiduje ona integrację cywilnych łańcuchów dostaw z potrzebami Sił Zbrojnych poprzez wspólne planowanie rezerw, ochronę infrastruktury krytycznej (zwłaszcza paliwowej i transportowej) oraz wymianę informacji o dostępnych zasobach. Jednym z podstawowych celów jest tworzenie warunków do utrzymania ciągłości dostaw towarów, usług i świadczeń (art. 4 ust. 1 pkt 3 lit. g u.o.l.). Newralgiczne znaczenie z perspektywy łańcuchów dostaw mają regulacje dotyczące infrastruktury niezbędnej do realizacji zadań ochrony ludności. Obejmuje ona w szczególności systemy zapewniające dostawy energii elektrycznej, paliw, łączności, usług teleinformatycznych oraz transportu (art. 8 pkt 3 u.o.l.). Utrzymanie ich drożności w czasie pokoju stanowi warunek funkcjonowania logistyki wojskowej. Istotny jest również mechanizm planowania rezerw materiałowych. Ustawodawca zobowiązuje właściwe organy do tworzenia rezerw służących wykonywaniu zadań ochrony ludności (art. 4 ust. 1 pkt 3 lit. e u.o.l.), przy czym zadania te realizuje minister właściwy do spraw wewnętrznych w ramach systemu rezerw strategicznych (art. 15 ust. 1 pkt 11 u.o.l.). U.o.l. znowelizowała ustawę o rezerwach strategicznych, wprowadzając nowy cel tworzenia rezerw, polegający na łagodzeniu zakłóceń ciągłości dostaw służących funkcjonowaniu gospodarki oraz zaspokajaniu podstawowych potrzeb obywateli. Rozwiązanie to wzmacnia stabilność bazy przemysłowo-technologicznej państwa. Znaczenie tej ustawy dla systemu obronnego uwidacznia się również w mechanizmie finansowania. Zgodnie z art. 155 ust. 4 u.o.l. Minister Obrony Narodowej, na etapie opracowywania projektu ustawy budżetowej, wyodrębnia z części środków przeznaczonych na potrzeby obronne – ustalanych co najmniej na poziomie 3% PKB zgodnie z art. 40 ust. 1 pkt 2 u.o.o. – środki na realizację zadań ochrony ludności o charakterze obronnym, określone w Programie Ochrony Ludności i Obrony Cywilnej.

Oznacza to, że część budżetu obronnego jest przeznaczana na wzmacnianie cywilnych ogniw łańcuchów dostaw, w tym na rozwój infrastruktury magazynowej oraz modernizację systemów teleinformatycznych. Ponadto, ustawa wprowadza mechanizm ewidencjonowania zasobów w Centralnej Ewidencji Zasobów Ochrony Ludności i Obrony Cywilnej (art. 23 ust. 1 oraz art. 24 ust. 1 u.o.l.), do której dostęp posiadają również Siły Zbrojne (art. 31 ust. 1 pkt 2 u.o.l.). Umożliwia to wojskowym organom logistycznym precyzyjne mapowanie dostępnych cywilnych zasobów transportowych i materiałowych w kraju.

Kolejny filar zabezpieczenia odporności państwa oraz ciągłości funkcjonowania łańcuchów dostaw stanowi ustawa z dnia 17 grudnia 2020 r. **o rezerwach strategicznych**²² (dalej: u.r.s.). Celem tworzenia rezerw strategicznych jest nie tylko wsparcie realizacji zadań w zakresie obronności i ochrony ludności, lecz także bezpośrednie łagodzenie zakłóceń ciągłości dostaw służących funkcjonowaniu gospodarki oraz zaspokajaniu podstawowych potrzeb obywateli (art. 3 u.r.s.). Dzięki szerokiemu zakresowi ustawowego pojęcia rezerw strategicznych przepisy tej ustawy mogą być wykorzystane jako instrument zapewniania zdolności wytwórczych i usługowych niezbędnych dla utrzymania ciągłości łańcuchów dostaw. Możliwość deponowania rezerw u przedsiębiorców, zgodnie z art. 6 u.r.s., prowadzi do dywersyfikacji ryzyka ich utraty w przypadku zdarzeń dotyczących infrastruktury magazynową pozostającą w dyspozycji Rządowej Agencji Rezerw Strategicznych (RARS). Podstawą tworzenia rezerw strategicznych jest Rządowy Program Rezerw Strategicznych (art. 8 u.r.s.). Z perspektywy przemysłu obronnego istotne znaczenie ma rozdział 5a u.r.s., regulujący tworzenie rezerw nieobjętych rządowym Programem Rezerw Strategicznych, lecz służących realizacji zadań określonych w Planie zabezpieczenia potrzeb Sił Zbrojnych. Takie rezerwy strategiczne są tworzone decyzją ministra właściwego do spraw wewnętrznych i mogą być deponowane bezpośrednio u przedsiębiorcy, na którego potrzeby zostały one utwo-

21 Dz. U. z 2024 r., poz. 1907.

22 Dz. U. z 2024 r. poz. 1598 ze zm.

rzony, i na jego koszt, co pozwala zwiększyć efektywność łańcucha logistycznego w razie uruchomienia takich rezerw.

Rozszerzenie reżimu rezerw strategicznych zakłada ustawa dnia 16 lutego 2007 r. **o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym**²³ (dalej: u.z.r.p.n.g.) wraz z rozporządzeniem Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 12.02.2003 r. **w sprawie zapasów paliw w przedsiębiorstwach energetycznych**²⁴. System bezpieczeństwa paliwowego państwa, jako element odporności łańcuchów dostaw, opiera się na dualistycznym modelu zapasów interwencyjnych, obejmującym zapasy obowiązkowe – tworzone i finansowane przez producentów i handlowców – oraz zapasy agencyjne utrzymywane przez RARS. Łączna wielkość tych zapasów musi odpowiadać co najmniej 90 dniom średniego dziennego przywozu netto ekwiwalentu ropy naftowej. Finansowanie zapasów agencyjnych odbywa się poprzez system opłaty zapasowej uiszczanej przez podmioty rynkowe na Fundusz Zapasów Interwencyjnych. Obowiązek utrzymywania zapasów obowiązkowych ropy naftowej, paliw, a także gazu spoczywa na producentach. Poziom zapasów gazu ziemnego określono jako równoważny co najmniej 30 dniom średniego dziennego przywozu (art. 3 ust. 3 u.z.r.p.n.g.). Przedsiębiorcy są zobowiązani do bieżącego raportowania Prezesowi RARS danych o stanie zapasów.

Zabezpieczeniu łańcuchów dostaw na potrzeby obronności – w wymiarze administracyjno-operacyjnym, fizycznym oraz cyfrowym – służą również przepisy ustawy z dnia 26 kwietnia 2007 r. z dnia 26 kwietnia 2007 r. **o zarządzaniu kryzysowym**²⁵ (dalej: u.z.k.). **Zarządzanie kryzysowe** stanowi element kierowania bezpieczeństwem narodowym i obejmuje działania polegające na zapobieganiu sytuacjom kryzysowym, przy-

gotowaniu do przejścia nad nimi kontroli, reagowaniu na ich wystąpienie, usuwaniu skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej (art. 2 u.z.k.). Elementem zarządzania kryzysowego jest ochrona infrastruktury krytycznej, definiowanej w art. 3 pkt 2 u.z.k. jako systemy obiektów – w tym obiektów budowlanych, urządzeń, instalacji oraz usług – kluczowych dla bezpieczeństwa państwa i jego obywateli, a także dla zapewnienia sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. Infrastruktura ta obejmuje w szczególności systemy zaopatrzenia w energię, surowce energetyczne i paliwa, systemy łączności oraz systemy zaopatrzenia w żywność i inne dobra podstawowe. Za ochronę infrastruktury krytycznej, w tym utrzymanie zdolności rezerwowych do czasu jej pełnego odtworzenia, odpowiadają jej właściciele i posiadacze (art. 6 ust. 5 u.z.k.). Minimalizuje to ryzyko przerwania dostaw surowców i usług logistycznych niezbędnych dla bazy przemysłowo-obronnej.

Filarem zabezpieczenia cyfrowych ogniw łańcuchów dostaw jest ustawa z dnia 5 lipca 2018 r. **o krajowym systemie cyberbezpieczeństwa**²⁶ (dalej: u.k.s.c.) określająca m.in. strukturę i zadania zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT). Z perspektywy łańcuchów dostaw na potrzeby obronności kluczowe znaczenie powierzenie CSIRT MON koordynacji obsługi incydentów zgłaszanych przez przedsiębiorców realizujących zadania na rzecz Sił Zbrojnych. Warto zwrócić uwagę na rygorystyczny system raportowania incydentów do CSIRT MON przez podmioty kluczowe i podmioty ważne w rozumieniu ustawy (art. 11 ust. 1 u.k.s.c.). Tworzy to mechanizm wczesnego ostrzegania przed zagrożeniami dla obronnych łańcuchów dostaw, którego centralnym elementem operacyjnym jest CSIRT MON. Ponadto podstawowym obowiązkiem przedsiębiorców realizujących zadania na rzecz Sił Zbrojnych jest wdrożenie systemu zarządzania bezpieczeństwem informacji zapewniającego bezpieczeństwo

23 Dz. U. z 2024 r. poz. 1281 ze zm.

24 Dz. U. z 2023 r. poz. 2002 ze zn.

25 Dz. U. z 2023 r. poz. 122 ze zm.

26 Dz. U. z 2026 r. poz. 20 ze zm.

i ciągłość łańcucha dostaw produktów, usług i procesów ICT. Obliguje to do systematycznego szacowania ryzyka z uwzględnieniem podatności dostawców oraz ogólnej jakości dostarczanych rozwiązań technologicznych (art. 8 ust. 2 u.k.s.c.). Z perspektywy zabezpieczenia dostaw wojskowych istotna jest procedura uznawania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, wszczynana przez ministra właściwego do spraw informatyzacji w celu ochrony bezpieczeństwa państwa (art. 67b ust. 1 u.k.s.c.). Wydanie decyzji – poprzedzone analizą zagrożeń ekonomicznych i wywiadowczych oraz opinią Kolegium do Spraw Cyberbezpieczeństwa – skutkuje zakazem nabywania oraz obowiązkiem wycofania produktów danego dostawcy w określonym terminie, wynoszącym co do zasady siedem lat, a w przypadku funkcji krytycznych dla sieci – cztery lata (art. 67b ust. 11 oraz art. 67c ust. 1 i 2 u.k.s.c.). Integralność cyfrową łańcuchów dostaw zapewnia również instytucja polecenia zabezpieczającego, umożliwiającą ministrowi właściwemu do spraw informatyzacji wydanie natychmiastowego zakazu korzystania z określonych produktów ICT lub nakazu zastosowania określonych środków technicznych w razie wystąpienia incydentu krytycznego (art. 67g ust. 1 oraz ust. 10 pkt 6 u.k.s.c.).

Identyfikowalności, kontroli oraz kształtowaniu przepływów materiałowych i technologicznych o przeznaczeniu wojskowym lub podwójnego zastosowania służy złożony reżim regulacyjny obejmujący zarówno prawo krajowe, jak i prawo Unii Europejskiej. Podstawowe znaczenie mają przepisy ustawy z dnia 13 czerwca 2019 r. **o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią**

o przeznaczeniu wojskowym lub policyjnym²⁷ oraz ustawy z dnia 29 listopada 2000 r. **o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa oraz dla utrzymania międzynarodowego pokoju i bezpieczeństwa (dalej: u.o.z.t.)**²⁸, wraz z aktami wykonawczymi, implementuje rozwiązania wynikające z dyrektywy 2009/43/WE²⁹ oraz zapewnia stosowanie rozporządzenia (UE) 2021/821 (Dual-Use Regulation)³⁰. Przepisy te kształtują kompleksowy reżim kontroli obrotu uzbrojeniem oraz produktami podwójnego zastosowania. W odniesieniu do produktów podwójnego zastosowania znaczenie mają również przepisy **ustawy z dnia 21 czerwca 2002 r. o materiałach wybuchowych przeznaczonych do użytku cywilnego**³¹ oraz dyrektywy (UE) 2014/28/UE (*Civil Explosives Directive*)³². Reżim ten zakłada rozdzielanie sfery cywilnej i wojskowej. W warunkach rosnącego znaczenia towarów o podwójnym zastosowaniu taka konstrukcja może generować ryzyka operacyjne na styku obu reżimów regulacyjnych. Przejście komponentów, technologii i usług pomiędzy reżimem cywilnym i wojskowym może prowadzić do niejednołitości standardów nadzorczych, luk w identyfikowalności lub opóźnień wynikających z konieczności stosowania odmiennych procedur administracyjnoprawnych.

Specyficzny mechanizm powiązania potencjału krajowego przemysłu obronnego z procesem modernizacji technicznej Sił Zbrojnych wprowadza ustawa z dnia 7 października 1999 r. **o wspieraniu restrukturyzacji przemysłowego potencjału obronnego i modernizacji technicznej Sił Zbrojnych Rzeczypospolitej Polskiej (dalej: u.w.r.p.)**³³. Ustawa przewiduje przeznaczanie środków pochodzących z gospodarowania majątkiem

27 Dz. U. z 2023 r. poz. 1743.

28 Dz. U. z 2023 r. poz. 1582.

29 Dyrektywa Parlamentu Europejskiego i Rady 2009/43/WE z dnia 6 maja 2009 r. w sprawie uproszczenia warunków transferów produktów związanych z obronnością we Wspólnocie, Dz. U. UE. L. z 2009 r. Nr 146, str. 1 z zm.

30 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/821 z dnia 20 maja 2021 r. ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania, Dz. Urz. UE L 206 z 11.06.2021, s. 1, ze zm.

31 Dz. U. z 2022 r. poz. 2378.

32 Dyrektywa Parlamentu Europejskiego i Rady 2014/28/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku i kontroli materiałów wybuchowych przeznaczonych do użytku cywilnego, Dz. U. z 2022 r. poz. 2378.

33 Dz. U. z 2020 r. poz. 1663 ze zm.

Skarbu Państwa, w tym z prywatyzacji przedsiębiorstw sektora obronnego, na restrukturyzację sektora obronnego oraz finansowanie zakupów uzbrojenia i modernizacji technicznej wojska (art. 5, 5a i 7 u.w.r.p.). Mechanizm opiera się na założeniu sprzężenia zwrotnego pomiędzy popytem generowanym przez zamówienia publiczne Sił Zbrojnych a rozwojem krajowego przemysłu obronnego. Zamówienia pełnią nie tylko funkcję zakupową, ale również stymulują modernizację przedsiębiorstw i mogą służyć wzmacnianiu zdolności produkcyjne oraz stabilizacji krajowych ogniw łańcuchów dostaw.

1.2.2. Kontekst Unii Europejskiej

Polska uczestniczy w pogłębionej współpracy wojskowej w ramach Stałej Współpracy Strukturalnej (*Permanent Structured Cooperation* – PESCO), ustanowionej na podstawie art. 42 ust. 6 i art. 46 Traktatu o Unii Europejskiej³⁴ (dalej: TUE). Umożliwia to realizację wspólnych przedsięwzięć w zakresie rozwoju zdolności obronnych. Koordynacja współpracy w obszarze zdolności wojskowych jest wspierana przez Europejską Agencję Obrony (*European Defence Agency* – EDA).

Zgodnie z art. 4 ust. 2 TUE³⁵ (WPZiB), w tym stopniowego kształtowania wspólnej polityki obronnej, której częścią jest Wspólna Polityka Bezpieczeństwa i Obrony (dalej: WPBiO). Ramy prawne wyznaczają przepisy tytułu V TFUE (art. 42 i n.). WPZiB nie funkcjonuje w izolacji, lecz jest powiązana z innymi politykami unijnymi. Do przemysłu obronnego znajdują zastosowanie ogólne reguły prawa unijnego, w tym zasady rynku wewnętrznego, ochrony konkurencji, kontroli pomocy państwa, zamówień publicznych oraz wspólnej polityki handlowej wobec państwa. Art. 346 ust. 1 Traktatu o funkcjonowaniu Unii Eu-

ropejskiej³⁶ (dalej: TFUE) pozostawia jednak istotny zakres swobody państw członkowskich UE w obszarze bezpieczeństwa. Przepis ten uprawnia państwa członkowskie do podejmowania środków niezbędnych do ochrony podstawowych interesów bezpieczeństwa w odniesieniu do produkcji i handlu bronią, amunicją oraz materiałami wojennymi. Środki te nie mogą jednak zakłócać konkurencji w odniesieniu do produktów, które nie mają wyłącznie wojskowego przeznaczenia, dlatego istotne znaczenie ma wykaz broni, amunicji i materiałów wojennych zawarty w decyzji Rady 255/58³⁷. Unijne traktaty i prawo pochodne przewidują również inne klauzule ochronne odnoszące się do bezpieczeństwa publicznego, obronności oraz podstawowych interesów państw członkowskich³⁷.

Sektor obronny pozostaje objęty ogólnym reżimem pomocy publicznej państwa (art. 107 i n. TFUE). Oznacza to, że wsparcie ekonomiczne przedsiębiorstw sektora obronnego nie może zakłócać konkurencji na rynku wewnętrznym, chyba że zostanie uznane za zgodne z tym rynkiem przez Komisję Europejską (KE). Ocena dopuszczalności środków pomocowych dokonywana przez KE uwzględnia jednak funkcję pomocy w obszarze bezpieczeństwa i obronności, m.in. w zakresie wzmocnienia odporności krytycznych łańcuchów dostaw w obszarze produktów podwójnego zastosowania i obronności³⁸.

Przemysłu obronnego i tworzenia w nim łańcuchów dostaw dotyczą bezpośrednio: dyrektywa 2009/81/WE dotycząca zamówień w dziedzinach obronności i bezpieczeństwa³⁹ (DSPD), dyrektywa 2009/43/WE w sprawie transferów produktów związanych z obronnością (ICT)⁴⁰, rozporządzenie (UE) 2024/1252 na rzecz zapewnienia bezpiecznych i zrównoważonych dostaw surowców krytycznych (CR-

34 Dz. U. z 2004 r. Nr 90, poz. 864/30 ze zm.

35 Dz. U. z 2004 r. Nr 90, poz. 864/2 ze zm.

36 Decyzja Rady w sprawie ustalenia listy produktów (broń, amunicja i materiały wojenne), do których odnoszą się przepisy art. 223 ust. 1 lit. b) - obecnie art. 346 ust. 1 lit. b) - Traktatu (dok. 255/58). Protokół z 15.04.1958 r.: dok. 368/58.

37 Zob. np. art. 36 i art. 72 TFUE, art. 2 ust. 3 rozporządzenia (WE) nr 1907/2006.

38 Komunikacie Komisji „Wytyczne Unii w sprawie pomocy państwa na rzecz promowania inwestycji w zakresie finansowania ryzyka” (2021/C 508/01), pkt. 164, lit. i.

39 Dyrektywa Parlamentu Europejskiego i Rady 2009/81/WE z 13.07.2009 r. w sprawie koordynacji procedur udzielania niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa i zmieniająca dyrektywy 2004/17/WE i 2004/18/WE (Dz. U. UE. L. z 2009 r. Nr 216, str. 76 ze zm.).

40 Dyrektywa Parlamentu Europejskiego i Rady 2009/43/WE z 6.05.2009 r. w sprawie uproszczenia warunków transferów produktów związanych z obronnością we Wspólnocie (Dz. U. UE. L. z 2009 r. Nr 146, str. 1 ze zm.).

MA)⁴¹, rozporządzenie (UE) 2021/821 dotyczące kontroli produktów podwójnego zastosowania (*EU Dual-Use Regulation*)⁴². W związku z Europejską Strategią Przemysłu Obronnego (*European Defence Industrial Strategy* – EDIS)⁴³, ukierunkowaną na wzmocnienie do 2035 r. europejskiej bazy technologiczno-przemysłowej sektora obronnego (*European Defence Technological and Industrial Base* – EDTIB), uchwalono sektorowe i horyzontalne akty unijne, takie jak: rozporządzenie (UE) 2025/2643 ustanawiające Program na rzecz europejskiego przemysłu obronnego⁴⁴ (EDIP), rozporządzenie (UE) 2021/697 ustanawiające Europejski Fundusz Obronny⁴⁵ (EDF), rozporządzenie (UE) 2025/1106 ustanawiające Instrument na rzecz Zwiększenia Bezpieczeństwa Europy⁴⁶ („SAFE”).

Unijne ramy prawne dla rozwoju technologii strategicznych i odporności gospodarczej wyznaczają m.in. rozporządzenie (UE) 2024/2747 ustanawiające ramy środków dotyczących sytuacji nadzwyczajnej na rynku wewnętrznym (IMERA)⁴⁷, rozporządzenie

(UE) 2024/795 ustanawiające Platformę na rzecz Technologii Strategicznych dla Europy (STEP)⁴⁸, rozporządzenie (UE) 2023/1781 w sprawie półprzewodników (ECA)⁴⁹, rozporządzenie (UE) 2021/887 ustanawiające Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC)⁵⁰. W kontekście odporności cyfrowej szczególną rolę pełni rozporządzenie (UE) 2025/38 w sprawie tzw. cybersolidarności (CySA)⁵¹, wzmacniające zdolności Unii w zakresie wykrywania incydentów cybernetycznych. Funkcję prewencyjnego mechanizmu ochronnego dla EDTIB rozporządzenie (UE) 2019/452 służące monitorowaniu bezpośrednich inwestycji zagranicznych (BIZ)⁵².

-
- 41 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1252 z 11.04.2024 r. w sprawie ustanowienia ram na potrzeby zapewnienia bezpiecznych i zrównoważonych dostaw surowców krytycznych oraz zmiany rozporządzeń (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1724 i (UE) 2019/1020 Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1252 ze zm.).
- 42 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/821 z 20.05.2021 r. ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania (wersja przekształcona) (Dz. U. UE. L. z 2021 r. Nr 206, str. 1 ze zm.).
- 43 Wspólny komunikat Komisji Europejskiej i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 5.03.2024 r., Nowa strategia na rzecz europejskiego przemysłu obronnego: osiągnięcie gotowości UE dzięki zdolnemu do reagowania i odpornemu europejskiemu przemysłowi obronnemu, JOIN(2024) 10 final. Więcej informacji na ten temat dostępnych jest na stronie Komisji Europejskiej: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-or-common-defence-industrial-strategy_en (data dostępu: 30.04.2026 r.).
- 44 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/2643 z 16.12.2025 r. w sprawie ustanowienia Programu na rzecz europejskiego przemysłu obronnego oraz ram środków w celu zapewnienia terminowej dostępności i terminowych dostaw produktów związanych z obronnością („rozporządzenie w sprawie EDIP”) (Dz. U. UE. L. z 2025 r. poz. 2643).
- 45 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/697 z 29.04.2021 r. ustanawiające Europejski Fundusz Obronny i uchylające rozporządzenie (UE) 2018/1092 (Dz. U. UE. L. z 2021 r. Nr 170, str. 149 z późn. zm.).
- 46 Rozporządzenie Rady (UE) 2025/1106 z 27.05.2025 r. ustanawiające Instrument na rzecz Zwiększenia Bezpieczeństwa Europy („instrument SAFE”) poprzez Wzmocnienie Europejskiego Przemysłu Obronnego (Dz. U. UE. L. z 2025 r. poz. 1106 ze zm.).
- 47 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2747 z 9.10.2024 r. w sprawie ustanowienia ram środków dotyczących sytuacji nadzwyczajnej na rynku wewnętrznym i odporności rynku wewnętrznego (...) (Dz. U. UE. L. z 2024 r. poz. 2747).
- 48 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/795 z 29.02.2024 r. w sprawie ustanowienia Platformy na rzecz Technologii Strategicznych dla Europy (STEP) oraz zmiany dyrektywy 2003/87/WE (...) (Dz. U. UE. L. z 2024 r. poz. 795 ze zm.).
- 49 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1781 z 13.09.2023 r. w sprawie ustanowienia ram dotyczących środków na rzecz wzmocnienia europejskiego ekosystemu półprzewodników oraz zmiany rozporządzenia (UE) 2021/694 (akt w sprawie czipów) (Dz. U. UE. L. z 2023 r. Nr 229, str. 1).
- 50 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/887 z 20.05.2021 r. ustanawiające Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji (Dz. U. UE. L. z 2021 r. Nr 202, str. 1).
- 51 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z 19.12.2024 r. w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie cyberzagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności) (Dz. U. UE. L. z 2025 r. poz. 38 z późn. zm.).
- 52 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/452 z dnia 19 marca 2019 r. ustanawiające ramy monitorowania bezpośrednich inwestycji zagranicznych w Unii (Dz. U. UE. L. z 2019 r. poz. 79 z późn. zm.).

1.3. Analiza wsparcia administracji państwowej

Instrumentarium administracji publicznej w obszarze zabezpieczania i organizacji łańcuchów dostaw przemysłu obronnego tworzy wielopoziomowy system, integrujący kompetencje organów krajowych oraz instytucji Unii Europejskiej. Jego podstawę stanowią dyrektywy konstytucyjne dotyczące ochrony niepodległości (art. 5 Konstytucji RP) w korelacji z unijnymi ramami ochrony podstawowych interesów bezpieczeństwa państw członkowskich (art. 346 ust. 1 lit. b TFUE). Struktura instytucjonalna na poziomie krajowym jest scentralizowana wokół Rady Ministrów, która odpowiada za prowadzenie bieżącej polityki obronnej (art. 146 ust. 2 Konstytucji RP). Prezes Rady Ministrów dysponuje kompetencją do wydawania wiążących poleceń przedsiębiorcom w celu zapewnienia funkcjonowania infrastruktury krytycznej (art. 7a ust. 1 ustawy o zarządzaniu kryzysowym) oraz do uruchamiania Planu zabezpieczenia potrzeb Sił Zbrojnych (art. 654 ust. 1 u.o.O.). Kluczową rolę operacyjną pełni Minister Obrony Narodowej (MON), który nakłada na przedsiębiorców obowiązki utrzymywania mocy produkcyjnych i naprawczych (art. 648 ust. 1 u.o.O.), zarządza wykazem jednostek przewidzianych do militaryzacji (art. 601 ust. 5 u.o.O.) oraz pełni funkcję organu kontroli przy bezpośrednich inwestycjach zagranicznych w sektorze obronnym (art. 3 ust. 1 pkt 5 lit. c ustawy o kontroli niektórych inwestycji⁵³, dalej: u.k.n.i.). Minister Aktywów Państwowych (MAP) sprawuje nadzór właścicielski nad spółkami strategicznymi, takimi jak Polska Grupa Zbrojeniowa S.A., i posiada kompetencje do blokowania zbywania ich akcji (art. 13 ust. 1 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym⁵⁴, dalej: u.z.m.p.). Ważnym ogniwem wykonawczym jest RARS, nadzorowana przez MSWiA (art. 30 u.r.s.) i realizująca zadania w zakresie gromadzenia zapasów surowców i technologii o przeznaczeniu wojskowym (art. 4 u.r.s.). Na poziomie unijnym architektura organów opiera się na kompetencjach Komisji Europejskiej, która prowadzi politykę ochrony konkurencji na rynku wewnętrznym i oce-

nia plany pomocy publicznej dla przedsiębiorstw (art. 107 TFUE), zarządza Programem na rzecz europejskiego przemysłu obronnego (EDIP) (rozporządzenie 2025/2643) oraz instrumentami wsparcia rynku półprzewodników (rozporządzenie 2023/1781). Organem doradczym i koordynującym w zakresie bezpieczeństwa dostaw jest Rada ds. Bezpieczeństwa Dostaw w Sektorze Obronności (RBDSO) (art. 76 rozporządzenia EDIP), **wspierana przez Europejską Agencję Obrony (EDA), która uczestniczy w procesach certyfikacji i mapowania łańcuchów dostaw (art. 55-56 rozporządzenia 2025/2643). Decyzje o uruchomieniu stanów kryzysowych, umożliwiających interwencję w łańcuchy dostaw, podejmuje Rada Unii Europejskiej na wniosek Komisji (art. 60 i 64 rozporządzenia 2025/2643).**

Głównym instrumentem planistycznym i diagnostycznym administracji krajowej jest **Plan zabezpieczenia potrzeb Sił Zbrojnych** realizowanych przez przedsiębiorców, który zawiera szczegółowy wykaz kooperantów i podwykonawców (krajowych i zagranicznych) dostarczających surowce i komponenty niezbędne do produkcji obronnej (art. 651 u.o.O.). Plan służy identyfikacji „wąskich gardeł” oraz braków, których krajowy przemysł nie jest w stanie zaspokoić, co obliguje MON do sporządzania informacji o alternatywnych źródłach dostaw (art. 656 ust. 1-2 u.o.O.). Na poziomie unijnym analogiczną funkcję pełni mechanizm strategicznego mapowania łańcuchów dostaw, identyfikujący wskaźniki wczesnego ostrzegania o zakłóceniach (art. 56 rozporządzenia 2025/2643) oraz obowiązkowe audyty dużych przedsiębiorstw w zakresie surowców strategicznych (art. 24 rozporządzenia 2024/1252 - CRMA).

Instrumenty **interwencyjne** umożliwiają administracji publicznej bezpośrednią modyfikację relacji rynkowych w sytuacjach zagrożenia. Najdalej idącym mechanizmem są zlecenia i zamówienia priorytetowe (art. 63 i 66 rozporządzenia 2025/2643). Na ich mocy

⁵³ Ustawa z dnia 24 lipca 2015 r. o kontroli niektórych inwestycji (t.j. Dz. U. z 2026 r. poz. 47).

⁵⁴ Dz. U. z 2026 r. poz. 373.

Komisja Europejska może nałożyć na producenta obowiązek realizacji zamówienia istotnego dla bezpieczeństwa z pierwszeństwem przed innymi kontraktami (art. 66 rozporządzenie 2025/2643). W prawie krajowym MON nakłada na wybranych przedsiębiorców obowiązki utrzymywania mocy produkcyjnych, naprawczych lub usługowych na podstawie decyzji administracyjnej i umów (art. 648 ust. 1 pkt 2 u.o.O.). Środkiem o charakterze nadzwyczajnym jest militaryzacja jednostek gospodarczych, polegająca na ich pełnym podporządkowaniu organom administracji rządowej w celu zapewnienia dostaw energii, paliw lub uzbrojenia (art. 600 ust. 2 u.o.O.). Warto również wyróżnić kompetencję Prezesa Rady Ministrów do wydawania poleceń w sytuacji kryzysowej przedsiębiorcom i innym podmiotom z art. 7a u.z.k. Zabezpieczenie materiałowe łańcuchów dostaw realizowane jest przez system rezerw strategicznych, których celem jest łagodzenie zakłóceń ciągłości dostaw służących funkcjonowaniu gospodarki (art. 3 u.r.s.). Rezerwy te mogą obejmować surowce, maszyny, urządzenia, a także moce produkcyjne i technologie o przeznaczeniu wojskowym (art. 4 u.r.s.). Ustawa umożliwia deponowanie rezerw bezpośrednio u przedsiębiorcy, na którego potrzeby zostały one utworzone, co zapewnia natychmiastową dostępność wkładów produkcyjnych po uruchomieniu Planu zabezpieczenia potrzeb SZ (art. 28a i 28b u.r.s.). Ponadto administracja wykorzystuje mechanizmy wspólnych zakupów surowców strategicznych w celu wzmocnienia pozycji negocjacyjnej unijnych podmiotów (art. 25 CRMA). Wsparcie finansowe i strukturalne dla bazy przemysłowej realizowane jest poprzez fundusze celowe oraz preferencje podatkowe. Rozporządzenie 2025/2643 (EDIP) ustanawia Strukturę na rzecz europejskiego programu zbrojeniowego (SEAP) – podmiot o osobowości prawnej i statusie organizacji międzynarodowej (art. 43 rozporządzenia 2025/2643). SEAP korzysta ze zwolnień z podatku VAT i akcyzy przy nabywaniu produktów obronnych, pod warunkiem zachowania prawa własności do tych produktów.

Dostęp do kapitału dla małych i średnich przedsiębiorców (MŚP) zapewnia Fundusz na rzecz Przyspieszenia Transformacji Łańcuchów Dostaw (FAST) (art. 14 rozporządzenia 2025/2643) oraz Fundusz Wsparcia Sił Zbrojnych zarządzany przez BGK (art. 41 u.o.O.). Utrzymywanie niewykorzystanych w czasie pokoju mocy produkcyjnych przez przedsiębiorców prywatnych jest finansowane z dotacji celowych budżetu państwa (art. 659 u.o.O.). Administracja wymusza również transfer technologii do krajowych podmiotów poprzez mechanizm offsetu przy zamówieniach o podstawowym znaczeniu dla bezpieczeństwa (art. 2 pkt 14 ustawy z dnia 26 czerwca 2014 r. o niektórych umowach zawieranych w związku z realizacją zamówień o podstawowym znaczeniu dla bezpieczeństwa państwa (u.n.u.)⁵⁵.

Kontrola i ochrona ogniw łańcuchów dostaw odbywa się poprzez „filtrację” kapitału, kontrolę obrotu oraz nadzór nad bezpieczeństwem cyfrowym. Organy administracji (MON, MAP) monitorują bezpośrednio inwestycje zagraniczne i mogą blokować przejęcia podmiotów dysponujących infrastrukturą krytyczną lub technologiami strategicznymi przez kapitał z państw trzecich (art. 4 rozporządzenia 2019/452⁵⁶; art. 12b u.k.n.i.). Kontrola wywozu produktów podwójnego zastosowania oraz uzbrojenia reglamentuje zarówno fizyczny eksport, jak i niematerialne transfery technologii (know-how, oprogramowanie) poza obszar celny UE (rozporządzenie 2021/821; u.o.z.t.). W wymiarze cybernetycznym bezpieczeństwo łańcucha dostaw zapewnia CSIRT MON, koordynujący obsługę incydentów u przedsiębiorców realizujących zadania obronne (art. 26 ust. 5 pkt 2 u.k.s.c.). Administracja posiada kompetencję do wykluczenia z łańcucha dostaw produktów ICT pochodzących od tzw. dostawców wysokiego ryzyka (art. 67b u.k.s.c.).

Z punktu widzenia funkcjonowania całego systemu kluczowe znaczenie ma koordynacja. Kompetencje dotyczące rozwoju przemysłu obronnego i bezpieczeństwo dostaw

⁵⁵ Dz. U. z 2022 r. poz. 1218.

⁵⁶ W styczniu 2028 r. zostanie ono zastąpione rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2026/1386 z dnia 17 czerwca 2026 r. w sprawie monitorowania inwestycji zagranicznych w Unii oraz uchylecia rozporządzenia (UE) 2019/452, Dz. U. UE. L. z 2026 r. poz. 1386.

są rozproszone między liczne organy i instytucje. Wielośrodkowy charakter systemu jest uzasadniony wielosektorowością obronnych łańcuchów dostaw, których odporność zależy m.in. od planowania obronnego, zamówień, finansowania, rezerw, infrastruktury, energii, transportu i cyberbezpieczeństwa. Rozproszenie kompetencji może jednak prowadzić do fragmentaryzacji polityki przemysłowo-obronnej. Mimo istniejących mechanizmów koordynacyjnych uzasadnione jest ich dalsze wzmacnianie, tak aby państwo dysponowało pełnym rozpoznaniem zasobów i zależności istotnych dla obronności oraz mogło wykorzystywać je w sposób spójny i przewidywalny.

1.3.1. Agencje państwowe, Bank Gospodarstwa Krajowego i spółki z udziałem Skarbu Państwa

Instrumentami wykorzystywanymi w celu zapewnienia bezpieczeństwa łańcuchów dostaw mogą być agencje państwowe, Bank Gospodarstwa Krajowego (BGK) oraz spółki z udziałem Skarbu Państwa (dalej SPP). Korzystając z tych instrumentów państwo powinno mieć jednak na uwadze przepisy unijne i krajowe dotyczące pomocy publicznej (art. 107 TFUE) oraz ochrony konkurencji.

Elementem sektora publicznego są agencje wykonawcze będące państwowymi osobami prawnymi tworzonymi na podstawie ustaw w celu realizacji zadań państwa (art. 9 pkt 5 i art. 18 ustawy z 27.08.2009 r. o finansach publicznych⁵⁷, dalej: u.f.p.). Agencje te stanowią formę pośredniej administracji gospodarczej w celu realizacji konkretnych zadań państwa (w szczególności działalności interwencyjnej) z bezpośrednim wykorzystaniem środków publicznych. W obszarze obronności i bezpieczeństwa państwa podstawowe znaczenie mają dwie agencje wykonawcze, tj. Agencja Mienia Wojskowego, działająca na podstawie ustawy z 10.07.2015 r. o Agencji Mienia Wojskowego (dalej: AMW)⁵⁸ i nadzorowana przez MON, oraz Rządowa Agencja

Rezerw Strategicznych, działająca na podstawie u.r.s. i podlegająca nadzorowi ministra właściwego do spraw wewnętrznych. RARS jest centralnym organem wykonawczym systemu rezerw strategicznych i odpowiada za utrzymywanie, rotację, realizację decyzji o tworzeniu, udostępnianiu i likwidacji rezerw, a także za kontrolę podmiotów zewnętrznych uczestniczących w tym systemie (art. 31 ust. 1 pkt 1 i 2 oraz art. 48 ust. 1 u.r.s.). RARS wykonuje decyzje ministra właściwego ds. wewnętrznych o utworzeniu rezerw strategicznych, zgodnie z Programem Rezerw Strategicznych. RARS stała się jednym z najważniejszych podmiotów odpowiedzialnych za zabezpieczenie dostaw strategicznych, zarazem jednak pojawiły się wątpliwości dotyczące przejrzystości jej działania, skali kompetencji oraz efektywności wykorzystania środków publicznych.

BGK jest bankiem państwowym (państwową osobą prawną), którego głównym celem jest wspieranie zrównoważonego rozwoju społeczno-gospodarczego Polski, konkurencyjności gospodarki oraz innowacyjności. Do podstawowych celów działalności BGK należy m.in. wspieranie polityki gospodarczej państwa i rządowych programów społeczno-gospodarczych, obejmujących w szczególności projekty infrastrukturalne i związane z rozwojem sektora MŚP (art. 4 ustawy z 14.03.2003 r. o Banku Gospodarstwa Krajowego⁵⁹). BGK jest jedynym akcjonariuszem spółki celowej (SPV) utworzonej na podstawie ustawy z 4.12.2025 r. o szczególnych zasadach realizacji zadań związanych z inwestycją w zakresie bezpieczeństwa i obronności realizowaną w ramach Krajowego Planu Odbudowy i Zwiększania Odporności⁶⁰.

Spółki Skarbu Państwa (dalej SPP) podlegają przepisom Kodeksu spółek handlowych oraz ustawy z 16.12.2016 r. o zasadach zarządzania mieniem państwowym (dalej: u.z.m.p.)⁶¹. Z jednej strony SPP (w szczególności będące spółkami giełdowymi) powinny ukierunkowywać swoją działalność na generowanie

⁵⁷ T.j. Dz.U. z 2025 r., poz. 1483.

⁵⁸ T.j. Dz. U. z 2025 r. poz. 817.

⁵⁹ T.j. Dz.U. z 2026 r., poz. 195.

⁶⁰ Dz.U. z 2025 r., poz. 1846.

⁶¹ Dz. U. z 2026 r. poz. 373.

zysku i zwiększanie swojej wartości dla akcjonariuszy. Z drugiej strony, spółki te mogą być instrumentalizowane do realizacji celów publicznych (w tym z zakresu polityki obronnej i bezpieczeństwa) pod warunkiem, że nie zagraża to ich trwałej rentowności. Państwo oddziałuje na SPP głównie poprzez instrumenty władztwa korporacyjnego, tj. wykonywanie prawa głosu i wpływ na obsadę rady nadzorczej i zarządu. U.z.m.p. określa zasady zarządzania SPP oraz ogranicza możliwość dekompozycji kluczowych ogniw łańcucha dostaw. W szczególności ustawa wprowadza zakaz zbywania akcji spółek o charakterze strategicznym należących do Skarbu Państwa, takich jak Polska Grupa Zbrojeniowa S.A. (art. 13 ust. 1 u.z.m.p.). Jej sztywne regulacje mogą jednak przeszkadzać w rozwoju łańcuchów dostaw, np. utrudniając tworzenie międzynarodowych konsorcjów kapitałowych. Jeszcze dalej idące ograniczenia w dysponowaniu aktywami spółek strategicznych są ograniczenia przewidziane w ustawie z 8.03.2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych⁶² oraz w ustawie z 24.07.2015 r. o kontroli niektórych inwestycji⁶³. Przepisy tej ostatniej ustawy mają na celu ochronę strategicznych polskich spółek przed wrogim przejęciem, tj. nabyciem lub osiągnięciem istotnego uczestnictwa albo nabyciem dominacji nad spółką, przez inwestora, który zagraża porządkowi publicznemu lub bezpieczeństwu publicznemu. Nabycie istotnego uczestnictwa lub dominacji wymaga uprzedniej kontroli przez Ministra Aktywów Państwowych (MAP) względnie MON, który może wyrazić sprzeciw w formie decyzji administracyjnej. Nabycie akcji lub udziałów wbrew wymogom określonym w tej ustawie jest nieważne.

Nowe systemowe podejście tworzenia odpornych i elastycznych łańcuchów dostaw

przejawia się w działaniach MAP podejmowanych w celu do wspierania komponentu krajowego (*local content*) w tych łańcuchach, tak, aby uczynić je mniej podatnymi na zawirowania geopolityczne i presję cenową. Komponent krajowy to wartość towarów lub usług wyprodukowanych lub świadczonych przez podmiot krajowy. MAP oddziałuje na politykę przetargową i zamówieniową SPP w celu wzmacniania tego komponentu, czego wyrazem jest opracowanie i przyjęcie „Dobrych Praktyk w zakresie zwiększenia przez spółki z udziałem Skarbu Państwa udziału komponentu krajowego w kluczowych procesach inwestycyjnych”⁶⁴. W dokumencie tym określono kryteria (wraz z przypisaniem im wag procentowych) służących ocenie poziomu krajowości podmiotów, które mają zostać włączone w łańcuchy dostaw SPP.

1.3.2. Współpraca sektora publicznego z sektorem prywatnym (zamówienia publiczne, partnerstwo publiczno-prywatne i umowy offsetowe)

Współpraca sektora publicznego z sektorem prywatnym w obszarze obronności i bezpieczeństwa państwa zyskuje na znaczeniu w warunkach rosnących zagrożeń geopolitycznych, intensyfikacji procesów modernizacyjnych sił zbrojnych oraz konieczności szybkiej absorpcji innowacji. Państwo, pozostając gwarantem bezpieczeństwa i podmiotem odpowiedzialnym za realizację zadań o charakterze strategicznym, coraz częściej sięga po kompetencje, zasoby oraz zdolności organizacyjno-techniczne podmiotów prywatnych.

Dyrektywa 2009/81/WE⁶⁵ ma na celu stworzenie wyspecjalizowanego reżimu proceduralnego, który eliminuje niepewność prawa, wzmacnia uczciwą konkurencję, a zarazem respektuje konieczne wyjątki w sytuacjach wymagających szczególnej ochrony informacji lub zabezpieczenia ciągłości dostaw. Dyrektywa ta wprowadza zharmonizowa-

62 T.j. Dz. U. z 2020 r. poz. 2173.

63 Dz.U. z 2017 r. poz. 1857.

64 <https://www.gov.pl/web/aktywa-panstwowe/local-content-z-korzyscia-dla-polski-wspieramy-krajowe-firmy-budujemy-gospodarke>

65 Dyrektywa Parlamentu Europejskiego i Rady 2009/81/WE z 13.07.2009 r. w sprawie koordynacji procedur udzielania niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa i zmieniająca dyrektywy 2004/17/WE i 2004/18/WE (Dz. U. UE. L. z 2009 r. Nr 216, str. 76 ze zm.).

ne ramy prawne dla zamówień na produkty wojskowe, sprzęt i usługi na potrzeby bezpieczeństwa, a także roboty budowlane bezpośrednio związane z obronnością i bezpieczeństwem. Przewiduje przy tym specyficzne rozwiązania w odniesieniu do ochrony informacji niejawnych i wymogów bezpieczeństwa dostaw. Jej rdzeniem jest mechanizm równowagi między zasadami rynku wewnętrznego a specyfiką zamówień strategicznych, osiągnięty przez selektywne stosowanie procedur konkurencyjnych, rozbudowane możliwości negocjacyjne oraz szczególne przesłanki wyłączeń w sprawach o istotnym znaczeniu dla bezpieczeństwa.

Ustawa PZP z 2019 r.⁶⁶ implementuje dyrektywę 2009/81/WE wyodrębniając regulacje dotyczące **zamówień w dziedzinach obronności i bezpieczeństwa** oraz dostosowując ogólne zasady udzielania zamówień do specyfiki tych zamówień. W szczególności określono, iż zamawiający może udzielić zamówienia w dziedzinach obronności i bezpieczeństwa w trybie przetargu ograniczonego lub negocjacji z ogłoszeniem, natomiast w trybie dialogu konkurencyjnego, negocjacji bez ogłoszenia lub zamówienia z wolnej ręki w przypadkach określonych przepisami ustawy. Uwzględniono potrzebę zachowania poufności i elastyczności negocjacyjnej w projektach, w których zasadnicze znaczenie mają warunki techniczne, bezpieczeństwo dostaw oraz zdolność wykonawcy do ochrony informacji niejawnych.

Ustawa z 26.06.2014 r. o niektórych umowach zawieranych w związku z realizacją zamówień o podstawowym znaczeniu dla bezpieczeństwa państwa⁶⁷ stanowi unikalny w polskim systemie prawnym instrument pozwalający państwu na **precyzyjne regulowanie relacji z podmiotami prywatnymi** realizującymi zadania o szczególnej doniosłości dla bezpieczeństwa narodowego. Akt ten został uchwalony jako odpowiedź na konieczność zabezpieczenia krajowych zdolności przemysłowych w obszarze obronności, a także jako narzędzie zwiększające odporność państwa w potencjalnych sy-

tuacjach kryzysowych, w których rynek nie jest w stanie zapewnić wymaganej ciągłości dostaw lub usług. Offset jest kooperacją między Skarbem Państwa i offsetobiorcą a zagranicznym dostawcą konieczną do utrzymania lub ustanowienia na terytorium Rzeczypospolitej Polskiej potencjału w zakresie zdolności produkcyjnych, serwisowych i obsługowo-naprawczych, a także innych, niezbędnych z punktu widzenia ochrony podstawowych interesów bezpieczeństwa państwa, polegającą w szczególności na przekazaniu technologii, know-how wraz z przeniesieniem autorskich praw majątkowych lub korzystania z utworu na podstawie udzielonej licencji w celu zapewnienia wymaganej przez Skarb Państwa niezależności od zagranicznego dostawcy. Zagraniczny dostawca zawiera umowę offsetową na zasadach określonych w ustawie offsetowej i żadna ze stron nie może odstąpić od umowy offsetowej. Umowa offsetowa to umowa zawarta między Skarbem Państwa a zagranicznym dostawcą, określająca w szczególności wartość, przedmiot i harmonogram wykonania zobowiązań offsetowych oraz warunki, na jakich te zobowiązania mają być wykonane, mająca na celu ochronę podstawowych interesów bezpieczeństwa państwa zgodnie z art. 346 ust. 1 lit. b TFUE. **Ustawa o PPP z 2008 r.**⁶⁸ wprowadza model współpracy, w którym podział ryzyk oraz wynagrodzenia kształtowany jest w sposób kontraktowy, pozwalając państwu wykorzystywać kapitał, know-how i efektywność operacyjną sektora prywatnego. W obszarze obronności i bezpieczeństwa PPP może znaleźć zastosowanie przede wszystkim w przedsięwzięciach infrastrukturalnych, takich jak budowa i utrzymanie obiektów technicznych, centrów szkoleniowych, zaplecza logistycznego czy infrastruktury teleinformatycznej. Możliwe są również projekty dotyczące bezpieczeństwa cyfrowego i cyberbezpieczeństwa, w których kluczowe znaczenie ma dostęp do najnowszych rozwiązań technologicznych oraz elastyczność w świadczeniu usług w długich horyzontach. Równocześnie tworzenie partnerstw w obszarze wrażliwym wymaga szczególnego ukształtowania klau-

⁶⁶ t.j. Dz.U. z 2024 r., poz. 1320 ze zm.

⁶⁷ t.j. Dz.U. z 2022 r., poz. 1218 ze zm.

⁶⁸ j. Dz.U. z 2023 r., poz. 1637 ze zm.

zul dotyczących ochrony informacji niejawnych, bezpieczeństwa dostaw, kontroli nad podwykonawcami i nadzoru państwowego nad infrastrukturą krytyczną. Kluczowe jest precyzyjne rozłożenie ryzyk oraz utrzymanie możliwości interwencji publicznej w sytuacjach nadzwyczajnych.

Ustawa o koncesji z 2016 r.⁶⁹ uzupełnia katalog możliwych rozwiązań o model, w którym wynagrodzenie wykonawcy pochodzi zasadniczo z prawa eksploatacji obiektu lub świadczenia usług, a ryzyko ekonomiczne w projekcie spoczywa w przeważającej mierze na koncesjonariuszu. W sektorze obronności i bezpieczeństwa koncesja może mieć zastosowanie węższe niż PPP, z uwagi na ograniczoną możliwość komercjalizacji świadczeń i szczególnie status infrastruktury. Może jednak sprawdzić się w określonych niszach, na przykład w przedsięwzięciach dotyczących infrastruktury okołowojskowej, w obszarze usług logistycznych, ochrony i utrzymania obiektów, modernizacji niektórych elementów zaplecza technicznego lub w specyficznych przedsięwzięciach o mieszanym charakterze cywilno-wojskowym. Również w tym modelu niezbędne jest zapewnienie zgodności z wymogami ochrony informacji oraz zabezpieczeń operacyjnych, a także dostosowanie alokacji ryzyk do wymogów bezpieczeństwa.

Zagadnieniem o zasadniczym znaczeniu pozostaje **relacja krajowych przepisów do art. 346 TFUE**. Przepis ten pozwala państwu członkowskiemu na przyjęcie środków, które uznają za konieczne dla ochrony podstawowych interesów bezpieczeństwa, w szczególności w zakresie produkcji broni, amunicji i materiałów wojennych. Powoływanie się na art. 346 TFUE jest możliwe wyłącznie w odniesieniu do ściśle ograniczonych, wyjątkowych przypadków. Wymaga to każdorazowo przeprowadzenia szczegółowej analizy zasadności jego zastosowania, w tym analizy pod kątem zgodności z zasadą proporcjonalności. Państwo członkowskie, które chce skorzystać z możliwości odstępstwa od przepisów Traktatu, ma obowiązek wykazać, że ochrona podstawowych interesów jego bezpieczeństwa nie może zostać równie

skutecznie zagwarantowana w inny sposób, zwłaszcza poprzez zastosowanie przepisów dyrektywy 2009/81/WE (w Polsce, Działu VI ustawy PZP). Ponadto, środki te nie mogą negatywnie wpływać na warunki konkurencji na rynku wewnętrznym w odniesieniu do produktów, które nie są przeznaczone wyłącznie do celów wojskowych.

Przepisów ustawy PZP nie stosuje się zatem w zakresie, w jakim ochrona istotnych interesów bezpieczeństwa państwa nie może zostać zagwarantowana w inny sposób, w szczególności z zastosowaniem przepisów działu VI „Zamówienia w dziedzinach obronności i bezpieczeństwa”. Dotyczy to zamówień lub konkursów którym nadano klauzulę zgodnie z przepisami ustawy z 5.08.2010 r. o ochronie informacji niejawnych⁷⁰ lub którym muszą towarzyszyć, na podstawie odrębnych przepisów, szczególne środki bezpieczeństwa lub jeżeli wymaga tego istotny interes bezpieczeństwa państwa. Wyłączenie obejmuje również zamówienia dotyczące produkcji lub handlu bronią, amunicją lub materiałami wojennymi, o których mowa w art. 346 TFUE, jeżeli wymaga tego podstawowy interes bezpieczeństwa państwa, a udzielenie zamówienia bez zastosowania ustawy nie wpłynie negatywnie na warunki konkurencji na rynku wewnętrznym w odniesieniu do produktów, które nie są przeznaczone wyłącznie do celów wojskowych.

Z perspektywy współpracy publiczno-prywatnej dyrektywa 2009/81/WE promuje otwarcie zamówień wrażliwych na dostawców z całej Unii, jeśli tylko pozwala na to ich charakter, a wymagania w zakresie poufności, bezpieczeństwa łańcucha dostaw i kontroli pochodzenia produktów mogą być zapewnione w trybach przewidzianych przez prawo zamówień. Instrumenty przewidziane przez dyrektywę 2009/81/WE, takie jak dialog konkurencyjny, kryteria kwalifikacji dotyczące zdolności w zakresie bezpieczeństwa czy kontrole podwykonawstwa, umożliwiają zamawiającym precyzyjne ukształtowanie wymagań wobec wykonawców oraz zarządzanie ryzykiem w całym cyklu realizacji zamówienia.

69 t.j. Dz.U. z 2025 r., poz. 1688

70 t.j. Dz.U. z 2025 r., poz. 1209.

1.4. Wnioski i rekomendacje

Wnioski

Bezpieczeństwo łańcuchów dostaw przemysłu obronnego jest jednym z warunków utrzymania zdolności operacyjnych Sił Zbrojnych. Zarządzanie tymi łańcuchami **powinno zapewniać równowagę między efektywnością działania w czasie pokoju a możliwością szybkiego zwiększenia produkcji, dostaw i usług w sytuacji kryzysu, mobilizacji lub wojny**. W odniesieniu do zasobów krytycznych odporność i ciągłość działania powinny mieć pierwszeństwo przed doraźną optymalizacją kosztową.

Polski system prawny przewiduje szeroki katalog instrumentów służących zabezpieczeniu łańcuchów dostaw. Obejmuje on w szczególności militaryzację, świadczenia na rzecz obrony, zadania nakładane na przedsiębiorców, utrzymywanie zdolności produkcyjnych, rezerwy strategiczne, ochronę infrastruktury krytycznej, kontrolę inwestycji i obrotu strategicznego, mechanizmy cyberbezpieczeństwa, zamówienia obronne, offset oraz instrumenty finansowania działalności przemysłowej. **Zasadniczym problemem nie jest zatem brak instrumentów, lecz ich rozproszenie i niewystarczająco skoordynowane wykorzystywanie.**

Ryzyko niespójności występuje zwłaszcza w ustawie o obronie Ojczyzny. Reżym przygotowania jednostek do militaryzacji, świadczeń na rzecz obrony oraz zadań realizowanych przez przedsiębiorców na rzecz Sił Zbrojnych częściowo odnoszą się do tych samych zdolności produkcyjnych, naprawczych i usługowych. Nie jest przy tym dostatecznie jasny ich wzajemny stosunek ani uzasadnienie odmiennego sposobu finansowania obowiązków nakładanych na przedsiębiorców.

Wieloośrodkowy charakter zarządzania przemysłem obronnym jest uzasadniony, ponieważ bezpieczeństwo dostaw zależy równocześnie od planowania obronnego, zamówień, finansowania, rezerw, transportu, energii, łączności, cyberbezpieczeństwa, ochrony ludności, polityki przemysłowej i nadzoru właścicielskiego. Rozproszenie

kompetencji między liczne organy, agencje, instytucje finansowe i spółki z udziałem Skarbu Państwa może jednak prowadzić do fragmentaryzacji polityki oraz niepełnego rozpoznania zależności dostawczych.

Prawo Unii Europejskiej tworzy coraz bardziej rozbudowane instrumenty wspierania europejskiej bazy przemysłowo-obronnej, wspólnych zamówień, agregowania popytu, bezpieczeństwa surowcowego, kontroli inwestycji oraz odporności rynku wewnętrznego. Instrumenty te mogą wspierać rozwój polskiego przemysłu obronnego, pod warunkiem aktywnego udziału polskich przedsiębiorstw i zapewnienia zgodności krajowych rozwiązań z regułami rynku wewnętrznego, pomocy państwa i ochrony konkurencji.

Artykuł 346 TFUE nie ustanawia generalnego wyłączenia sektora obronnego spod prawa Unii. Może być stosowany jedynie w przypadkach, w których jest to konieczne i proporcjonalne do ochrony podstawowych interesów bezpieczeństwa państwa, a celu tego nie można osiągnąć za pomocą szczególnego reżimu zamówień w dziedzinach obronności i bezpieczeństwa.

Rekomendacje

Należy uporządkować w ustawie o obronie Ojczyzny relacje między przygotowaniem jednostek do militaryzacji, świadczeniami na rzecz obrony oraz zadaniami realizowanymi przez przedsiębiorców na rzecz Sił Zbrojnych. Regulacja powinna wyraźniej określać zakres poszczególnych obowiązków, przesłanki ich nakładania, sposób finansowania oraz zasady unikania wielokrotnego obciążania przedsiębiorcy obowiązkami dotyczącymi tych samych zdolności.

Należy zintegrować istniejące mechanizmy identyfikowania zależności i ryzyk w łańcuchach dostaw. Informacje gromadzone w ramach Planu zabezpieczenia potrzeb Sił Zbrojnych powinny być koordynowane z mechanizmami dotyczącymi rezerw strategicznych, infrastruktury krytycznej,

ochrony ludności, cyberbezpieczeństwa, surowców krytycznych, półprzewodników i odporności podmiotów krytycznych. Celem powinno być uzyskanie całościowego obrazu dostawców, podwykonawców, zdolności produkcyjnych i potencjalnych wąskich gardeł.

Zarządzanie ryzykiem powinno mieć charakter proaktywny. Należy rozwijać systemy wczesnego ostrzegania, kwalifikować alternatywnych dostawców, utrzymywać strategiczne rezerwy surowców i komponentów o długim czasie pozyskania oraz przygotowywać plany odtworzenia produkcji, usług i infrastruktury po wystąpieniu zakłócenia.

Należy wzmacniać koordynację działań Rady Ministrów, MON, ministrów właściwych do spraw gospodarki, aktywów państwowych i spraw wewnętrznych, a także RARS, AMW, BGK, ARP, PFR oraz spółek z udziałem Skarbu Państwa. Koordynacja powinna obejmować wspólne określanie priorytetów inwestycyjnych, finansowanie zdolności krytycznych oraz ocenę skutków decyzji poszczególnych instytucji dla całego łańcucha dostaw.

W ocenie działalności spółek z udziałem Skarbu Państwa działających w sektorze obronnym **należy uwzględniać nie tylko wyniki finansowe, lecz także utrzymywanie zdolności produkcyjnych, serwisowych, naprawczych i mobilizacyjnych istotnych dla bezpieczeństwa państwa.** Instrumenty ładu korporacyjnego i zasady wynagradzania organów spółek mogą wspierać realizację tych celów.

Należy wzmacniać udział krajowych przedsiębiorstw i komponentów w zamówieniach obronnych, z zachowaniem wymogów prawa Unii Europejskiej. Polityka w zakresie komponentu krajowego powinna służyć przede wszystkim utrzymywaniu w Polsce zdolności produkcyjnych, serwisowych i naprawczych oraz ograniczaniu zależności od pojedynczych dostawców zagranicznych, a nie wyłącznie formalnemu preferowaniu przedsiębiorstw ze względu na miejsce ich siedziby.

Należy aktywnie wykorzystywać instrumenty przewidziane w prawie Unii Euro-

pejskiej, w szczególności wspólne zamówienia, agregowanie popytu, mechanizmy wzmacniania europejskiego przemysłu obronnego oraz struktury na rzecz europejskiego programu zbrojeniowego. Wymaga to zbadania, czy przepisy dotyczące zarządzania mieniem państwowym, zgód korporacyjnych i rozporządzania istotnymi aktywami zapewniają spółkom z udziałem Skarbu Państwa wystarczającą elastyczność uczestnictwa w takich przedsięwzięciach.

Należy doprecyzować kryteria identyfikowania podstawowego interesu bezpieczeństwa państwa na potrzeby zamówień obronnych i stosowania art. 346 TFUE. Pozwoliłoby to ograniczyć zarówno ryzyko nadużywania wyłączeń od zasad konkurencyjnych, jak i nadmierną ostrożność organów, która może prowadzić do wydłużania postępowań zakupowych.

W pierwszej kolejności powinny być wykorzystywane instrumenty szczególnego reżimu zamówień w dziedzinach obronności i bezpieczeństwa, w tym wymagania dotyczące ochrony informacji, bezpieczeństwa dostaw, zdolności wykonawców i kontroli podwykonawstwa. Całkowite wyłączenie stosowania Prawa zamówień publicznych powinno następować wyłącznie wtedy, gdy ochrona podstawowego interesu bezpieczeństwa państwa nie może zostać skutecznie zapewniona w ramach tego reżimu.

Należy dostosować ustawę o partnerstwie publiczno-prywatnym do specyfiki przedsięwzięć obronnych i bezpieczeństwa. Regulacja powinna uwzględniać ochronę informacji niejawnych, bezpieczeństwo podwykonawstwa, szczególne zasady ciągłości świadczenia usług, możliwość interwencji państwa oraz elastyczne kształtowanie umowy w sytuacjach nadzwyczajnych.

Należy rozwijać współpracę sektora wojskowego z przedsiębiorstwami prywatnymi, uczelniami, instytutami badawczymi i start-upami technologicznymi. Szczególne znaczenie ma współpraca dotycząca sztucznej inteligencji, systemów autonomicznych, technologii kosmicznych, zaawansowanych materiałów, cyberbezpieczeństwa oraz produktów i technologii podwójnego zastosowania.

MAPA ŁAŃCUCHÓW DOSTAW DLA WYBRANEGO SPRZĘTU WOJSKOWEGO I ŚRODKÓW BOJOWYCH

2.1. Analiza przedmiotowa polskiego przemysłu obronnego

2.1.1. Modernizacja Sił Zbrojnych RP od wstąpienia Polski do NATO do chwili obecnej

Przystąpienie Polski do Sojuszu Północnoatlantyckiego wymusiło na decydentach dostosowanie ówczesnie użytkowanego w Siłach Zbrojnych RP (SZ RP) postsowieckiego sprzętu wojskowego do wymagań NATO. Jednym z najważniejszych procesów modernizacyjnych SZ RP w XXI wieku było uruchomienie w 2003 roku procesu pozyskiwania od fińskiej firmy Patria AMV nowego kołowego transportera opancerzonego KTO „Rosomak” oraz przeniesienie produkcji transportera do zakładów w Siemianowicach. Do SZ RP dostarczono dotychczas ponad 1000 sztuk KTO Rosomak, także w wersjach do ewakuacji medycznej, rozpoznania i zabezpieczenia technicznego⁷¹. Do końca 2004 roku zakończono proces wyboru środków obrony przeciwpancernej, w procesie oceny dostępnych

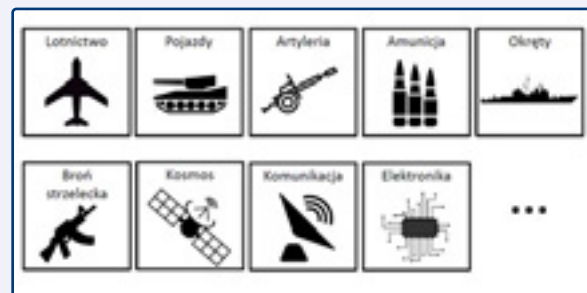
do pozyskania technologii oraz możliwości ich polonizacji zdecydowano o wyborze wyrzutni z pociskami Spike-LR Izraelskiej firmy Rafael. Następnym bardzo wielkim zadaniem modernizacyjnym jak na możliwości ówczesnych SZ RP było rozpoczęcie procesu wprowadzenia na wyposażenie sił powietrznych samolotów wielozadaniowych F-16. Atak Rosji na Ukrainę w 2014 roku zapoczątkował, na niespotykaną dotąd skalę, w SZ RP proces modernizacji i zakupów nowoczesnego sprzętu i uzbrojenia. Zwiększono wydatki na obronność do poziomu 4,6% w roku 2026 z tendencją wzrostu do 5% do roku 2030. Proces modernizacji technicznej Sił Zbrojnych RP uzyskał również ogromne wsparcie z Unii Europejskiej poprzez wprowadzenie nowego mechanizmu finansowego w celu wsparcia i przyspieszenia modernizacji zdolności obronnych państw członkowskich Unii Europejskiej oraz wzmocnienia europejskiego przemysłu zbrojeniowego SAFE (Security Ac-

71 T. Jałowicz, Sz. Mitkow. System Logistyczny SZ RP. Raport 2019.ASzWoj. Warszawa. 2019 str.115

tion for Europe). Polska uzyskała z tego programu dofinansowanie na zakup nowego sprzętu wojskowego w wysokości 43,7 mld euro. Zgodnie z założeniami rządowymi około 89 % przyznanych funduszy trafi bezpośrednio do polskiego przemysłu zbrojeniowego i krajowych kooperantów. Środki te sfinansują m.in.: realizację programu Tarcza Wschód oraz umocnienie wschodniej flanki NATO, zakup i rozwój systemów dronowych i antydronowych, rozbudowę obrony przeciwlotniczej oraz artylerii (m.in. Piorun, Borsuk, Krab), modernizacja infrastruktury transportowej i logistycznej o znaczeniu obronnym. Wiązał się z tym również znaczny wzrost liczności SZ RP poprzez tworzenie nowych związków taktycznych i dowództw.

2.1.2. Analiza wybranych systemów uzbrojenia i amunicji

Istotnym czynnikiem funkcjonowania przemysłu obronnego w Polsce są aktualne możliwości produkcji sprzętu wojskowego oraz środków materiałowych ze szczególnym uwzględnieniem środków bojowych. Przemysł obronny opiera się obecnie głównie na sektorze państwowym, skupionym wokół Polskiej Grupy Zbrojeniowej (PGZ), oraz na sektorze prywatnym (zarówno z kapitałem narodowym, jak i zagranicznym) reprezentującym podmioty zajmujące się produkcją na potrzeby bezpieczeństwa i obronności państwa. Przemysł obronny w Polsce ma możliwości produkcji szerokiego wachlarza sprzętu wojskowego i środków materiałowych, w tym środków bojowych, jednakże produkcja ta jest częściowa - poszczególne komponenty pochodzą od podwykonawców ulokowanych poza granicami Polski lub niewystarczająca - brak możliwości realizacji większych partii produkcyjnych niezbędnych dla zaspokojenia potrzeb Sił Zbrojnych RP. Niezależnie od struktury własnościowej przemysł zbrojeniowy skupiony jest wokół obszarów przedstawionych na rysunku 2.1



Rys. 2.1. Struktura branżowa narodowego przemysłu obronnego

W celu odwzorowania realnych wyzwań stojących przed polskim przemysłem obronnym badaniem szczegółowym objęto pięć pozycji sprzętu wojskowego i środków bojowych: amunicję artyleryjską 155 mm, BWP BORSUK, system WARMATE, AHS KRAB oraz AHS K9. Każdy z wybranych systemów reprezentuje odmienny model architektury logistycznej i technologicznej, co pozwala na przekrojowe mapowanie ryzyk systemowych:

Amunicja artyleryjska kalibru 155 mm



Rys. 2.2. Komponenty produkcyjne pocisku 155 mm

Źródło: opracowanie własne na podstawie <https://portalmilitarny.pl/analizy-i-komentarze/polska-grupa-zbrojeniowa-zaprezentowala-narodowy-plan-amunicyjny> (dostęp 02.02.2026).

Amunicja 155 mm stanowi komponent środków bojowych o absolutnym priorytecie w kontekście zapewnienia zdolności do prowadzenia działań obronnych o wysokiej intensywności. Badania w tym obszarze koncentrują się na domykaniu krajowego łańcucha produkcyjnego (produkcja skorup, zapalników, ładunków miotających oraz pozyskiwanie komponentów chemicznych, takich jak nitroceluloza i proch). Jest to model krytycznego zaopatrzenia materiałowego, w którym nadrzędnym celem jest eliminacja zależności od zewnętrznych dostawców komponentów chemicznych i hutniczych. Należy zwrócić uwagę, że w wielu obszarach mimo możliwości produkcyjnych, obecnie nie produkujemy w ogóle lub tylko częściowo wybrane egzemplarze sprzętu wojskowego i środki bojowe. Przykładem jest tu właśnie pocisk 155 mm. Choć składa się on z ograniczonej liczby komponentów, jego produkcja nie jest sprawą prostą. Wynika to przede wszystkim z bardzo wysokich wymagań w zakresie precyzji wykonania pocisku, co potem przekłada się na celność na polu walki. Stąd ważny jest potencjał wytwórczy

przedsiębiorstw przemysłu obronnego oraz jakość komponentów do produkcji tej amunicji. Amunicja kal. 155 mm tylko częściowo wytwarzana samodzielnie przez zakłady PGZ jest bowiem amunicją rozdzielnego ładowania i składa się z takich elementów jak: zapalnika, pocisku (z gazogeneratorem lub bez), zespołu modułowych ładunków miotających oraz zapłonika. Zarówno wcześniej, jak i obecnie produkcja amunicji w Polsce, w państwowych zakładach, odbywała i odbywa się z wykorzystaniem kluczowych komponentów pochodzących z zagranicy. W kraju produkujemy: zapalniki (na licencji) oraz pociski z gazogeneratorem lub bez (na licencji) metodą kucia i następnie elaborowane ładunkiem wybuchowym. Pozostałe komponenty, jak modułowe ładunki miotające nadal pochodzą z importu, choć już teraz trwa proces ich polonizacji⁷².

⁷² <https://portalmilitarny.pl/analizy-i-komentarze/polska-grupa-zbrojeniowa-zaprezentowala-narodowy-plan-amunicyjny/> (dostęp: 04.02.2026).

Bojowy Wóz Piechoty (BWP) BORSUK



Rys. 2.3. Bojowy wóz piechoty BORSUK

Źródło: materiały HSW, <https://static.prsa.pl/images/51d59dde-b849-4387-aa81-b483331c7514.jpg>, dostęp (07.06.26 r.)⁷³

BWP BORSUK reprezentuje model zaawansowanego projektu rozwojowego i innowacyjnego, opartego na krajowych kompetencjach konstrukcyjnych. Łańcuch dostaw nowego pływającego bojowego wozu piechoty Borsuk opiera się na strukturze konsorcjalnej pod przewodnictwem PGZ, gdzie głównym integratorem platformy jest Huta Stalowa Wola S.A. Architektura logistyczna pojazdu łączy krajowy potencjał przemysłowy z kluczowymi komponentami zagranicznymi z państw sojuszników NATO (USA, Niemcy, Izrael). Biorąc pod uwagę zestawienie komponentów tzw. BOM (*Bill of Materials*), która dla jednego wozu liczy ponad 11 tys. pozycji, łańcuch dostaw dzieli się na kilka kluczowych segmentów:

- integracja i kadłub – oparty na krajowych zdolnościach przemysłowych,
- system wieżowy i uzbrojenie – to hybryda

krajowego łańcucha dostaw z elementami pochodzącymi z USA i Izraela,

- układ napędowy i przeniesienie napędu – to głównie dostawcy zagraniczni z Niemiec i USA,
- systemy łączności i dowodzenia – to również miks krajowych zdolności uzupełniających współpracę z USA,
- system obrony – oparty na krajowych zdolnościach produkcyjnych.

W dalszej części raportu zostanie poddana analizie rozproszona sieć krajowych kooperantów oraz podatność na zakłócenia w dostawach zagranicznych komponentów specjalistycznych, takich jak układy napędowe (*powerpack*) czy zaawansowane systemy przeciwpancerne, przy jednoczesnym badaniu korzyści płynących ze stabilnego, wieloletniego wolumenu zamówień rządowych dla rozwoju krajowej bazy podwykonawczej.

⁷³ materiały HSW, <https://static.prsa.pl/images/51d59dde-b849-4387-aa81-b483331c7514.jpg>, dostęp (07.06.26 r.)

System Amunicji Krążącej WARMATE



Rys. 2.4. Amunicja krążąca Warmate

Źródło: https://wikitaneks.com/images/thumb/9/9e/WB_Electronics_Warmate.jpg/1200px-WB_Electronics_Warmate.jpg, (dostęp: 07.07.26 r.)

Łańcuch dostaw amunicji krążącej Warmate, produkowanej przez Grupę WB Electronics z Ożarowa Mazowieckiego, to zaawansowana sieć kooperacji, która opiera się na maksymalnej polonizacji kluczowych komponentów. Reprezentuje model bliski pełnej suwerenności technologicznej⁷⁴. Wywodzi się z sektora prywatnego i charakteryzuje się maksymalnym stopniem kontroli nad własnością intelektualną (IPR – Intellectual Property Rights) kodem źródłowym oraz architekturą systemu. Struktura łańcucha dostaw dla systemu Warmate dzieli się na kilka głównych poziomów: architektura i integracja główna – należy do Grupy WB Electronics, oprogramowanie i autopilot – całość kodu źródłowego systemów łączności szyfrowanej, algorytm sztucznej inteligencji (np. Target Lock – śledzenie celów) oraz stacji kierowania i kontroli – również należy do WB Electro-

nics, kluczowe komponenty i kooperanci (dostawcy P 1) – są to krajowi producenci prywatni jak i państwowi, głównie z grupy PGZ, sensory optoelektroniczne, półprzewodniki i układy scalone – dostawcami tzw. P 2 i P 3 są producenci rynku globalnego, głównie z Europy, USA i Japonii⁷⁵. Ponieważ system łączności, zarządzania polem walki (Topaz) i oprogramowanie są w 100% polskie, ewentualnie wąskie gardła w dostawach zagranicznych komponentów ograniczają się do ogólnoświatowej elektroniki użytkowej. Obszar badań obejmuje w tym przypadku specyficzne ryzyka dla zaawansowanej elektroniki, mikroprocesorów oraz podatność na sabotaż w globalnych łańcuchach dostaw komponentów *dual-use* (podwójnego zastosowania), przy jednoczesnym badaniu elastyczności szybkiego prototypowania i modyfikacji na podstawie doświadczeń wojennych.

⁷⁴ Dura M., Grupa WB jako modelowy przykład budowy odpornego łańcucha dostaw w przemyśle obronnym. Defence24 Study Raport, Warszawa 2023 r.

⁷⁵ Nowakowski T., Analiza potencjału produkcyjnego polskiego sektora bezzałogowców. Raport Instytutu Polityki Europejskiej i Bezpieczeństwa, 2024 r.

Armatohaubica KRAB



Rys. 2.5. Armatohaubica AHS Krab (155 mm)

Źródło: <https://www.bing.com/images/search?q=AHS+Krab+opis+budowy%2c+rysunki&form=HDRSC3&first=1>, (dostęp 07.06.26 r.)

Analiza łańcucha dostaw samobieżnej armatohaubicy AHS Krab (kal. 155 mm) to przykład modelu hybrydowego, łączącego krajową integrację, polskie systemy dowodzenia i kierowania ogniem (zintegrowany system wspomagania dowodzenia TOPAZ) oraz licencjonowane technologie zagraniczne (podwozie, lufa). Podział łańcucha dostaw rozpoczyna integrator główny, którym jest Huta Stalowa Wola – odpowiada za montaż końcowy, integrację systemów wieżowych z podwoziem, produkcję luf oraz testy zdawczo-odbiorcze gotowych wozów. Kluczowe komponenty zagraniczne to: podwozie i napęd, które pochodzą z Korei Południowej, od rodziny pojazdów K9 Thunder, silniki wysokoprężne MTU MT 881 Ka-500 dostarczają

wykonawcy z Niemiec, natomiast dostawcą automatycznej przekładni jest firma z USA Allison. Ważnym elementem wpływającym na bezpieczeństwo łańcucha dostaw dla AHS Krab jest system dowodzenia i łączności pochodzący od Grupy WB Electronics oraz optoelektronika oraz sensory pochodzące od PCO S.A. Najbardziej wrażliwymi punktami łańcucha dostaw pozostają komponenty napędowe (silnik MTU i przekładnie Allison) oraz dostępność komponentów chemicznych do produkcji ładunków miotających 155 mm. Badanie skupia się na analizie barier związanych z prawami do modyfikacji, serwisu oraz podatności łańcucha dostaw na decyzje polityczno-eksportowe państw licencjodawców.

Armatohaubica K9



Rys. 2.6. Armatohaubica K9 Thunder

Źródło: <https://polskieradio24.pl/artykul/3347786,rosna-polskie-wydatki-na-obronnosc-prowadzimy-w-krajach-nato>, (dostęp 07.06.26 r.)

Reprezentuje model stricte importowy z zaplanowaną lokalizacją wsparcia logistycznego w Polsce. Pierwsze partie w wersji K9A1, które dostarczono do Wojska Polskiego opierały się głównie na podzespołach koreańskich i zachodnich. Od 2026 roku rozpoczęte dostawy w docelowym standardzie K9PL uruchomiły proces głębokiej integracji z polskim przemysłem obronnym⁷⁶. Polski łańcuch dostaw dzieli się na trzy główne filary. Pierwszy dotyczy komponentów integrowanych bezpośrednio w strukturze pojazdu - głównie polskie systemy łączności, ochrony oraz uzbrojenia pomocniczego. Drugi to krajowy ekosystem dowodzenia i logistyki skupiony głównie na zabezpieczeniu Dywizyjnych Modułów Ogniwych. Trzeci dotyczy zabezpieczenia bazy remontowo-serwisowej – zwłaszcza za-

bezpieczenie łańcucha dostaw w okresie eksploatacji sprzętu (MRO – *Maintenance, Repair, and Overhaul*). Analiza przedmiotu badań w tym obszarze koncentruje się wokół identyfikacji ryzyk wynikających z głębokiej i długoterminowej zależności od zagranicznego producenta w zakresie dostaw części zamiennych, dokumentacji technicznej oraz ustanawiania suwerennego potencjału remontowo-serwisowego poziomu *depot* w kraju.

Trendy globalizacyjne skutkujące transgranicznością procesów gospodarczych doprowadziły do funkcjonowania koncepcji zintegrowanych łańcuchów dostaw. Głównym przesłaniem tworzenia takich łańcuchów dostaw jest uzyskanie maksymalnej efektywności ekonomicznej przez wszystkie składowe ogniwa takich łańcuchów⁷⁷.

⁷⁶ Agencja Uzbrojenia, Ministerstwo Obrony Narodowej, Komunikat prasowy dotyczący zatwierdzenia umowy ramowej, lipiec 2022, Umowy Wykonawczej nr 1, sierpień 2022 oraz Umowy Wykonawczej nr 2, grudzień 2023r.

⁷⁷ K. Ficoń. Łańcuch Bezpieczeństwa. Zagrożenia, Ryzyka, Kryzysy. Bel Studio. Warszawa 2021

Modernizacja SZ RP w zasadniczym wymiarze opiera się na dostawach systemów uzbrojenia od globalnych, światowych liderów produkujących nowoczesne systemy wojennego wyposażenia, przez co mitigacja ryzyka po stronie dostaw może być osiągnięta głównie poprzez jak największy wymiar polonizacji dostawców tego wyposażenia.

2.1.3. Analiza możliwości lokowania w polskim przemyśle elementów produkcji oraz budowania łańcuchów dostaw w oparciu o narodowe zdolności produkcyjno-dostawcze

Analiza możliwości lokowania produkcji i budowania łańcuchów dostaw w polskim przemyśle obronnym (2026-2030) wskazuje na dążenie do maksymalnej samowystarczalności, bezpieczeństwa dostaw i repolonizacji kluczowych technologii. Działania te wynikają z konieczności uniezależnienia się od zagranicznych kooperantów oraz reagowania na zagrożenia w zmieniającej się architekturze bezpieczeństwa globalnego.

W tabeli 2.1 przedstawiono możliwości lokowania produkcji w polskim przemyśle obronnym sprzętu wojskowego i środków bojowych i tym samym budowania łańcuchów dostaw w oparciu o narodowe zdolności.

Tab. 2.1. Możliwości lokowania produkcji i budowania łańcuchów dostaw w polskim przemyśle obronnym (2026-2030)

Sprzęt wojskowy, środki bojowe	Typ sprzętu wojskowego	Możliwości produkcyjne (2026-2030)	Rekomendacje
Artyleria i systemy raketowe	Artyleria lufowa	○	Zwiększenie możliwości produkcyjnych
	Moździerz samobieżny (na podwoziu kołowym i gąsienicowym)	○	Realizacja prac rozwojowych poprzez międzynarodowe projekty
	Wieża moździerzowa	○	Zwiększenie możliwości produkcyjnych
	Moździerz	○	Realizacja prac rozwojowych poprzez międzynarodowe projekty
	Wyrzutnie raketowe	●	Zwiększenie możliwości produkcyjnych oraz częściowa polonizacja produkcji. Realizacja prac rozwojowych w celu dążenia do uzyskania własnych systemów
Bojowe wozy piechoty i pojazdy opancerzone	Bojowy wóz piechoty	○	Zwiększenie możliwości produkcyjnych oraz pozyskanie licencji na produkcję wybranych komponentów np. armaty 30/40 mm
	Kołowy transporter opancerzony	○	Realizacja prac rozwojowych poprzez międzynarodowe projekty
	Zdalnie sterowany system wieżowy	○	Zwiększenie możliwości produkcyjnych oraz pozyskanie licencji na produkcję wybranych komponentów np. armaty 30/40 mm
	Opancerzone pojazdy patrolowe i wsparcia	○	Polonizacja produkowanych systemów
Systemy bezzałogowe	Bezzałogowe systemy powietrzne	●	Realizacja prac rozwojowych w celu dążenia do uzyskania własnych systemów
	Bezzałogowe systemy lądowe	○	Realizacja prac rozwojowych w celu dążenia do uzyskania własnych systemów
	Bezzałogowe systemy morskie	○	Realizacja prac rozwojowych w celu dążenia do uzyskania własnych systemów

Sprzęt wojskowy, środki bojowe	Typ sprzętu wojskowego	Możliwości produkcyjne (2026-2030)	Rekomendacje
Systemy obrony przeciwlotniczej	Przenośne przeciwlotnicze zestawy raketowe	○	Realizacja prac rozwojowych w celu uzyskania kolejnych wersji rozwojowych
	Systemy obrony przeciwlotniczej bardzo krótkiego zasięgu	○	Zwiększenie zdolności produkcyjnych. Realizacja prac rozwojowych w celu uzyskania kolejnych wersji rozwojowych
	Systemy obrony przeciwlotniczej średniego zasięgu	●	Realizacja prac rozwojowych poprzez międzynarodowe projekty
	Systemy obrony przeciwlotniczej dalekiego zasięgu	●	Realizacja prac rozwojowych poprzez międzynarodowe projekty
Nowoczesne radiolokatory rozpoznania przestrzeni	Radary średniego i dalekiego zasięgu	●	Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Systemy radiolokacyjne i walki elektronicznej	●	Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
Broń strzelecka	Karabinki automatyczne kalibru 5,56 mm	○	Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Pistolety samopowtarzalne 9 mm	○	Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Karabiny wyborowe	○	Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Uniwersalne karabiny maszynowe	○	Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Granatniki	○	Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
Wyposażenie indywidualne żołnierza	Optyka, ochrona osobista, systemy nośne, wyposażenie przetrwania	○	Realizacja prac rozwojowych poprzez międzynarodowe projekty
Systemy BMS różnych poziomów dowodzenia		●	Polonizacja produkowanych systemów
Systemy łączności		○	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów
Pojazdy transportowe i wozy wsparcia		○	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów
Samoloty i śmigłowce	Samoloty transportowe/wielozadaniowe	○	Realizacja prac rozwojowych poprzez międzynarodowe projekty
	Śmigłowce wielozadaniowe	●	Realizacja prac rozwojowych poprzez międzynarodowe projekty
Okręty morskie	Fregaty	●	Realizacja prac rozwojowych poprzez międzynarodowe projekty
	Okręty specjalistyczne	○	Realizacja prac rozwojowych poprzez międzynarodowe projekty
Broń pancerna	Czołgi	●	Polonizacja produkowanych systemów

Sprzęt wojskowy, środki bojowe	Typ sprzętu wojskowego	Możliwości produkcyjne (2026-2030)	Rekomendacje
Amunicja i środki bojowe	Amunicja artyleryjska	❶	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Amunicja średniokalibrowa	❶	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Amunicja małokalibrowa	❶	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Amunicja czołgowa	❶	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Amunicja moździerzowa	❶	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Przeciwpancerne pociski kierowane	❶	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Pociski raketowe	❶	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Granaty, miny	❶	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
	Bomby lotnicze	❶	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
Systemy antydronowe		❶	Zwiększenie możliwości produkcyjnych. Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty
Satelity wojskowe rozpoznawcze i łącznościowe		❶	Polonizacja produkowanych systemów. Realizacja prac rozwojowych poprzez narodowe i międzynarodowe projekty

Legenda: ○ - produkcja w polskim przemyśle narodowym, ❶ - częściowa produkcja, niektóre elementy pochodzą od podwykonawców ulokowanych poza Polską, ● - brak produkcji.

Analizując przedstawione materiały można postawić tezę, że Polski przemysł obronny zmierza w kierunku repolonizacji produkcji, zwiększając moce w kluczowych obszarach (amunicja, pojazdy opancerzone) i budując lokalne łańcuchy dostaw, co ma na celu zapewnienie suwerenności i bezpieczeństwa w obliczu obecnych i przyszłych zagrożeń. Jednak pomimo rozwoju, wciąż znajduje się w fazie transformacji i dlatego kluczowym jest efektywne wykorzystanie coraz większych środków finansowych (budżetowych i pozabudżetowych) przeznaczanych na realizację programów zbrojeniowych.

2.1.4. Trendy technologiczne rozwoju przemysłu obronnego

W tej części raportu autorzy zasygnalizowali trendy technologiczne oraz możliwości produkcyjne wybranych produktów polskiego przemysłu w domenach: rozpoznania kosmicznego, bezzałogowych platformach rozpoznawczych i bojowych oraz systemach zarządzania polem walki. Wybór tych, a nie innych systemów był obiektywnym wyborem autorów raportu i podyktowany przede wszystkim ich innowacyjnym charakterem, zdolnościami do multiplikowania sił oraz

skokowym wzrostem wprowadzania opisanych zdolności do Sił Zbrojnych RP w ostatnich kilku latach.

W zakresie możliwości produkcyjnych Polska należy do istotnych producentów systemów bezzałogowych w Europie Środkowo-Wschodniej, z rosnącą specjalizacją w wybranych niszach (np. systemy rozpoznawcze, łączność taktyczna). Szczególnie wojna na Ukrainie, ale także konflikty na Bliskim Wschodzie czy wojny Azersko-Armeńskiej pokazały, że platformy bezzałogowe stały się kluczowym elementem prowadzonych operacji. Polski przemysł, reprezentowany głównie przez państwową Grupę PGZ, ale także przez prywatne podmioty takie jak: Grupa WB, STEKOP, MACRO-SYSTEM Sp. z o.o., Sieć Badawcza Łukasiewicz, PIAP oraz wojskowe instytuty badawcze takie jak: WITPiS, WITU, ITWL, WITI aktywnie odpowiedział na zapotrzebowanie w tym segmencie sprzętu wojskowego, projektując i produkując zaawansowane platformy bezzałogowe⁷⁸. Należy zaznaczyć, że poszczególni producenci przedmiotowego asortymentu znajdują się na różnych poziomach w zakresie zdolności produkcji. Niektóre produkty są na poziomie demonstratorów technologii inne na etapie produkcji seryjnej, a jeszcze inne są wykorzystywane w realnych warunkach bojowych.

Rozwój platform bezzałogowych nie ogranicza się już tylko do rozpoznania powietrznego, ale ewoluuje w stronę systemów uderzeniowych, wielodomenowych oraz lądowych i morskich robotów autonomicznych. Systemy bezzałogowe produkowane przez polski przemysł zbrojeniowy można podzielić ze względu na środowisko w jakim operują, a mianowicie na: Bezzałogowe Systemy Powietrzne (z ang. *Unmanned Aerial Vehicles* - UAV), Bezzałogowe Pojazdy Lądowe – BPL (z ang. *Unmanned Ground Vehicles* - UGV) oraz Bezzałogowe Platformy Wodne/Morskie - BPW lub BPM (z ang. *Unmanned Maritime Vehicles* – UMV)⁷⁹.

Sytuacja geopolityczna Polski, a zwłaszcza wojna na Ukrainie wymusiła działania zmierzające do bardzo szybkiego rozwoju zdolności polskiego przemysłu do produkcji bezzałogowych platform operujących we wszystkich domenach operacyjnych, a więc powietrznej, lądowej i morskiej. Obowiązujący na świecie trend w tym obszarze związany z integracją bezzałogowych platform z systemami walki sieciocentrycznej i autonomicznego przetwarzania danych powoduje, że polscy producenci tych platform powinni skoncentrować swoją uwagę na projektowaniu systemów bezzałogowych jako elementu „kill web”, a nie pojedynczych platform w poszczególnych domenach. Aby sprostać tym wyzwaniom przemysł obronny musi przejść z fazy „manufaktury produkcji” i budowy zaawansowanych prototypów do fazy „przemysłowej produkcji masowej” z silnym komponentem sztucznej inteligencji (AI), rozumianym jako rozwój zdolności platformy do wykorzystania w sieciocentrycznym systemie walki, aby sprostać wymaganiom nowoczesnej wojny asymetrycznej

2.1.5. Możliwości budowy domeny rozpoznania powietrznego (w tym kosmicznego) przez polskie przedsiębiorstwa w kontekście budowy świadomości operacyjnej we współczesnym konflikcie zbrojnym

Współczesne konflikty zbrojne pokazują, że informacja o przeciwniku, o jego sile, położeniu, kierunkach marszu, uformowaniu logistyki, dostępności zapasów itp. stała się podstawowym czynnikiem decydującym o wyniku każdego konfliktu. Można więc postawić tezę, że informacja o wrogich siłach jest ważniejsza niż liczba czołgów czy samolotów. Dobitnie pokazują to doświadczenia z wojny w Ukrainie wskazując, że wiedza operacyjna o przeciwniku nie jest już tylko problemem technicznym, który można rozwiązać za pomocą sensorów, al-

⁷⁸ Simiński P. Koncepcja Bezzałogowych Platform Lądowych na potrzeby działań ratowniczych. Logistyka w ratownictwie, s. 147-158. Instytut Naukowo Wydawniczy „Spatium”. Radom 2021.

⁷⁹ Dura M., Rewolucja dronowa odjeżdża Polsce, Defence 24, https://defence24.pl/sily-zbrojne/rewolucja-dronowa-odjeżdża-polsce#goog_rewarded, dostęp 19.03.2026 r.

gorytmów i transmisji danych, lecz stała się wielodomenową analizą przestrzenną zdolności przeciwnika do prowadzenia wojny, odporności jego zaplecza przemysłowo-produkcyjnego oraz stabilnych łańcuchów dostaw. Polska, posiadając bogaty zestaw firm dysponujących odpowiednimi zdolnościami technologicznymi, wsparta rozwiązaniami sojuszniczymi w ramach NATO i UE, rozpoczęła budowę unikalnej narodowej zdolności w domenie rozpoznania powietrznego, w tym kosmicznego, która zdefiniuje naszą świadomość operacyjną na dekady.

Wojna w Ukrainie uświadomiła wszystkim graczom z domeny rozpoznania powietrznego, w tym kosmicznego, że współczesne pole walki to środowisko sieciocentryczne. Świadomość operacyjna, czyli między innymi prowadzenie walki, nie polega już tylko na wiedzy o tym, gdzie znajduje się przeciwnik i jakimi siłami dysponuje, ale na skróceniu pętli decyzyjnej od momentu rozpoznania przez sensory po zniszczenie celu przez efektory. Łańcuch ten, nazywany w Siłach Zbrojnych „kill chain”, w nowoczesnej doktrynie przechodzi w „kill web” i składa się z następujących etapów⁸⁰: wykrycie celu, identyfikacja, wybór środka rażenia, zarządzanie i kontrola, zniszczenie celu, ocena skutków uderzenia. W realnych scenariuszach użycia systemów rozpoznawczych, występuje szereg ograniczeń systemowych w tym, integracja danych (*interoperability*), odporność transmisji sygnałów (*EW/jamming*), jakość i ilość danych oraz suwerenność architektury C4ISR. Zarządzanie takim strumieniem danych wymaga integracji systemów C4ISR w ramach uzgodnionych profili interoperacyjności. Przykłady takie jak DELTA⁸¹, TOPAZ, JAŚMIN⁸² czy rozwijany BMS LEGION należy w tym raporcie traktować jako potencjalne kierunki integracji i obszary wymagające testów, standaryzacji oraz potwierdzenia interoperacyjności operacyjnej, a nie jako istniejący, jednolity ekosystem. Komponent rozpoznania satelitarnego to jedna z najszybciej rozwijających się zdolności Polskich Sił Zbrojnych. Pozyskiwane satelity są wykorzystywane zarówno na potrzeby

wojska, jak i gospodarki cywilnej. Instytucją odpowiedzialną za budowanie zdolności rozpoznania kosmicznego w Siłach Zbrojnych RP jest Agencja Rozpoznania Geoprzestrzennego i Usług Satelitarnych (ARGUS). Polski przemysł obronny, zarówno państwowy jak i prywatny, oferuje dziś rozwiązania, które konkurują z globalnymi graczami, w tym obszarze przemysłu. W warstwie rozpoznania powietrznego z wykorzystaniem platform bezzałogowych można stwierdzić, że jest jednym z kluczowych graczy na rynku Europy Środkowo-Wschodniej.

2.1.6. Zdolności polskiego przemysłu obronnego w zakresie produkcji i wdrożenia Systemu Zarządzania Polem Walki (Battlefield Management System) w perspektywie odporności cyfrowego łańcucha dostaw

System Zarządzania Polem Walki (BMS - *Battlefield Management System*) jest komponentem cyfrowego wsparcia dowodzenia w wojskach lądowych. Na szczeblu taktycznym umożliwia tworzenie wspólnego obrazu sytuacji (*Common Operational Picture*, COP), wymianę meldunków, planowanie i dystrybucję zadań oraz integrację z systemami łączności, rozpoznania i rażenia. Z perspektywy bezpieczeństwa dostaw ryzyka BMS obejmują nie tylko dostępność sprzętu informatycznego, lecz także ciągłość wsparcia i aktualizacji oprogramowania, prawa do utrzymania systemu, komponenty kryptograficzne, dane geoprzestrzenne, usługi serwisowe oraz zgodność z profilami interoperacyjności NATO. W raporcie BMS jest analizowany jako element integrowany z wybranymi platformami lądowymi, w szczególności Borsukiem, Krabem i K9, a nie jako samodzielny system uzbrojenia.

Dla celów analizy należy odróżnić: BMS – aplikacyjno-procesowe wsparcie dowodzenia, meldowania, śledzenia sił własnych i budowy

80 <https://netflowit.pl/modele-analzy-cyberzagrozen-cyber-kill-chain/>, dostęp 05.02.2026 r.

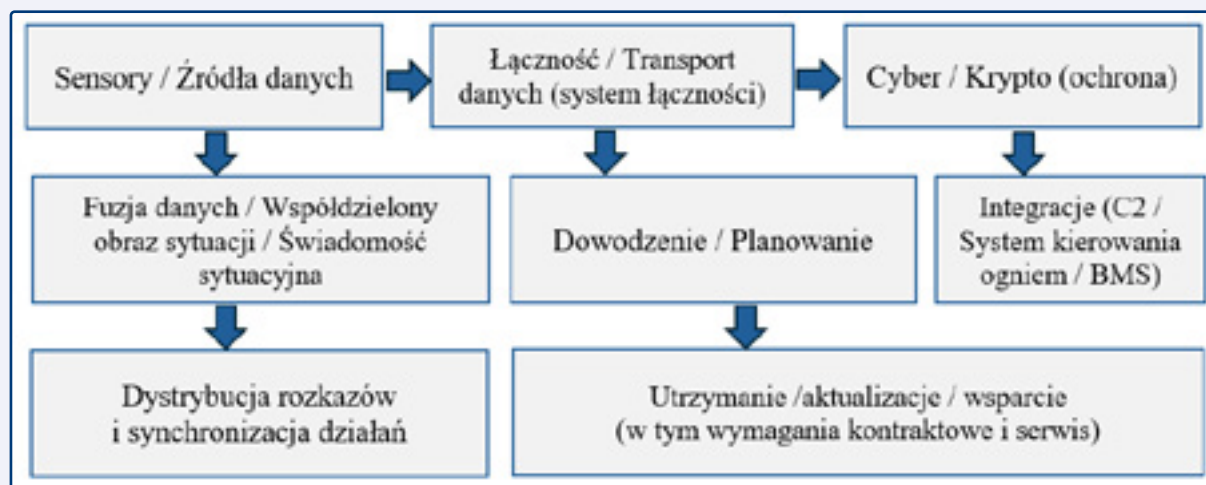
81 https://geopolityka.org/20241004/ukrainski-system-bojowy-delta-z-sukcesem-zadebiutowal-na-imprezach-nato-co-go-wyroznia/#google_vignette, dostęp 10.02.2026 r.

82 <https://www.teldat.com.pl/oferta/produkty/systemy/84-hms-jasmin.html>, dostęp 10.02.2026 r.

obrazu sytuacji; CIS – usługi łączności i transportu danych; FCS/AFCS – systemy kierowania ogniem; C4I/C4ISR – szerszą architekturę dowodzenia, łączności, informatyki, rozpoznania i obserwacji. Systemy te mogą być integrowane na jednej platformie, ale mają odmienne zależności dostaw, cykle kwalifikacji i ryzyka utrzymaniowe. Interoperacyjność

BMS jest warunkowana nie tylko architekturą krajową, lecz także zgodnością ze standardami STANAG, profilami NATO Interoperability Standards and Profiles (NISP), wymaganiami Federated Mission Networking (FMN) oraz wynikami testów integracyjnych. Schemat referencyjnej architektury BMS/C4I przedstawiono na rysunku 2.1.

Rys. 2.7. Model domen zależności dostaw BMS/C4I



Źródło: opracowanie P. Zamelek/WAT na podstawie analizy jawnych klas komponentów i wymagań interoperacyjności.

Logikę bezpieczeństwa dostaw BMS oparto o podejście warstwowe uwzględniające uproszczone zestawienie komponentów i zależności, które pozwala zachować jawność danych, a jednocześnie identyfikować realne „wąskie gardła” w łańcuchu dostaw. W praktyce takie podejście zastępuje pełny wykaz części mapą klas komponentów i zależności w trzech porządkach: sprzętowym (urządzenia i elektronika), programowym (zestawienie komponentów oprogramowania, licencje, aktualizacje) oraz integracyjno-konfiguracyjnym (interfejsy, profile interoperacyjności, dane geoprzestrzenne, polityki kryptograficzne), bez ujawniania numerów elementów, dostawców szczegółowych i wrażliwych konfiguracji wojskowych. Dzięki temu dla każdej warstwy można jawnie przypisać typową zależność rynkowo-geograficzną, mechanizm wąskiego gardła oraz zestaw działań proaktywnych i reaktywnych, co umożliwia porównywalną ocenę odporności w warunkach pokoju.

BMS traktuje się tu jako system systemów, obejmujący warstwy: źródła danych/sensory, łączność i sieci, fuzję danych i wspólny obraz sytuacji, dowodzenie i planowanie, dystrybucję rozkazów i synchronizację efektorów, cyberbezpieczeństwo i kryptografię, utrzymanie i aktualizacje. Ryzyka bezpieczeństwa dostaw porządkuje się dodatkowo w triadzie: dostęp/zakłócenia, zależność oraz gwarancje dostaw. Ta typologia jest niezbędna dla BMS, ponieważ znacząca część krytycznych zależności ma charakter „niematerialny” (licencje, prawa użycia, aktualizacje bezpieczeństwa)⁸³.

2.1.7. Analiza patentów i stosowanych technologii, jak również potencjalnych zdolności technologicznych wynikających z prowadzonych prac naukowo-badawczych

W logice raportu patenty i prace badawczo-rozwojowe nie są traktowane jako sa-

83 D. Fiott, Sovereignty by Design? Security of Supply in Defence in the European Union, ARES Policy Paper No. 113, May 2025, Institut de Relations Internationales et Stratégiques, [online], dostęp: 20.12.2025, <https://www.iris-france.org/2025/05/sovereignty-by-design-security-of-supply-in-defence-in-the-european-union/>.

moistny miernik innowacyjności, lecz jako wskaźnik możliwości polonizacji, dywersyfikacji zaopatrzenia i budowy krajowych kompetencji w tych obszarach, które decydują o ciągłości dostaw dla Sił Zbrojnych RP, czyli nie przesądzają one o wdrożeniu ani o mocach produkcyjnych, ale stanowią mierzalny ślad aktywności wynalazczej i potencjalnego kierunku specjalizacji. Równolegle, projekty B+R (krajowe i unijne) ujawniają obszary, w których istnieje strumień rozwiązań mogących w średnim horyzoncie zmniejszać ryzyka w łańcuchach dostaw (np. przez krajowe zamienniki, przeprojektowanie komponentów, transfer technologii do przemysłu).

Metodyka oceny zakresu posiadania przez polski przemysł obronny oraz współpracujące z nim instytuty badawcze i uczelnie dysponujące zasobami wiedzy technicznej, własności przemysłowej i wynikami prac badawczo-rozwojowych (B+R), opiera się na triadzie źródeł w ramach replikowalnej procedury i na mapowaniu wyników na koszyki technologiczne. Wynikami kwerend w rejestrach patentowych objęto lata 2015–2025 w zakresie zasobów Urzędu Patentowego RP, weryfikacji w europejskiej bazie Espacenet oraz jakościowego potwierdzenia i doprecyzowania obrazu technologicznego na podstawie materiału z bazy PATENTSCOPE. Badaniem objęto wybrane przedsiębiorstwa obronne (państwowe i prywatne), wojskowe instytuty badawcze i uczelnie oraz instytuty Sieci Łukasiewicz, w tym podmioty zaplecza B+R⁸⁴.

Równolegle uwzględniono jawnie dostępne informacje o projektach badawczo-rozwojowych, zwłaszcza tych, które mogą przekładać się na krajowe opracowanie innowacyjnych rozwiązań technicznych, technologicznych, czy innych procesów istotnych dla bezpie-

czeństwa dostaw (Narodowe Centrum Badań i Rozwoju oraz CORDIS dla projektów UE).

W warstwie jawnej najbardziej spójny i technicznie relewantny profil patentowy posiada Wojskowy Instytut Techniczny Uzbrojenia (WITU). WITU utrzymuje wyspecjalizowane centra w obszarze materiałów wybuchowych i środków bojowych, osłon balistycznych, techniki raketowej, systemów treningowych i bezzałogowych. Dokumenty Urzędu Patentowego RP potwierdzają, że nie jest to potencjał deklaracyjny WITU. Do jawnie identyfikowalnych przykładów należą między innymi patent PL 244151 B1 „Zapalnik z elektronicznie programowaną nastawą czasową” oraz patent PL 244686 B1 „Sposób rozczalania granatnikowego pocisku kumulacyjnego o napędzie raketowym”⁸⁵.

Drugi ważny filar krajowych kompetencji tworzą technologie utrzymaniowe i diagnostyczne. Instytut Techniczny Wojsk Lotniczych (ITWL) potwierdza obecność takich zdolności zarówno poprzez własne komunikaty, jak i jawne dokumenty Urzędu Patentowego RP. Przykłady obejmują patent PL 230085 dotyczący układu do wyznaczania ciężaru i położenia środka masy statku powietrznego oraz patent 244521 odnoszący się do testowania algorytmów identyfikacji wysokocyklicznych drgań łopatek wysokoobrotowych maszyn wirnikowych. Wniosek dla bezpieczeństwa dostaw jest tu jednoznaczny: krajowa autonomia techniczna buduje się nie tylko przez wytwarzanie nowego wyrobu, lecz również przez zdolność jego diagnozowania, pomiaru, badania i utrzymania⁸⁶.

Po stronie przemysłowej najbardziej czytelny ślad technologiczny mają PIT-RADWAR i RADMOR. PIT-RADWAR deklaruje prowadzenie pełnego cyklu dostaw - od badań

84 Polska Grupa Zbrojeniowa S.A., Huta Stalowa Wola S.A., MESKO S.A., PCO S.A., PIT-RADWAR S.A., NITRO-CHEM S.A., Fabryka Broni „Łucznik” – Radom sp. z o.o., Rosomak S.A., OBRUM sp. z o.o., Ośrodek Badawczo-Rozwojowy Centrum Techniki Morskiej S.A., WB Electronics S.A., TELDAT sp. z o.o., Wojskowa Akademia Techniczna, Sieć Badawcza Łukasiewicz, wojskowe instytuty badawcze, wojskowe przedsiębiorstwo remontowo-produkcyjne.

85 Wojskowy Instytut Techniczny Uzbrojenia, „Osiągnięcia”. [online], dostęp: 19.03.2026, <https://www.witu.mil.pl/osiagniecia>; Urząd Patentowy RP, PL 244151 B1 „Zapalnik z elektronicznie programowaną nastawą czasową”, data publikacji patentu: 11.12.2023; Urząd Patentowy RP, PL 244686 B1 „Sposób rozczalania granatnikowego pocisku kumulacyjnego o napędzie raketowym”, data publikacji patentu: 26.02.2024.

86 Instytut Techniczny Wojsk Lotniczych, „Nagradzany wynalazek” (komunikat dot. wyróżnień i odniesienie do patentu PL230085). 17.05.2022. [online], dostęp: 19.03.2026, <https://www.itwl.pl/aktualnosci/504-nagradzany-wynalazek>; Urząd Patentowy RP, WUP 06/2024, poz. 244521 „Układ do testowania algorytmów identyfikacji wysokocyklicznych drgań łopatek wysokoobrotowych maszyn wirnikowych”.

i projektowania po produkcję i wsparcie logistyczne - w obszarze radiolokacji, radioelektronicznych systemów rozpoznania oraz systemów automatyzacji i wspomagania dowodzenia. Urząd Patentowy RP potwierdza bieżącą aktywność zgłoszeniową spółki, czego przykładem jest opublikowane w Biuletynie Urzędu Patentowego nr 5/2026 zgłoszenie wzoru użytkowego „Podwójny moduł nadawczo-odbiorczy”. RADMOR pozostaje producentem i dostawcą nowoczesnych urządzeń łączności dla wojska, co potwierdza istnienie krajowej bazy technologicznej w segmencie łączności taktycznej⁸⁷.

Z punktu widzenia bezpieczeństwa łańcuchów dostaw analiza prowadzi do wniosku jednoznacznego: najsilniejszy, jawnie rozpoznawalny zasób technologiczny istotny

dla bezpieczeństwa dostaw dotyczy domeny amunicyjnej, materiałów wysokoenergetycznych, zapalników i wybranych części eksploatacyjnych dla artylerii. Ponadto, w obszarze łączności, radarów i systemów obserwacji istnieją kompetencje krajowe o istotnym znaczeniu, ale mają one charakter bardziej wybiórczy i nie obejmują pełnego łańcucha najbardziej złożonych komponentów. Podczas gdy największa luka utrzymuje się w obszarach najbardziej nasyconych elektroniką i mikroelektroniką, czyli tam, gdzie wskutek globalizacji łańcuchów dostaw najczęściej powstają „wąskie gardła” czasu pokoju (długie terminy, ograniczenia eksportowe, rynek komercyjny konkurujący z wojskowym). Zaprezentowane dane pozwalają na sformułowanie następujących wniosków i rekomendacji:

2.2. Analiza podmiotowa potencjału polskiego przemysłu

Bezpieczeństwo łańcuchów dostaw w przemyśle obronnym jest determinowane zarówno przez strukturę sieci dostaw, jak i potencjał przedsiębiorstw stanowiących poszczególne ogniwa. Szczególną rolę w łańcuchu dostaw pełnią integratorzy (*prime contractors*), odpowiedzialni za projektowanie architektury łańcucha dostaw, koordynację relacji z dostawcami oraz zapewnienie integracji technologicznej i organizacyjnej systemów uzbrojenia. Podejmowane przez nich decyzje dotyczące konfiguracji łańcucha dostaw są w znacznym stopniu zależne od wymagań strony publicznej, wynikających z systemu planowania obronnego. W jego ramach Sztab Generalny Wojska Polskiego definiuje zdolności operacyjne Sił Zbrojnych RP, Ministerstwo Obrony Narodowej określa priorytety rozwoju potencjału obronnego i zapewnia finansowanie, natomiast Agencja Uzbrojenia przekłada te decyzje na konkretne programy pozyskania sprzętu wojskowego oraz kontrakty realizowane z przemysłem (rys. 2.8).

Jednocześnie zdolność do zapewnienia ciągłości dostaw jest w znacznym stopniu zależna od potencjału przedsiębiorstw tworzących kolejne ogniwa łańcucha dostaw – od integratorów, przez dostawców poziomu P1, po podmioty dostarczające krytyczne komponenty, materiały, technologie i surowce. Z tego względu ocena bezpieczeństwa łańcucha dostaw wymaga nie tylko identyfikacji jego uczestników i wzajemnych powiązań, ale przede wszystkim analizy ich potencjału oraz zdolności do długoterminowego zapewnienia ciągłości dostaw, gdyż łańcuch jest tak mocny jak jego najsłabsze ogniwo.

87 PITRADWAR S.A., „O firmie”. [online], dostęp: 19.03.2026, <https://www.pitradwar.com/o-firmie>; Urząd Patentowy RP, BUP 05/2026, zgłoszenie U1 nr 132299 „Podwójny moduł nadawczo - odbiorczy”, PIT-RADWAR S.A.; RADMOR S.A., „O nas”. [online], dostęp: 19.03.2026, https://www.radmor.com.pl/about/o_nas.



Rys. 2.8. Schemat łańcucha dostaw w polskim przemyśle obronnym

Na potrzeby niniejszego badania **potencjał przedsiębiorstw** zdefiniowano jako zespół zasobów, kompetencji i zdolności organizacyjnych, które umożliwiają podmiotom trwałe uczestnictwo w łańcuchach dostaw przemysłu obronnego, realizację złożonych projektów oraz adaptację do zmieniających się warunków otoczenia. Potencjał ten ma charakter wielowymiarowy i obejmuje zarówno elementy materialne (np. fabryki, linie produkcyjne), jak i niematerialne (technologie, kompetencje, *know-how*, zdolności zarządcze), a jego kluczową cechą jest zdolność zapewniania odporności (*resilience*) oraz budowania przewagi konkurencyjnej w warunkach wysokiej niepewności.

Przyjęto, iż na potencjał przedsiębiorstw składa się:

- 1. potencjał produkcyjny** rozumiany jako zdolność do wytwarzania określonych wyrobów w wymaganej ilości, jakości, czasie i konfiguracji technologicznej przy wykorzystaniu posiadanych zasobów; w przemyśle obronnym potencjał produkcyjny uwzględnia również zdolność do sprawnego skalowania produkcji w warunkach wzrostu popytu, mobilizacji lub zakłóceń w łańcuchu dostaw;
- 2. potencjał technologiczno-innowacyjny**, który oznacza zdolność do pozyskiwania, rozwijania, wdrażania i doskonalenia technologii niezbędnych do projektowania, produkcji, modernizacji oraz utrzy-

mania sprzętu wojskowego; w przemyśle obronnym przesądza on o suwerenności technologicznej;

- 3. potencjał kapitału ludzkiego** oznacza ilościowy i jakościowy zasób pracowników, ich kompetencji, doświadczenia, kwalifikacji oraz zdolność organizacji do pozyskiwania, utrzymania i rozwijania kompetencji niezbędnych do realizacji produkcji, działań badawczo-rozwojowych, logistycznych i zarządczych;
- 4. potencjał finansowy**, determinujący zdolność przedsiębiorstwa do finansowania działalności bieżącej i inwestycyjnej oraz absorpcji środków zewnętrznych;
- 5. potencjał do budowania ekosystemu partnerstw** z dostawcami, integratorami, instytucjami badawczymi, wojskiem oraz partnerami zagranicznymi w celu zapewniania ciągłości, jakości, elastyczności i odporności produkcji.

W badaniu skoncentrowano się na PGZ S.A. jako liderze konsorcjum PGZ-AMUNICJA, wraz ze spółkami ZM DEZAMED S.A., ME-SKO S.A., NITRO-CHEM S.A., BZE BELMA S.A. oraz ZPS GAMRAT sp. z o.o. zaangażowanymi w produkcję amunicji artyleryjskiej kalibru 155 mm, Hucie Stalowa Wola S.A. (również członku PGZ) jako producencie Bojowego Wozu Piechoty (BWP) BORSUK czy armatohauby (AHS) KRAB oraz WB Electronics S.A., producencie inteligentnego systemu kierowania do rażenia celów WAREMATE.

Analiza ta pozwala na identyfikację mocnych i słabych stron podmiotów oraz określenie efektywności ich funkcjonowania w coraz bardziej zintegrowanej i konkurencyjnej europejskiej przestrzeni przemysłowoobronnej.

Podczas analizy polskich przedsiębiorstw wykorzystano dane Głównego Urzędu Statystycznego (GUS), raporty roczne dostępne w Krajowym Rejestrze Sądowym (KRS) oraz dane z Portalu Przedsiębiorcy Sektora Obronnego⁸⁸. Europejskie dane makroekonomiczne zaczerpnięto z Europejskiej Agencji Obrony (European Defence Agency – EDA), dane branżowe z European Aerospace, Security and Defence Industries – ASD, a dane dotyczące sprawozdawczości przedsiębiorstw ze Sztokholmskiego Międzynarodowego Instytutu Badań nad Pokojem (Stockholm International Peace Research Institute – SIPRI). Korzystano też z danych bazy PONT-INFO

Wiele danych dotyczących przemysłu obronnego ma charakter szacunkowy, co wynika z ograniczeń związanych z identyfikacją pełnej populacji przedsiębiorstw oraz dostępnością informacji. Po pierwsze, nie wszystkie podmioty funkcjonujące w przemyśle obronnym w Polsce są klasyfikowane w odpowiednich kodach PKD, ponieważ część z nich formalnie prowadzi działalność w innych branżach (np. elektronice), mimo istotnego zaangażowania w produkcję na potrzeby obronności. Po drugie, specyfika branży, uwarunkowana względami bezpieczeństwa państwa oraz ochroną informacji o charakterze strategicznym, ogranicza dostęp do danych dotyczących przedsiębiorstw, w szczególności dostawców z wyższych poziomów łańcucha dostaw. W konsekwencji zastosowanie danych szacunkowych stanowi uzasadnione podejście metodologiczne, pozwalające na możliwie pełne odzwierciedlenie analizowanej branży.

2.2.1. Potencjał produkcyjny

W 2025 roku **wydatki Polski na obronność osiągnęły 166,2 mld PLN, czyli 4,3% PKB**, co jest najwyższym poziomem w NATO, wobec 3,76% PKB w 2024 roku. Jednocześnie budżet na 2026 rok zakłada około 4,8% PKB⁸⁹, przy czym wielkość popytową należy odróżnić od skali krajowej produkcji zbrojeniowej, która w 2024 roku wyniosła około 22,3 mld PLN i wzrosła o 47% rok do roku, co wobec PKB rządu 3,6 bln PLN daje relację rządu 0,6% PKB.

W 2024 roku **eksport uzbrojenia osiągnął rekordowe 3,14 mld EUR**, czyli o 79% więcej rok do roku. Dostawy trafiły do 59 krajów, w tym 79% na Ukrainę⁹⁰. W eksporcie dominują segmenty amunicji i artylerii, obrony powietrznej, radiolokacji oraz systemów bezzałogowych, przy utrzymującej się luce w mikroelektronice i optoelektronice.

Branża ma strukturę dualną, w której kontrolowana przez Skarb Państwa Polska Grupa Zbrojeniowa (PGZ) odpowiada za około 60% rynku, a silnie skoncentrowany sektor prywatny za około 40%⁹¹.

Centralną pozycję w branży zajmuje GK PGZ z przychodami ze sprzedaży na poziomie ok. 18,49 mld PLN w 2025 roku, która awansowała na 51. miejsce w zestawieniu SIPRI Top 100⁹². GK PGZ skupia ponad 50 spółek oraz posiada udziały w 32 innych spółkach. Największym podmiotem w grupie jest Huta Stalowa Wola S.A. (HSW), odpowiadająca za ok. 28% przychodów, której skonsolidowana sprzedaż w 2025 roku wzrosła o 63,3% r/r. Spółka specjalizuje się w produkcji Armatohaubicy Samobieżnej (AHS) KRAB, wież moździerzowych oraz Bojowego Wozu Piechoty (BWP) BORSUK. Drugą co do wielkości spółką w grupie PGZ jest Mesko S.A. – producent

88 <https://polishdefenceindustry.gov.pl/> (dostęp: 10.07.2026).

89 NATO (2026). The Secretary General's Annual Report 2025 (Aneks III: Defence Expenditure of NATO Countries 2014–2025), <https://www.nato.int/content/dam/hqo/webready/documents/publications-and-reports/annual-reports/sgar25-en.pdf> (dostęp: 6.07.2026).

90 MSZ (2025). Eksport uzbrojenia i sprzętu wojskowego z Polski. Raport za rok 2024, <https://www.gov.pl/web/dyplomacja/eksport-uzbrojenia-i-sprzetu-wojskowego-z-polski-raport-za-rok-2024> (dostęp: 6.07.2026).

91 Rogowski W. i in. (2026). Rola i znaczenie sektora bankowego w procesie finansowania działalności przedsiębiorców sektora obronnego. Sygn. PAB/WIB 17/2026 Rola i znaczenie sektora bankowego w procesie finansowania działalności przedsiębiorców sektora obronnego - Zespół Badań i Analiz Związku Banków Polskich (dostęp: 6.07.2026).

92 The SIPRI Top 100 ranking (2025) <https://www.sipri.org/visualizations/2026/sipri-top-100-ranking-2024>

amunicji, rakiet, pocisków oraz materiałów wybuchowych, która w 2025 roku zwiększyła skonsolidowane przychody ze sprzedaży o 41,7%⁹³.

Sektor prywatny w Polsce rozwija się bardzo dynamicznie i obejmuje kilkadziesiąt podmiotów, spośród których cztery odgrywają kluczową rolę, generując łącznie około 40% wartości całego rynku zbrojeniowego (co stanowi 70% sektora prywatnego). Wśród nich wskazać należy: WB Electronics S.A. (największą polską prywatną firmę zbrojeniową, obejmującą ponad 20 spółek w Polsce i za granicą), WSK PZL Świdnik Sp. z o.o. (część włoskiego koncernu Leonardo), Pratt & Whitney Rzeszów S.A. (należąca do amerykańskiego koncernu RTX) oraz PZL Sp. z o.o. Mielec (część amerykańskiej grupy Lockheed Martin).

W segmencie średnich przedsiębiorstw warto wymienić ZSP Niewiadów, zajmującą się sprzedażą amunicji, Advanced Protection Systems S.A. (APS) dostarczającą systemy antydronowe, radarowe i kinetyczne, które

wykrywają i neutralizują bezzałogowe statki powietrzne, czy Mista Sp. z o.o. – producenta pojazdów opancerzonych.

W Polsce obserwujemy również **dynamiczny wzrost małych i mikroprzedsiębiorstw** działających w przemyśle obronnym, które są dostawcami wyspecjalizowanych komponentów, technologii oraz usług, stanowiąc dostawców drugiego, trzeciego, a czasem również dalszych poziomów w łańcuchach dostaw. Ważne miejsce w portfolio przedsiębiorstw przemysłu obronnego zajmują również **licznie powstające start-upy**, koncentrujące się na innowacyjnych technologiach, elektronice wojskowej i systemach bezpieczeństwa. Warto wśród nich wymienić: DefendEye P.S.A., rozwijający systemy obserwacyjne i detekcyjne; Probus Group S.A., specjalizująca się w nowoczesnych rozwiązaniach balistycznych; Polski Holding Rozwojowy S.A., wspierający komercjalizację innowacji obronnych; RBL Defence Polska Sp. z o.o., produkujący systemy dronowe i modułowe schrony; oraz Terra Hexen Sp. z o.o. specjalizującą się w technologiach antydronowych.

Dobrym przykładem rozwoju potencjału produkcyjnego są inwestycje realizowane w PGZ, w tym rozbudowa i modernizacja mocy produkcyjnych Huty Stalowa Wola, nowe linie produkcyjne amunicji i prochu Mesko 400, rozbudowa mocy produkcyjnych PIT RADWAR oraz inwestycje w laboratorium Hardware-in-the-Loop dedykowane testom układów naprowadzania pocisków raketowych⁹⁴. PGZ wspólnie z Wojskowymi Zakładami Elektronicznymi S.A. inwestuje także w budowę Centrum Serwisowo-Produkcyjnego pocisków raketowych CAMM-ER oraz hali produkcyjnej elementów systemu obrony przeciwlotniczej i przeciwraketowej⁹⁵.

Mimo wielu pozytywnych zmian polski przemysł obronny dysponuje umiarkowanie rozwiniętym potencjałem produkcyjnym, który wymaga modernizacji. Mamy kilka wiodących podmiotów produkujących flagowe sprzęty oraz dynamicznie rozwijający się sektor prywatny. Jednak udział krajowej produkcji w zamówieniach Wojska Polskiego w 2025 roku był niski i kształtował się na poziomie ok. 35%⁹⁶, co wskazuje na dużą lukę między skalą zamówień a krajowymi zdolnościami

produkcyjnymi. Należy także nadmienić, że zagraniczne zakupy sprzętu są skoncentrowane geograficznie w niewielu wybranych krajach (np. USA), co wiąże się z ryzykiem. Ponadto nie wykorzystujemy potencjału eksportowego. Mimo spektakularnych wzrostów eksportu sprzętu wojskowego na rynki globalne (w ostatnich pięciu latach nawet 4000%), nasz udział w rynku eksportowym UE nadal wynosi poniżej 1%⁹⁷.

93 FinancialCraft Analytics (2025). Rynek zbrojeniowy w Polsce w 2024 roku, <https://financialcraft.pl/rynek-zbrojeniowy-w-polsce-2024-raport/> (dostęp: 6.07.2026).

94 <https://grupapgz.pl/o-nas/misja-i-wizja/>

95 <https://polska-zbrojna.pl/home/articleshow/46039?t=Fabryka-pociskow-ziemia-powietrze>

96 Rogowski W. i in. (2026). Rola i znaczenie sektora bankowego w procesie finansowania działalności przedsiębiorców sektora obronnego. Sygn. PAB/WIB 17/2026

97 MSZ (2025). Eksport uzbrojenia i sprzętu wojskowego z Polski. Raport za rok 2024, <https://www.gov.pl/web/dyplomacja/eksport>

Warto zaznaczyć, że rozwijanie potencjału produkcyjnego wymaga wysokich nakładów. Warszawski Instytut Bankowości oszacował, iż 10-15 mld PLN rocznie potrzebne jest na modernizację linii produkcyjnych, urządzeń i automatyki, 5-8 mld PLN rocznie na technologie informatyczne i cyberbezpieczeństwo, oraz 2-4 mld PLN rocznie na rozwój kompetencji pracowniczych⁹⁸. Niewątpliwą szansą jest perspektywa utrzymania wydatków na obronność do 2030 roku, dostępność funduszy unijnych oraz zwiększanie współpracy w ramach programów obronnych w UE.

2.2.2. Potencjał technologiczno-innowacyjny

Potencjał produkcyjny odzwierciedla bieżącą zdolność przedsiębiorstwa do realizacji procesów wytwórczych, jednak sam w sobie nie zapewnia długookresowej przewagi konkurencyjnej ani odporności przedsiębiorstwa. Dlatego w przypadku przemysłu obronnego szczególnego znaczenia nabiera zdolność do tworzenia, rozwijania i wdrażania nowych rozwiązań technicznych, a także ich materializacji w postaci produktów odpowiadających aktualnym wymaganiom operacyjnym wojska jako użytkownika.

Istotnym czynnikiem kształtującym potencjał technologiczno-innowacyjny jest intensywność nakładów na badania i rozwój (B+R), które przyczyniają się do budowy suwerenności technologicznej, uniezależnienia od zewnętrznych dostawców, wzmacniają krajowy przemysł obronny oraz podnoszą poziom innowacyjności.

W Polsce od 2020 roku wydatki na obronność rosły szybciej niż w innych krajach NATO, a w 2025 roku osiągnęły poziom 4,3% PKB. Niestety, od kilkunastu lat wzrost poziomu nakładów publicznych na B+R w obszarze obronności nie nadąża za wzrostem

całkowitych wydatków na obronność i wciąż pozostaje on poniżej 1%, co może być kluczową barierą dla rozwoju innowacyjnego przemysłu obronnego w Polsce⁹⁹.

Warto zauważyć, że **w 2025 roku wydatki na B+R wyniosły 1,198 mld PLN** (0,71% łącznych wydatków na obronność), jednak w tym samym roku rząd udzielił 7,63 mld PLN wsparcia z Funduszu Inwestycji Kapitałowych (FIK) spółkom GK PGZ na rozbudowę zdolności produkcyjnych. Podpisano 14 umów inwestycyjnych na lata 2025–31, dzięki którym ma być prowadzona produkcja systemów Nawew, amunicji 155 mm, min, czołgów K2PL i wozów towarzyszących na podwoziu K2, ciężarówek Jelcz, bezzałogowych wież ZSSW-30 oraz pojazdów opancerzonych¹⁰⁰.

Poziom nakładów na działalność B+R stanowi istotny, lecz niewystarczający miernik potencjału technologiczno-innowacyjnego przedsiębiorstw przemysłu obronnego. O rzeczywistej zdolności do budowania przewagi konkurencyjnej i wzmacniania bezpieczeństwa państwa decyduje przede wszystkim **zdolność do projektowania oraz rozwijania własnych, zaawansowanych technologicznie systemów uzbrojenia i rozwiązań cyfrowych**, których kluczowe komponenty – w szczególności oprogramowanie, algorytmy, systemy dowodzenia, sensory oraz technologie integracyjne – pozostają pod kontrolą krajową. To właśnie takie produkty tworzą podstawę suwerenności technologicznej, rozumianej jako zdolność państwa do samodzielnego rozwijania, wytwarzania, modernizacji i utrzymania krytycznych zdolności obronnych przy ograniczonej zależności od zagranicznych dostawców. Jednym z mierników innowacyjności mogą być patenty, które zostały przeanalizowane w rozdziale 2.1.7.

t-uzbrojenia-i-sprzetu-wojskowego-z-polski-raport-za-rok-2024 (dostęp: 6.07.2026).

98 Podkomisja stała do spraw polskiego przemysłu obronnego oraz modernizacji technicznej Sił Zbrojnych RP (OBN04S), Sejm Rzeczypospolitej Polskiej, <https://www.sejm.gov.pl/sejm10.nsf/PosKomZrealizowane.xsp?komisja=OBN04S#4> (dostęp: 10.07.2026).

99 <https://pfr.pl/artykul/przeglad-danych-o-wydatkach-na-obronnosc-i-technologie-dual-use-w-polsce>

100 Dmitruk, T. (2026). Wydatki obronne Polski w 2025 roku. Dziennik Zbrojny 06.06.2026. <https://dziennikzbrojny.pl/artykuly-art-2,4,12298,armie-swiata,wojsko-polskie,wydatki-obronne-polski-w-2025-roku> (dostęp 10.07.2026).

W polskim przemyśle obronnym do najbardziej zaawansowanych rozwiązań należą m.in. system rozpoznawczo-uderzeniowy GLADIUS, system kierowania walką TOPAZ oraz amunicja krążąca WARMATE, opracowane przez Grupę WB¹⁰¹. Przykładami wysokich kompetencji technologicznych są również radary z aktywnym skanowaniem elektronicznym Bystra i Sajna, rozwijane przez PIT-RADWAR S.A.¹⁰², przeciwlotniczy zestaw rakietowy Piorun, produkowany przez Mesko S.A.¹⁰³, a także bojowy wóz piechoty Borsuk wraz z bezzałogowym systemem wieżowym ZSSW-30, rozwijane przez Hutę Stalowa Wola S.A. we współpracy z partnerami przemysłowymi¹⁰⁴. Wspólną cechą tych rozwiązań jest wysoki udział krajowej myśli technicznej oraz własności intelektualnej, co ogranicza ryzyko wynikające z zależności technologicznych, zwiększa możliwości dalszego rozwoju produktów oraz wzmacnia odporność krajowych łańcuchów dostaw w długim okresie.

Warto podkreślić, że o suwerenności technologicznej nie decyduje sama zdolność do produkcji platform uzbrojenia (np. pojazdu czy armatohauby), lecz kontrola nad technologiami o najwyższej wartości dodanej – oprogramowaniem, elektroniką, sensorami, systemami C4ISR, sztuczną inteligencją, technologiami rakietowymi czy zaawansowanymi materiałami. Z tego punktu widzenia produkty takie jak GLADIUS, TOPAZ czy radary PIT-RADWAR mają strategiczne znaczenie większe niż mogłaby sugerować ich wartość produkcyjna, ponieważ koncentrują krajowe kompetencje w obszarach najtrudniejszych do pozyskania z zagranicy i najistotniejszych dla długoterminowej autonomii technologicznej.

Zasadne jest, aby polskie przedsiębiorstwa przemysłu obronnego **intensyfikowały działania ukierunkowane na rozwój potencjału technologiczno-innowacyjnego**, szczególnie w obszarach technologii krytycznych, obejmujących m.in. systemy dowodzenia i komunikacji (C4ISR), sensorykę, mikroelektronikę, zaawansowaną elektronikę, technologie cyfrowe, sztuczną inteligencję, systemy autonomiczne oraz technologie rakietowe i materiałowe. Rozwój tych kompetencji pozwala ograniczyć ryzyko strategicznej zależności technologicznej od podmiotów zagranicznych oraz wzmocnić odporność krajowych łańcuchów dostaw¹⁰⁵.

Istotnym kierunkiem rozwoju jest również **zwiększanie zdolności przedsiębiorstw do opracowywania technologii podwójnego zastosowania (dual-use)**, które znajdują zastosowanie zarówno w sektorze wojskowym, jak i cywilnym. Technologie te sprzyjają efektywniejszemu wykorzystaniu potencjału badawczo-rozwojowego, dywersyfikacji źródeł przychodów oraz utrzymaniu i rozwojowi krajowych kompetencji technologicznych,

wzmacniając tym samym długoterminową odporność przemysłowej bazy obronnej.

2.2.3. Potencjał kapitału ludzkiego

Potencjał kapitału ludzkiego polskiego przemysłu obronnego obejmuje zasób pracowników, ich kompetencje, doświadczenie i kwalifikacje, a także zdolność przedsiębiorstw do pozyskiwania, utrzymywania i rozwijania kadr potrzebnych do realizacji produkcji, działalności badawczo-rozwojowej, procesów logistycznych, serwisowych i zarządzania złożonymi projektami. Jego znaczenie rośnie wraz z rozbudową mocy produkcyjnych i transformacją technologiczną w branży. Inwestycje w nowe linie produkcyjne i technologie nie prowadzą do zwiększenia zdolności wytwórczych, jeżeli nie towarzyszy im zapewnienie odpowiednio przygotowanych pracowników.

Z perspektywy bezpieczeństwa łańcuchów dostaw kluczowe znaczenie ma **odporność kompetencyjna**, rozumiana jako zdolność przedsiębiorstwa i całego łańcucha dostaw

101 <https://www.wbgroup.pl/produkt/system-gladius/>

102 <https://portal-mundurowy.pl/index.php/innowacje-i-biznes/howosci-pit-radwar-sa-radar-wielofunkcyjny-kierowania-ogniem-sajna>

103 <https://forsa.pl/kraj/bezpieczenstwo/artykuly/10633974,polski-piorun-bije-rekordy-polnoc-nato-stawia-na-nasze-rakiety.html>

104 <https://www.wojsko-polskie.pl/bwp-borsuk/>

105 Polska buduje suwerenność amunicyjną. PGZ tworzy spółkę z francuskim gigantem, <https://radar.rp.pl/modernizacja-sil-zbrojnych/art44615451-polska-buduje-suwerennosc-amunicyjna-pgz-tworzy-spolke-z-francuskim-gigantem>

do utrzymania kompetencji niezbędnych do zapewnienia ciągłości działania, zwiększenia skali produkcji oraz odtworzenia zdolności po wystąpieniu zakłócenia. Kapitał ludzki wpływa bezpośrednio na jakość wyrobów, możliwość uruchamiania dodatkowych zmian produkcyjnych, ciągłość serwisowania sprzętu oraz zdolność dostosowywania produkcji do potrzeb Sił Zbrojnych RP.

Monitorowanie odporności wymaga uwzględnienia dostępności kompetencji krytycznych, procesów zależnych od pojedynczych ekspertów, struktury wieku, rotacji, czasu rekrutacji i przygotowania pracowników, dostępności zastępstw oraz skuteczności sukcesji. Obserwacja tych wskaźników pełni funkcję systemu wczesnego ostrzegania przed ograniczeniem elastyczności zdolności produkcyjnych.

Dane z rynku pracy wskazują na niedobór pracowników w niektórych zawodach technicznych oraz na **rosnące znaczenie pozyskiwania i utrzymywania specjalistycznych kompetencji**¹⁰⁶. Przemysł obronny konkuruje o pracowników z branżami motoryzacyjną, lotniczą, energetyczną, maszynową i ICT. Poszukiwane są kompetencje związane z obróbką metali, spawalnictwem, mechaniką, chemią, materiałami wysokoenergetycznymi, utrzymaniem ruchu i zapewnieniem jakości, a także z elektroniką, automatyką, cyberbezpieczeństwem, oprogramowaniem, analizą danych i sztuczną inteligencją. W branży widoczny jest wzrost aktywności rekrutacyjnej związany z rosnącą skalą zamówień i rozbudową potencjału produkcyjnego¹⁰⁷.

Dla odporności łańcuchów dostaw istotne są struktura kompetencji, możliwość obsadzenia kluczowych stanowisk oraz **czas potrzebny na przygotowanie pracowników** do

zadań wymagających znajomości specjalistycznych technologii, procedur bezpieczeństwa i standardów jakości.

Dodatkowym wyzwaniem jest **luka pokoleniowa** związana z odchodzeniem doświadczonych pracowników i niedostatecznie szybkim przygotowywaniem ich następców. Dotyczy to zwłaszcza konstruktorów systemów uzbrojenia, technologów procesów specjalnych, specjalistów materiałów wysokoenergetycznych, integratorów systemów, pracowników laboratoriów oraz osób odpowiedzialnych za testowanie i dopuszczanie wyrobów. Kompetencje te wymagają wieloletniego doświadczenia, a uzależnienie procesu od niewielkiej liczby ekspertów może tworzyć wąskie gardła kadrowe.

Przedsiębiorstwa łączą bieżącą rekrutację z budowaniem własnych źródeł przyszłych pracowników. Huta Stalowa Wola S.A. prowadzi staże i praktyki dla uczniów, studentów i absolwentów¹⁰⁸, MESKO S.A. oferuje praktyki i staże osobom związanym z kształceniem technicznym¹⁰⁹, a NITRO-CHEM S.A. w ramach współpracy z Politechniką Bydgoską organizuje praktyki studenckie i staże krótkoterminowe¹¹⁰.

Firmy rozwijają również kompetencje obecnych pracowników. Huta Stalowa Wola S.A. prowadzi szkolenia specjalistyczne, miękkie i menedżerskie oraz dofinansowuje studia i kursy¹¹¹. MESKO S.A. realizuje szkolenia warsztatowe i program sukcesji, wspierając pracowników podnoszących kwalifikacje¹¹². Grupa WB deklaruje możliwość rozwoju zawodowego i udziału w szkoleniach¹¹³. Działania te sprzyjają utrzymywaniu wiedzy w organizacji oraz przygotowywaniu następców.

106 Barometr zawodów 2025. Raport podsumowujący badanie w Polsce, Wojewódzki Urząd Pracy w Krakowie, Kraków 2024, badanie zrealizowane na zlecenie Ministerstwa Rodziny, Pracy i Polityki Społecznej; <https://info.randstad.pl/hubfs/Randstad%20Enterprise%202025%20Talent%20Trends%20Report%20-%20PL.pdf.pdf?hsLang=pl-pl>

107 <https://businessinsider.com.pl/praca/lawina-rekrutacji-w-polskiej-zbrojeniowce-najwieksi-gracze-szukaja-specjalistow/0b2jjb9>

108 <https://www.hsw.pl/kariera/staze-i-praktyki/>

109 <https://www.mesko.com.pl/kariera/realizuj-sie-z-nami/praktyki-i-staze>

110 <https://pbs.edu.pl/pl/aktualnosc/nitro-chem-zaciesnia-wspolprace-z-politechnika-bydgoska>

111 <https://www.hsw.pl/kariera/staze-i-praktyki/>

112 <https://www.mesko.com.pl/kariera/realizuj-sie-z-nami/praktyki-i-staze>

113 <https://pbs.edu.pl/pl/aktualnosc/nitro-chem-zaciesnia-wspolprace-z-politechnika-bydgoskahttps://kariera.wbgroup.com/>

Znaczenie mają także kompetencje inżynierskie, laboratoryjne i badawczo-rozwojowe. Oferty pracy Grupy WB obejmują stanowiska związane z projektowaniem architektury systemów oraz integracją komponentów sprzętowych i oprogramowania¹¹⁴. BELMA S.A. posiada własne biura konstrukcyjne zatrudniające specjalistów z zakresu mecha-

ki, elektrotechniki i elektroniki¹¹⁵. DEZAMET S.A. dysponuje laboratorium badawczym, które prowadzi badania analityczne, pomiarowe i materiałowe, wspierające doskonalenie wyrobów¹¹⁶, natomiast ZPS GAMRAT realizuje projekty badawczo-rozwojowe i rozwija kompetencje laboratoryjne¹¹⁷.

MESKO S.A. współpracuje z Politechniką Świętokrzyską przy badaniach i projektach badawczo-rozwojowych¹¹⁸. Współpraca NITRO-CHEM S.A. z Politechniką Bydgoską obejmuje praktyki, wspólne prace badawcze, seminaria i prace dyplomowe¹¹⁹. Huta Stalowa Wola S.A. prowadzi program stypendialny skierowany do osób kształcących się w obszarach odpowiadających potrzebom spółki, a współpraca Grupy WB z Politechniką Gdańską obejmuje działania dydaktyczne, naukowe, badawczo-rozwojowe i produkcyjne¹²⁰. Przykłady te pokazują, że relacje z systemem edukacji służą jednocześnie pozyskiwaniu przyszłych pracowników i rozwijaniu zaplecza technologicznego przedsiębiorstw.

Odporność kompetencyjna powinna być analizowana nie tylko u integratorów, lecz także u dostawców w górze łańcucha dostaw (P1, P2 i P3). Niedobór specjalistów u producenta komponentów, przedsiębiorstwa elektronicznego lub materiałowego, laboratorium albo podmiotu działającego w obszarze technologii dual-use może zakłócić funkcjonowanie całego łańcucha, nawet jeżeli integrator dysponuje wystarczającym kapitałem ludzkim.

Potencjał kapitału ludzkiego ma również wymiar międzynarodowy. Udział polskich przedsiębiorstw w europejskich i transatlantyckich sieciach dostaw oraz w projektach realizowanych w ramach EDF, SAFE i planowanych rozwiązań EDIP zwiększa zapotrzebowanie na kompetencje związane z zarządzaniem projektami międzynarodowymi, certyfikacją, ochroną własności intelektualnej, kontrolą eksportu oraz pracą w wielonarodowych zespołach.

Uzupełniającym źródłem kadr może być mobilność międzybranżowa, szczególnie z motoryzacji, lotnictwa, przemysłu maszynowego, energetyki i sektora ICT. Kompetencje związane z produkcją seryjną, automatyką,

zapewnieniem jakości, utrzymaniem ruchu, elektroniką i tworzeniem oprogramowania mogą być wykorzystywane po odpowiednim przygotowaniu pracowników do specyfiki sektora obronnego. Programy przekwalifikowania i skrócone ścieżki adaptacyjne mogłyby ułatwiać szybkie zwiększanie zatrudnienia.

W perspektywie długoterminowej zasadne jest **rozwijanie programów pozyskiwania kadr technicznych**, łączących działania przedsiębiorstw, szkół branżowych, techników, uczelni i administracji publicznej. Programy te mogłyby obejmować m.in. klasy patronackie, kształcenie dualne, programy stypendialne, kierunki kształcenia odpowiadające potrzebom sektora oraz mechanizmy przekwalifikowania pracowników z branż pokrewnych.

Przygotowanie do kryzysu lub mobilizacji wymagałoby identyfikacji stanowisk i kompetencji krytycznych, określenia minimalnej obsady procesów, przygotowania zastępstw, dokumentowania wiedzy oraz analizy czasu potrzebnego na szkolenie nowych pracowników. Jednym z możliwych rozwiązań jest czasowe angażowanie doświadczonych

¹¹⁴ <https://www.wbgroup.pl/kariera-2/page/2/>

¹¹⁵ <https://www.belma.pl/>

¹¹⁶ <https://dezamet.com.pl/uslugi/laboratorium-badawcze>

¹¹⁷ <https://zpsgamrat.pl/projekty-badawczo-rozwojowe/>

¹¹⁸ <https://www.mesko.com.pl/aktualnosci/wspolpraca-przemyslu-i-nauki>

¹¹⁹ <https://pbs.edu.pl/pl/aktualnosc/nitro-chem-zaciesnia-wspolprace-z-politechnika-bydgoska>

¹²⁰ <https://www.wbgroup.pl/aktualnosci/grupa-wb-i-politechnika-gdanska-podpisaly-umowe-o-wspolpracy/>

emerytowanych pracowników oraz byłych specjalistów do szkolenia nowych kadr, sprawowania nadzoru technologicznego, prowadzenia kontroli jakości i uruchamiania dodatkowych zmian produkcyjnych.

Długookresowa odporność zależy także od **zdolności do przyciągania i zatrzymywania młodych pracowników**. Znaczenie mają możliwości udziału w zaawansowanych technologicznie projektach, rozwój zawodowy, czytelne ścieżki kariery oraz stabilność zatrudnienia. Istotne jest również tworzenie zespołów wielopokoleniowych, które umożliwiają przekazywanie wiedzy przed odejściem najbardziej doświadczonych specjalistów.

Potencjał kapitału ludzkiego polskiego przemysłu obronnego jest wzmacniany poprzez rekrutację, **rozwój obecnych pracowników oraz współpracę z systemem edukacji**. Jego trwałość zależy jednak przede wszystkim od utrzymania kompetencji krytycznych, skutecznego transferu wiedzy, ograniczenia zależności od pojedynczych ekspertów oraz zdolności pozyskania dodatkowych kadr w okresie zwiększonego zapotrzebowania. Odporność kompetencyjna na wszystkich poziomach łańcucha dostaw stanowi jeden z podstawowych warunków zapewnienia ciągłości dostaw dla Sił Zbrojnych RP.

2.2.4. Potencjał finansowy

Potencjał finansowy stanowi kolejny bardzo istotny wymiar oceny zdolności polskich przedsiębiorstw do trwałego pełnienia roli liderów łańcuchów dostaw w przemyśle

obronnym. Określa on zdolność podmiotów do finansowania działalności bieżącej i inwestycyjnej, realizacji dużych, wieloletnich kontraktów oraz absorpcji środków zewnętrznych, w tym instrumentów wsparcia Unii Europejskiej. W warunkach skokowego wzrostu zamówień i konieczności szybkiego skalowania zdolności produkcyjnych to właśnie kondycja finansowa decyduje o tym, czy potencjał strategiczny i kompetencyjny może zostać przełożony na realne dostawy. Analizę oparto na jednostkowych i skonsolidowanych sprawozdaniach finansowych badanych podmiotów za lata 2023–2025, a uzyskane wyniki odniesiono do benchmarków europejskich oraz średnich branżowych ustalonych w oparciu o dane pozyskane z bazy PONT-INFO.

Ogólna charakterystyka sytuacji finansowej i wyników

Ostatnie lata przyniosły wyjątkowo silną poprawę wyników finansowych całego badanego grona podmiotów, będącą bezpośrednią pochodną cyklu zbrojeniowego zapoczątkowanego po 2022 roku. Większość analizowanych podmiotów odnotowała w 2025 roku dwucyfrową dynamikę przychodów, znacząco przewyższającą poziomy wzrostu obserwowane w przypadku firm z Europy Zachodniej. Przychody Grupy PGZ wzrosły z 13,94 mld zł do 18,49 mld zł (+32,7%), natomiast Grupy WB Electronics - po skokowym wzroście w 2024 roku - obniżyły się nieznacznie z 2,96 mld zł do 2,86 mld zł (-3,5%), pozostając jednak na ponad dwukrotnie wyższym poziomie niż w 2023 roku.

WB Electronics odnotowała w 2024 roku wzrost przychodów o 106,5% (z 1,43 do 2,96 mld zł) a w 2025 roku utrzymała przychody na poziomie 2,86 mld zł, zwiększając zysk netto do 679 mln zł (wobec 623 mln zł rok wcześniej), co odzwierciedla wejście w fazę stabilnej realizacji dużych kontraktów. **MESKO S.A.** zwiększyło w 2025 roku przychody o 41,7% (do 3,85 mld zł), a zysk netto ponad dwukrotnie (z 421 do 933 mln zł), co potwierdza efekt uruchomienia produkcji amunicji w odpowiedzi na popyt kontraktowy. **BZE Belma S.A.** – mniejszy podmiot konsorcjum – zwiększyła w 2025 roku przychody o 43,5% (do 262 mln zł) i podniosła zysk netto do 85 mln zł (z 61 mln zł rok wcześniej), co pokazuje, że dynamika cyklu zbrojeniowego objęła również niższe szczeble łańcucha dostaw.

Wzrostowi skali towarzyszyła poprawa efektywności. Marża EBITDA badanych podmiotów uplasowała się wyraźnie powyżej benchmarku UE (8-15%): od ok. 21% w HSW

i 24,5% w PGZ po niemal 34% w WB i ok. 42% w spółce Gamrat. Tak wysoka zyskowność jest efektem łącznego oddziaływania efektów skali, struktury premiowej kontraktów

obronnych oraz korzystnej pozycji negocjacyjnej dostawców w warunkach silnego popytu. Z perspektywy oceny potencjału finansowego oznacza to, że badane podmioty wkraczają w okres intensywnych inwestycji z pozycji wysokiej zyskowności i znacznej zdolności do samofinansowania.

Warto podkreślić, że omawiane tendencje, tzn. wzrost zyskowności przy jednoczesnym zwiększaniu skali działalności, są widoczne w przypadku całego przemysłu zbrojeniowego. Wskaźniki opłacalności dla branży plasują się powyżej poziomów notowanych w przemyśle¹²¹.

Obraz przepływów pieniężnych jest jednak bardziej zróżnicowany. O ile w Mesko i Dezamecie operacyjne przepływy pieniężne w 2025 roku nadal przewyższały EBITDA (m.in. dzięki rozliczeniu zaliczek kontraktowych), a w WB Electronics relacja tych dwóch parametrów poprawiła się z ok. 0,49 do ok. 1,4, o tyle w Grupie PGZ gotówka operacyjna pokrywała ok. 78% EBITDA, a w Hucie Stalowa Wola przepływy operacyjne były ujemne. Wynika to z silnego zaangażowania środków w kapitał obrotowy (przede wszystkim zapasy) w fazie dynamicznego wzrostu produkcji. Jest to typowa cecha przedsiębiorstw rozwijających się w cyklu zbrojeniowym: wysoki wynik księgowy nie przekłada się automatycznie na nadwyżkę gotówkową, co czyni dostęp do finansowania kapitału obrotowego jednym z kluczowych czynników warunkujących zdolność realizacji zamówień.

Diagnostyka finansowa

Ocena kondycji finansowej w czterech klasycznych obszarach – płynności finansowej, sprawności zarządzania, zadłużenia i rentowności – ogólnie potwierdza dobry standing badanych podmiotów. **W zakresie płynności finansowej** sytuacja jest dość zróżnicowana. Wskaźniki z tego obszaru przyjmują wartości od uznawanych za umiarkowane, choć akceptowalne (np. ok. 1,4 HSW, przy wyraźnej poprawie w Dezamecie z ok. 1,1 do 1,8) do sugerujących nadpłynność

z racji kilkukrotnie większych aktywów obrotowych niż zobowiązania krótkoterminowe (Belma, Nitro-Chem, Gamrat), przy 1,50 na poziomie Grupy PGZ i 1,89 w Grupie WB. Bardziej wymowny jest wskaźnik płynności szybkiej, który w PGZ i HSW utrzymuje się poniżej 1 (odpowiednio 0,88 i 0,85), podczas gdy w MESKO poprawił się z 0,74 do 1,06, co oznacza, że płynność tych podmiotów jest w istotnym stopniu podtrzymywana przez zapasy – aktywa o niższej zbywalności i dłuższym czasie konwersji na gotówkę.

W obszarze sprawności zarządzania uwagę zwraca w większości przypadków długi cykl konwersji gotówki. Wydłużenie cyklu jest naturalną konsekwencją jednostkowego i małoseryjnego charakteru produkcji oraz konieczności gromadzenia materiałów i komponentów o długim czasie dostawy. Generuje ono jednak wysokie zapotrzebowanie na finansowanie kapitału obrotowego i stanowi jedną z głównych determinant popytu na kredyt obrotowy. W 2025 roku cykl konwersji gotówki w Grupie PGZ wydłużył się do ok. 447 dni, głównie wskutek dalszej rozbudowy zapasów pod realizowane kontrakty. Relatywnie korzystnie wypada natomiast krótki cykl inkasa należności (kilkanaście-kilkadziesiąt dni), wynikający z dominacji jednego wiarygodnego odbiorcy publicznego oraz powszechnego stosowania mechanizmów zaliczkowych. Warto jednocześnie zaznaczyć, że w przypadku kilku z analizowanych podmiotów miało miejsce istotne skrócenie cyklu, co znacząco wpływa na poprawę ich płynności oraz ogólnej kondycji finansowej.

W zakresie zadłużenia badane podmioty cechuje fundamentalna prawidłowość: wysokie zadłużenie ogółem ma charakter niemal wyłącznie operacyjny (zaliczki, zobowiązania wobec dostawców), a nie finansowy. Wskaźnik długu finansowego netto do EBITDA jest we wszystkich analizowanych przypadkach ujemny (od -1,5 w WB po -3,7 w HSW i -4,4 w PGZ), co oznacza, że posiadane środki pieniężne przewyższają zadłużenie wynikające z kredytów, pożyczek, obligacji i innych instrumentów finansowych. Branża funkcjonuje zatem w praktyce niemal bez

121 Rogowski W. i in. (2026). Rola i znaczenie sektora bankowego w procesie finansowania działalności przedsiębiorców sektora obronnego. Sygn. PAB/WIB 17/2026

klasycznego długu bankowego. Obserwacja ta ma podwójne znaczenie: z jednej strony świadczy o niskim ryzyku finansowym i komfortowej zdolności do obsługi zobowiązań, z drugiej zaś wskazuje, że potencjał absorpcji finansowania dłużnego pozostaje duży, a jego dotychczasowe wykorzystanie – niewielkie. Jednocześnie warto zaznaczyć, że ni-

ski poziom finansowania dłużnego w bilansach badanych przedsiębiorstw nie oznacza braku współpracy z instytucjami finansowymi, bowiem ta wyraża się zazwyczaj w udzielanych na zlecenie firm zbrojeniowych gwarancjach bankowych, chociażby z tytułu wadium, zwrotu otrzymanych zaliczek czy dobrego wykonania kontraktu.

Grupa PGZ wykazywała w 2025 roku wskaźnik długu finansowego netto do EBITDA na poziomie -4,4, przy środkach pieniężnych na koniec okresu rzędu 21,0 mld zł – znacznie przewyższających zadłużenie finansowe; oznacza to pozycję gotówki netto i praktyczny brak klasycznego długu bankowego. **Huta Stalowa Wola** osiągnęła wskaźnik na poziomie -3,7, co przy nadal wysokim zadłużeniu ogółem (relacja zobowiązań do kapitału własnego 2,4) potwierdza, że źródłem wysokiego zadłużenia są zobowiązania operacyjne i kontraktowe, a nie finansowe. **WB Electronics** – mimo modelu rynkowego – również utrzymywała pozycję gotówki netto (-1,5), zachowując relację zadłużenia do kapitału własnego na poziomie ok. 1,0 dzięki dalszemu silnemu wzrostowi kapitału własnego.

Najmocniejszą stroną pozostają zyskowność i rentowność. Rentowność kapitału własnego (ROE) wahała się w ostatnich latach od ok. 17% w PGZ, 28–30% w HSW i MESKO, ponad 41% w WB Electronics, a rentowność aktywów (ROA) wzrosła r/r w większości badanych podmiotów. Rosnąca rentowność jest bezpośred-

nią pochodną wzrostu wolumenów, efektów skali oraz korzystnej struktury kontraktów i – z perspektywy potencjału finansowego – stanowi najsilniejszy argument przemawiający za zdolnością badanych podmiotów do finansowania dalszego rozwoju, zarówno ze środków własnych, jak i zewnętrznych.

WB Electronics osiągnęła w 2025 roku ROE na poziomie 41,5% (wobec 57,6% rok wcześniej) oraz marżę netto 23,8% – wyniki zbliżone do profilu spółki technologicznej o wysokiej dynamice wzrostu. **MESKO S.A.** podniosło ROE z 26,6% do 30,0% i marżę netto z 15,5% do 24,2%, co odzwierciedla skokową poprawę efektywności wraz ze wzrostem skali produkcji. **Grupa PGZ** – ze względu na kapitałochłonność i skalę holdingu państwowego – osiągnęła niższe, lecz rosnące ROE (17,1%) oraz marżę EBITDA 24,5%, utrzymując się powyżej benchmarku europejskiego.

Ocena potencjału rozwojowego i inwestycyjnego

Zdolność badanych podmiotów do zwiększania skali działalności, finansowania inwestycji (CAPEX, B+R) oraz realizacji dużych kontraktów opiera się obecnie na trzech filarach: wysokiej rentowności i zdolności do samofinansowania, niskim poziomie zadłużenia finansowego oraz silnej pozycji kapitałowej. Kapitał własny Grupy PGZ wzrósł w 2025 roku do 16,36 mld zł (przy 8,70 mld zł na koniec 2023), a WB Electronics – do 1,64 mld zł (z 0,51 mld zł 2023), przy jednoczesnym utrzymaniu pełnego pokrycia aktywów trwałych kapitałem własnym (wskaźnik powyżej 1,0 we wszystkich badanych podmiotach). Oznacza to, że majątek trwały jest finansowany kapitałem o charakterze stałym, co stanowi korzystną i bezpieczną strukturę finansowania inwestycji.

Niemal zerowe zadłużenie finansowe netto tworzy znaczną przestrzeń do zaciągania długu inwestycyjnego. Przy obecnych poziomach EBITDA badane podmioty dysponują teoretyczną zdolnością do pozyskania finansowania dłużnego rzędu kilku krotności rocznej EBITDA bez przekroczenia ostrożnościowych progów zadłużenia (dług netto/EBITDA $\leq 3,5$). Stanowi to istotną rezerwę finansowania rozwoju, szczególnie w kontekście wieloletnich programów modernizacji technicznej Sił Zbrojnych RP. Modele finansowania rozwoju pozostają jednak odmienne: PGZ opiera się przede wszystkim na zapleczu właścicielskim Skarbu Państwa oraz dokapitalizowaniu, podczas gdy WB Electronics łączy finansowanie rynkowe z przychodami eksportowymi i aktywnością projektową.

Swego rodzaju wyzwaniem pozostaje natomiast ograniczona zdolność do długoterminowego finansowania dłużnego dopasowanego do wieloletnich cykli produkcyjnych. Zobowiązania badanych podmiotów mają w przeważającej mierze charakter krótkoterminowy, co można uznać za strukturalne niedopasowanie terminowe – krótkoterminowe finansowanie przy wieloletnich kontraktach. Lukę tę mogłyby wypełnić długoterminowe finansowanie inwestycyjne oraz elastyczne instrumenty finansowania kapitału obrotowego uwzględniające specyfikę kontraktów publicznych.

Znaczenie kondycji finansowej dla bezpieczeństwa łańcucha dostaw

Kondycja finansowa liderów łańcuchów dostaw przekłada się bezpośrednio na zdolność do utrzymania ciągłości produkcji, odporność na szoki oraz stabilność relacji z dostawcami. Wysoka rentowność i nadwyżki gotówkowe głównych integratorów ograniczają ryzyko przerwania produkcji z przyczyn finansowych i zwiększają zdolność do absorbowania wahań kosztów surowców, energii i komponentów. Jednocześnie jednak długi cykl konwersji gotówki i rosnące zaangażowanie kapitału obrotowego sprawiają, że stabilność finansowa liderów w istotnym stopniu zależy od sprawnego rozliczania kontraktów przez zamawiającego.

Istotnym sygnałem ostrzegawczym jest obserwowane w skali branży wydłużanie cyklu regulowania zobowiązań wobec dostawców.

Tendencja ta wskazuje na możliwość przenoszenia napięć płynnościowych z integratorów na dostawców i kooperantów, którzy – w przeciwieństwie do liderów – dysponują znacznie słabszą pozycją kapitałową oraz ograniczonym dostępem do finansowania. **W praktyce oznacza to, że najsłabszym ogniwem bezpieczeństwa finansowego łańcucha dostaw nie są integratorzy, lecz mniejsze przedsiębiorstwa sektora MŚP, których kondycja decyduje o terminowości dostaw komponentów krytycznych.** Wzmocnienie odporności łańcucha dostaw wymaga zatem instrumentów adresowanych nie tylko do liderów, lecz przede wszystkim do ich zaplecza kooperacyjnego.

Przeprowadzona analiza pozwala ocenić potencjał finansowy badanych liderów polskiego przemysłu obronnego jako wysoki. Do najważniejszych przewag należą: wysoka i rosnąca rentowność, silna pozycja kapitałowa, bezpieczna struktura finansowania majątku trwałego oraz niemal zerowe zadłużenie finansowe netto, co tworzy znaczną przestrzeń do finansowania rozwoju. **Kluczowe wyzwania koncentrują się natomiast w obszarze zarządzania kapitałem obrotowym oraz struktury terminowej finansowania, a także w ograniczonej absorpcji środków UE i niskim wykorzystaniu długoterminowego finansowania dłużnego.**

Syntetyczne podsumowanie oceny potencjału finansowego PGZ i Grupy WB w porównaniu z benchmarkami europejskimi przedstawia tabela 2.2.

Tab. 2.2. Ocena potencjału finansowego PGZ i Grupy WB względem wskaźników UE

Wskaźnik	Benchmark UE	PGZ	Grupa WB	Interpretacja
Marża EBITDA	8-15%	24,5% (↑ z 20,5%)	33,8% (↑ z 27,6%)	Obie grupy powyżej benchmarku; WB bliżej firm technologicznych
Marża netto	4-8%	15,1%	23,8%	Bardzo wysoka zyskowność wynikająca z premii kontraktowej i efektu skali
Dynamika przychodów (r/r)	8-12%	32,7%	-3,5%	Silny efekt cyklu zbrojeniowego; w WB stabilizacja przychodów po skokowej ekspansji 2024 roku
ROE	8-12%	17,1%	41,5%	WB zbliżona do modelu spółki wzrostowej; PGZ ograniczona kapitałochłonnością
Płynność bieżąca	1,2-2,0	1,50	1,89	PGZ akceptowalny poziom; WB komfortowy bufor

Wskaźnik	Benchmark UE	PGZ	Grupa WB	Interpretacja
Dług finansowy netto / EBITDA	≤ 2,5-3,0	ujemny (-4,4)	ujemny (-1,5)	Brak realnego zadłużenia finansowego; znaczna przestrzeń na dług
Cykl konwersji gotówki (dni)	60-120	447	198	Wysokie zaangażowanie kapitału obrotowego, zwłaszcza w PGZ
Dostęp do finansowania	wysoki	bardzo wysoki	bardzo wysoki	Zróżnicowane modele finansowania rozwoju
Absorpcja środków UE	rosnąca	ograniczona	umiarkowana / rosnąca	WB bardziej aktywna projektowo

Źródło: opracowanie własne na podstawie jednostkowych i skonsolidowanych sprawozdań finansowych badanych podmiotów za lata 2023–2025.

Zestawienie to potwierdza zasadniczy wniosek z analizy: **badane podmioty wchodzą w okres intensywnych inwestycji z pozycji wysokiej rentowności i niemal zerowego zadłużenia finansowego, a ich potencjał finansowy należy ocenić jako wysoki.** Różnice między PGZ a Grupą WB dotyczą nie samej kondycji – w obu przypadkach dobrej – lecz modelu finansowania rozwoju: stabilnego, opartego na zapleczu Skarbu Państwa w PGZ oraz dynamicznego, łączącego finansowanie rynkowe z eksportem w WB. O zdolności do terminowej realizacji dużych zamówień przesądzi jednak nie sam potencjał liderów, lecz ich obudowanie długoterminowym finansowaniem inwestycji oraz elastycznym finansowaniem kapitału obrotowego, obejmującym także pozostałe szczeble łańcucha dostaw.

2.2.5. Potencjał do budowania ekosystemu partnerstw

Rozwój potencjałów wewnętrznych przedsiębiorstwa, tj. potencjału produkcyjnego, technologiczno-innowacyjnego, kapitału ludzkiego i finansowego, stanowi warunek konieczny, lecz niewystarczający dla zapewnienia bezpieczeństwa i odporności łańcuchów dostaw w przemyśle obronnym. Równie istotna jest zdolność do budowania trwałych relacji z kluczowymi interesariuszami tworzącymi ekosystem przemysłowo-obronny w całym cyklu życia systemów uzbrojenia – od identyfikacji potrzeb operacyjnych i definiowania wymagań, poprzez badania i rozwój, projektowanie, produkcję, integrację i dostawę, aż po eksploatację, utrzymanie, modernizację oraz wycofanie z użytkowania.

Współpraca wymaga **zaangażowania szerego grona interesariuszy**, obejmującego

zarówno podmioty publiczne, jak i prywatne, w tym instytucje odpowiedzialne za kształtowanie polityki obronnej państwa i planowanie zdolności operacyjnych, podmioty realizujące procesy pozyskiwania uzbrojenia, przedsiębiorstwa pełniące funkcję integratorów systemów, dostawców komponentów, materiałów i technologii, jednostki naukowo-badawcze oraz uczelnie, instytucje finansujące działalność rozwojową, organizacje certyfikujące i standaryzacyjne, a także partnerów zagranicznych uczestniczących we wspólnych programach przemysłowych i technologicznych. Zdolność do efektywnego zarządzania tymi relacjami umożliwi przedsiębiorstwom pozyskiwanie komplementarnych zasobów i kompetencji, zwiększanie innowacyjności, ograniczanie ryzyka w łańcuchach dostaw oraz wzmacnianie odporności krajowego potencjału przemysłowo-obronnego.

Istotna jest **pogłębiona współpraca z dostawcami** w górze łańcucha jak i **relacje sprzedażowe**, które coraz częściej przyjmują formę długoterminowych relacji opartych na współdzieleniu wiedzy, współtworzeniu innowacji oraz wspólnym rozwoju kompetencji. Wczesne włączanie dostawców w procesy B+R umożliwia lepszą integrację rozwiązań technologicznych, skrócenie cyklu rozwoju produktów oraz zwiększenie efektywności całego łańcucha dostaw. Kluczowe znaczenie dla odporności łańcucha mają również dywersyfikacja bazy dostawców, rozwój kompetencji podmiotów tworzących kolejne szczeble łańcucha dostaw, cyfryzacja procesów współpracy oraz zapewnienie bezpieczeństwa technologicznego i zgodności regulacyjnej. Ważne jest także rozwijanie zdolności do konkurencyjności na rynkach zagranicznych. Warunkiem skutecznej ekspansji eksportowej jest oferowanie rozwiązań

odpowiadających wymaganiom odbiorców, charakteryzujących się wysokim poziomem innowacyjności, niezawodności, interoperacyjności oraz konkurencyjnością kosztową.

Ważny jest **rozwój współpracy wewnątrzbranżowej między podmiotami publicznymi i prywatnymi**, czego przykładem jest porozumienie między PGZ a Grupą WB, ukierunkowane na realizację wspólnych projektów badawczorozwojowych¹²², ale także na rozwój **partnerstw międzybranżowych**, obejmujących współpracę z podmiotami z branż

takich jak finansowa, IT, chemiczna, motoryzacyjna czy metalurgiczna. Partnerstwa te z jednej strony przyczyniają się do stabilizacji łańcuchów dostaw i zapewnienia dostępu do kluczowych komponentów, a z drugiej otwierają nowe możliwości finansowania i skalowania działalności. Przykładem tego typu inicjatywy jest strategiczna współpraca między PGZ a PKO Bankiem Polskim, która wspiera rozwój projektów o znaczeniu dla bezpieczeństwa państwa poprzez zapewnienie odpowiedniego zaplecza finansowego¹²³.

Znaczenia nabiera **współpraca z uczelniami i instytutami badawczymi**. Efektem takiej współpracy jest sztandarowy produkt MESKO, czyli system Piorun, który powstał w wyniku wspólnych prac z CRW Telesystem-Mesko oraz Wojskową Akademią Techniczną¹²⁴, ale także rozwijane przez Sieć Badawczą Łukasiewicz partnerstwa strategiczne m.in. z PGZ, Grupą WB, których celem jest transfer nowoczesnych technologii do polskiego przemysłu obronnego¹²⁵, czy też współpraca m.in. Huty Stalowa Wola z Wojskowym Instytutem Techniki Inżynierskiej w ramach projektu pojazdu minowania narzutowego o kryptonimie BAOBAB-K¹²⁶.

Uzupełnieniem krajowego ekosystemu partnerstw jest **współpraca międzynarodowa**, umożliwiająca przedsiębiorstwom dostęp do zaawansowanych technologii, kompetencji oraz nowych rynków. Udział w międzynarodowych programach badawczo-rozwojowych, konsorcjach przemysłowych i projektach realizowanych z partnerami zagranicznymi sprzyja transferowi wiedzy, rozwojowi zdolności produkcyjnych oraz integracji z europejską i transatlantycką bazą przemysłowo-obronną. Warto zauważyć, że mimo wyraźnego wzrostu aktywności międzynarodowej polskich przedsiębiorstw przemysłu obronnego skala partnerstw o charakterze strategicznym nadal pozostaje ograniczona. Dominują relacje związane z zakupem technologii, produkcją licencyjną, lokalizacją wytwarzania oraz wsparciem eksploatacji, podczas gdy relatywnie rzadziej przedsiębiorstwa polskie uczestniczą jako równorzędni partnerzy we wspólnym projektowaniu, rozwoju i komercjalizacji nowych technologii. Z perspektywy długookresowe-

go rozwoju krajowego potencjału przemysłowo-obronnego pożądane jest zwiększanie udziału polskich przedsiębiorstw w międzynarodowych programach badawczo-rozwojowych, konsorcjach przemysłowych oraz europejskich łańcuchach wartości, przy jednoczesnym zachowaniu kompetencji w obszarach technologii krytycznych.

Rozwojowi partnerstw międzynarodowych sprzyjają instrumenty finansowe Unii Europejskiej, takie jak Europejski Fundusz Obrony (EDF), Europejski Program na rzecz Przemysłu Obronnego (EDIP) oraz mechanizm SAFE, które tworzą zachęty do realizacji wspólnych projektów B+R, inwestycyjnych i produkcyjnych. Instrumenty te zwiększają możliwości uczestnictwa polskich przedsiębiorstw w europejskich konsorcjach przemysłowych, sprzyjając transferowi wiedzy, rozwojowi kompetencji technologicznych oraz integracji z Europejską Bazą Technologiczno-Przemysłową Sektora Obronnego (EDTIB).

¹²² <https://www.wbgroup.pl/wb-electronics/>

¹²³ <https://bank.pl/strategiczne-partnerstwo-dla-bezpieczenstwa-polski-pgz-i-pko-bp/>

¹²⁴ <https://forsal.pl/kraj/bezpieczenstwo/artykuly/10633974,polski-piorun-bije-rekordy-polnoc-nato-stawia-na-nasze-rakiety.html>

¹²⁵ <https://lukasiewicz.gov.pl/pgz-i-lukasiewicz-lacza-sily-na-rzecz-innowacji-w-polskim-przemysle-zbrojeniowym/>; <https://tech.wp.pl/niewidzialna-przewaga-jak-technologie-zmienia-polska-armie,7283620362037312a>

¹²⁶ <https://magazynprzemyslowy.pl/artykuly/polski-przemysl-obronny-w-pigulce>

Polskie przedsiębiorstwa uczestniczą w co drugim projekcie konsorcjalnym zatwierdzonym do realizacji przez EDF w ostatniej edycji naboru. Jest to pozytywny sygnał uwypuklający kompetencje innowacyjne i możliwości nawiązywania partnerstw międzynarodowych, chociaż niewątpliwie negatywnym zjawiskiem jest to, że żaden ze zgłoszonych projektów nie jest koordynowany przez polskie przedsiębiorstwa¹²⁷.

2.3. Analiza surowcowa

Mapując łańcuchy dostaw szczególną uwagę warto zwrócić na bezpieczeństwo surowcowe, zwłaszcza surowców o charakterze krytycznym, które stanowią podstawę produkcji o wysokim stopniu zaawansowania technologicznego, komponentów mikroelektroniki oraz materiałów chemicznych wykorzystywanych w produkcji sprzętu wojskowego. Ich dostępność jest często ograniczona geograficznie, a łańcuchy ich przetwarzania są silnie skoncentrowane poza granicami Polski, co generuje istotne ryzyko zależności od dostawców zewnętrznych oraz podatność na zakłócenia o charakterze geopolitycznym.

Analiza bezpieczeństwa surowcowych łańcuchów dostaw w przypadku polskiego przemysłu obronnego wymaga podejścia systemowego, obejmującego pełen cykl życia surowca – od wydobycia, poprzez rafinację, aż po recykling. Istotne jest przy tym uwzględnienie specyfiki poszczególnych kategorii sprzętu wojskowego, dla których modele zaopatrzenia różnią się poziomem krajowej autonomii – od rozwiązań względnie suwerennych technologicznie po systemy w dużym stopniu oparte na importowanych komponentach i surowcach.

Celem tej części raportu jest identyfikacja kluczowych surowców wykorzystywanych w analizowanych systemach uzbrojenia, mapowanie krajowych i zagranicznych łańcuchów ich dostaw oraz ocena ryzyka związanego z ich dostępnością w warunkach funkcjonowania przemysłu w czasie pokoju. Na podstawie analizy zostaną zaproponowane rekomendacje ukierunkowane na zwiększenie odporności, dywersyfikację źródeł zaopatrzenia oraz rozwój krajowych zdolności w obszarach o najwyższym znaczeniu strategicznym.

2.3.1. Identyfikacja kluczowych surowców wykorzystywanych w analizowanych systemach uzbrojenia

Rysunek 2.9 przedstawia macierz zapotrzebowania na surowce wykorzystywane do produkcji wybranych systemów uzbrojenia stanowiących istotny element potencjału obronnego Rzeczypospolitej Polskiej, tj. bojowego wozu piechoty Borsuk, amunicji artyleryjskiej kalibru 155 mm, armatohaubicy samobieżnej KRAB oraz K9, a także bezzałogowego systemu uderzeniowego Warmate. Dla każdego z analizowanych wyrobów wskazano występowanie poszczególnych surowców w konstrukcji lub zastosowanych rozwiązaniach technologicznych, umożliwiając identyfikację materiałów o największym znaczeniu dla krajowego przemysłu obronnego. Przedstawione zestawienie ma charakter poglądowy i zostało opracowane na podstawie ogólnodostępnych informacji dotyczących budowy analizowanych systemów uzbrojenia oraz stosowanych technologii materiałowych. Rzeczywisty zakres wykorzystania poszczególnych surowców może różnić się w zależności od wersji produktu, konfiguracji wyposażenia, zmian konstrukcyjnych, stosowanych technologii produkcyjnych oraz udziału komponentów i podzespołów pochodzących od krajowych i zagranicznych dostawców. Macierz stanowi narzędzie wspierające ocenę zapotrzebowania na surowce z punktu widzenia utrzymania i rozwoju krajowych zdolności produkcyjnych oraz odporności łańcuchów dostaw.

¹²⁷ Polskie podmioty w niemal co drugim projekcie Europejskiego Funduszu Obronnego, <https://zbiam.pl/polskie-podmioty-w-niemal-co-drugim-projekcie-europejskiego-funduszu-obronnego/>

Rys. 2.9. Macierz zapotrzebowania na surowce wykorzystywane w produkcji wybranych systemów uzbrojenia



Analiza macierzy wskazuje, że znaczna część surowców wykorzystywana jest równocześnie w kilku kluczowych systemach uzbrojenia. Dotyczy to w szczególności aluminium, dysprozu, galu, grafitu, indu, kobaltu, krzemu, miedzi, neodymu, niklu, prazeodymu, srebra, tantalu, tytanu, wanadu, wolframu, złota oraz żelaza. Ograniczona dostępność któregośkolwiek z tych surowców może oddziaływać jednocześnie na wiele programów modernizacji technicznej Sił Zbrojnych RP, zwiększając ryzyko zakłóceń w produkcji, remontach oraz utrzymaniu gotowości operacyjnej. Zestawienie stanowi punkt wyjścia do dalszych analiz dotyczących identyfikacji surowców krytycznych dla krajowego sektora obronnego.

2.3.2. Ocena ryzyk mogących zakłócić ciągłość łańcuchów dostaw

Rozwinięcie analizy zapotrzebowania na surowce wykorzystywane w produkcji wybranych systemów uzbrojenia stanowi zestawienie zawierające ocenę ryzyka dostaw surowców zaprezentowanych na rysunku 2.10. Na podstawie wcześniej opracowanej macierzy zapotrzebowania dokonano identyfikacji surowców wspólnych dla analizowanych wyrobów oraz przeprowadzono ocenę ryzyka ich dostępności.

RANKING	SUROWIEC	KRYTERIA OCENY (skala punktowa)				ILOŻYŃ (wynik łączny)
		Znaczenie strategiczne (1-4)	Dostępność na krajowym rynku (1-4)	Trudności w pozyskaniu (1-3)	Koncentracja surowca (1-3)	
1	Dysproz	4	4	3	3	144
2	Gal	4	4	3	3	144
3	Neodym	4	4	3	3	144
4	Praseodym	4	4	3	3	144
5	Wolfram	4	4	3	3	144
6	Antymon	3	4	3	3	108
7	Chrom	3	4	3	3	108
8	German	3	4	3	3	108
9	Kobalt	4	3	3	3	108
10	Grafit	4	4	2	3	96
11	Ind	4	4	3	2	96
12	Tantal	4	4	2	3	96
13	Aluminiurny (Boksyt)	4	3	2	3	72
14	Bor	2	4	3	3	72
15	Itr	2	4	3	3	72
16	Cyna	3	3	3	2	54
17	Kadm	2	3	3	3	54
18	Wanad	4	2	2	3	48
19	Beryl	1	4	3	3	36
20	Krzem	4	3	1	3	36
21	Rtęć	1	4	3	3	36
22	Molibden	4	3	3	1	36
23	Nikiel	4	2	2	2	32
24	Tytan	4	2	2	2	32
25	Mangan	3	3	3	1	27
26	Żelazo	4	2	3	1	24
27	Cynk	3	2	1	2	12
28	Węgiel kokosowy	3	3	1	1	9
29	Miedź	4	1	1	1	4
30	Srebro	4	1	1	1	4
31	Złoto	4	1	1	1	4

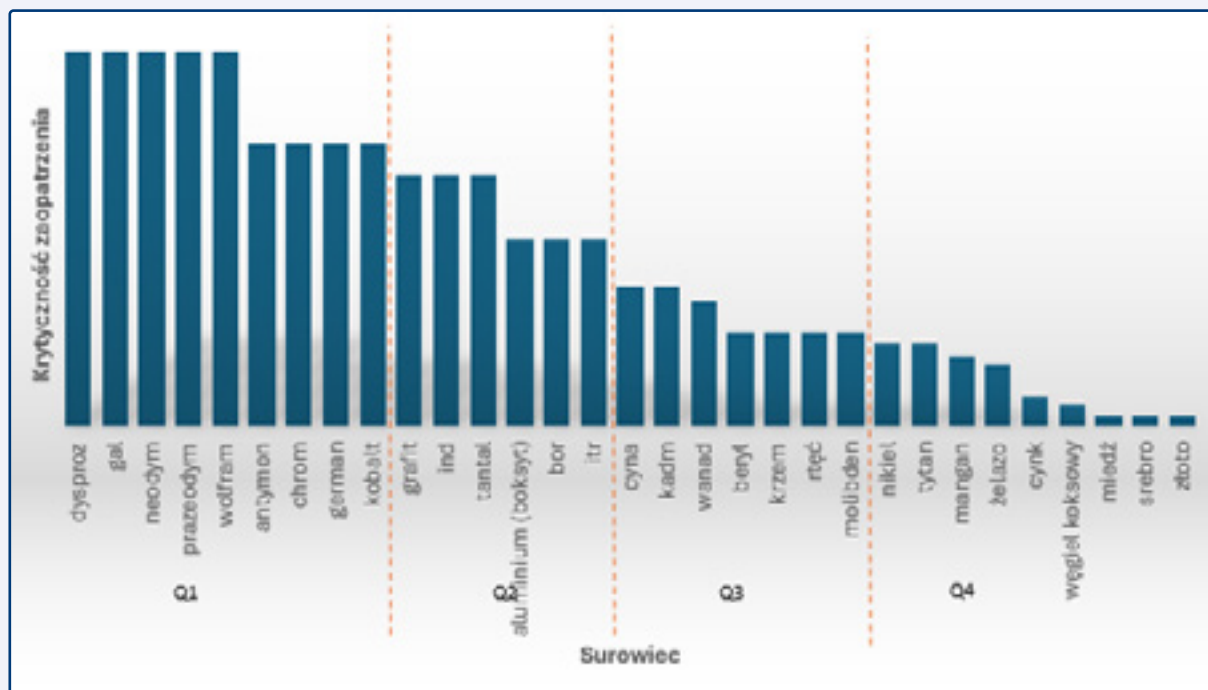
Rys. 2.10. Ocena ryzyka dostaw surowców

W przyjętej metodyce ryzyko dostaw rozumiano jako funkcję dwóch podstawowych składowych: prawdopodobieństwa wystąpienia zakłóceń dostaw oraz wpływu tych zakłóceń na funkcjonowanie krajowego przemysłu obronnego. Wpływ został określony na podstawie znaczenia strategicznego surowca, natomiast prawdopodobieństwo oszacowano z wykorzystaniem trzech kryteriów opisujących podatność łańcucha dostaw na zakłócenia, tj. dostępności surowca na rynku krajowym, trudności jego pozyskania oraz koncentracji światowych źródeł wydobycia. Dla każdego z nich ustalono wagi, które wskazywały na wzrastające ryzyko (od 1 do 3 lub 4). Przyjęto następujące kryteria:

- **znaczenie strategiczne surowca dla krajowego przemysłu obronnego**, określone na podstawie liczby analizowanego asortymentu, w których dany surowiec występuje. Założono, że wraz ze wzrostem liczby zastosowań rośnie jego znaczenie dla funkcjonowania krajowego przemysłu obronnego, a tym samym potencjalne skutki ewentualnych zakłóceń w dostawach;
- **dostępność surowca na rynku krajowym**, ocenianą z uwzględnieniem stopnia rozwoju krajowego łańcucha dostaw. Niższa dostępność krajowych źródeł pozyskania i przetwarzania surowca oznaczała wyższy poziom ryzyka wynikający z większej zależności od importu;
- **trudności związane z pozyskaniem surowca**, analizowane z uwzględnieniem lokalizacji głównych producentów. Kryterium to uwzględniało różnice pomiędzy pozyskiwaniem surowców z państw członkowskich Unii Europejskiej, charakteryzujących się wysoką stabilnością gospodarczą i polityczną, a importem z państw spoza UE, gdzie ryzyko zakłóceń dostaw może być większe ze względu na sytuację geopolityczną, konflikty zbrojne lub niestabilność polityczną;
- **koncentracja światowych źródeł surowca**, określana na podstawie liczby państw prowadzących wydobycie danego surowca. Przyjęto, że im większa koncentracja wydobycia w ograniczonej liczbie państw, tym wyższe ryzyko wystąpienia zakłóceń w globalnych łańcuchach dostaw.

Na tej podstawie dla każdego surowca wyznaczono syntetyczny wskaźnik istotności surowca będący iloczynem ocen poszczególnych kryteriów (rys. 2.11), co umożliwiło

uszeregowanie surowców według potencjalnego wpływu ich ograniczonej dostępności na bezpieczeństwo dostaw dla krajowego sektora obronnego.



Rys. 2.11. Uporządkowany poziom istotności kluczowych surowców

Najwyższe wartości wskaźnika ryzyka uzyskały przede wszystkim surowce ziem rzadkich oraz metale o wysokim znaczeniu technologicznym, tj. dysproz, gal, neodym, prazeodym i wolfram, a także kobalt, german, antymon czy grafity. Surowce te są wykorzystywane równocześnie w kilku analizowanych systemach uzbrojenia, których dostępność jest

silnie uzależniona od światowych łańcuchów dostaw oraz wysokiej koncentracji wydobycia. Ograniczenie dostępu do tych surowców mogłoby jednocześnie powodować zakłócenia w produkcji uzbrojenia obronnego, oddziaływać na realizację wielu programów jego modernizacji oraz utrudniać utrzymanie gotowości operacyjnej.

2.4. Wnioski i rekomendacje

Przeprowadzona analiza mapy łańcuchów dostaw dla wybranego sprzętu wojskowego i środków bojowych pozwala sformułować wnioski w trzech komplementarnych wymiarach. Po pierwsze, analiza przedmiotowa identyfikuje poziom krajowych kompetencji produkcyjnych i technologicznych oraz wskazuje obszary największych zależności od zagranicznych dostawców. Po drugie, analiza podmiotowa pozwala ocenić potencjał przedsiębiorstw przemysłu obronnego oraz zdolność krajowego ekosystemu do zapewnienia ciągłości i odporności dostaw. Po trzecie, analiza surowcowa określa sto-

pień zabezpieczenia dostępu do materiałów krytycznych, stanowiących podstawę funkcjonowania całego łańcucha dostaw. Łącznie wyniki tych analiz wskazują, że bezpieczeństwo łańcuchów dostaw w polskim przemyśle obronnym zależy od równoczesnego wzmacniania kompetencji technologicznych, potencjału przedsiębiorstw oraz bezpieczeństwa surowcowego, przy jednoczesnym wykorzystaniu współpracy międzynarodowej jako elementu budowania odporności systemu.

Wnioski z analizy przedmiotowej

Analiza objętych badaniem systemów uzbrojenia wskazuje, że krajowy przemysł obronny dysponuje zróżnicowanym poziomem kompetencji produkcyjnych i technologicznych. Relatywnie największy potencjał występuje w obszarze amunicji, materiałów wysokoenergetycznych oraz wybranych komponentów artyleryjskich, natomiast największe zależności od dostaw zagranicznych dotyczą zaawansowanej elektroniki, mikroelektroniki, systemów obliczeniowych oraz części systemów dowodzenia i łączności.

Przeprowadzona analiza potwierdza, że o bezpieczeństwie dostaw decyduje nie tylko zdolność do wytwarzania platform uzbrojenia, lecz także dostęp do dokumentacji technicznej, kompetencji projektowych, praw serwisowych, aktualizacji oprogramowania oraz kodu źródłowego. Ograniczona kontrola nad tymi zasobami może prowadzić do trwałego uzależnienia od dostawców zagranicznych nawet w przypadku krajowej produkcji części wyposażenia.

Istotnym kierunkiem wzmacniania odporności pozostaje stopniowe zwiększanie udziału krajowego przemysłu w realizacji programów modernizacji technicznej Sił Zbrojnych RP poprzez rozwój własnych kompetencji technologicznych, polonizację wybranych komponentów oraz skuteczny transfer technologii. Szczególne znaczenie mają technologie krytyczne związane z materiałami wysokoenergetycznymi, komponentami amunicji, elektroniką, mikroelektroniką oraz systemami autonomicznymi i bezzałogowymi.

Analiza wskazuje również, że odporność łańcuchów dostaw wymaga jednoczesnego rozwijania krajowego zaplecza podwykonawczego, dywersyfikacji źródeł zaopatrzenia oraz zdolności do szybkiego zwiększania skali produkcji i utrzymania gotowości serwisowej w warunkach kryzysu lub wojny.

Wnioski z analizy podmiotowej

Analiza podmiotowa wskazuje, że bezpieczeństwo łańcuchów dostaw jest determinowane nie tylko przez strukturę sieci dostaw, lecz także przez potencjał przedsiębiorstw

tworzących poszczególne ogniwa. O odporności krajowego przemysłu obronnego decyduje zdolność przedsiębiorstw do równoczesnego rozwijania potencjału produkcyjnego, technologiczno-innowacyjnego, kompetencyjnego, finansowego oraz partnerskiego.

Największym wyzwaniem pozostaje zwiększenie zdolności produkcyjnych umożliwiających zaspokojenie rosnących potrzeb modernizacyjnych państwa oraz szybkie skalowanie produkcji w sytuacjach kryzysowych. Wymaga to eliminowania wąskich gardeł w produkcji, rozwoju krajowej bazy dostawców i poddostawców oraz tworzenia rezerw zdolności wytwórczych.

Jednocześnie trwała odporność przemysłu obronnego zależy od systematycznego rozwoju potencjału technologiczno-innowacyjnego opartego na działalności badawczo-rozwojowej, technologiach podwójnego zastosowania oraz zdolności do szybkiego wdrażania nowych rozwiązań. Szczęólnego znaczenia nabierają kompetencje w obszarze sztucznej inteligencji, systemów autonomicznych, cyberbezpieczeństwa, półprzewodników i materiałów wysokoenergetycznych.

Analiza potwierdza również, że przewaga konkurencyjna przedsiębiorstw jest coraz silniej uzależniona od jakości kapitału ludzkiego, dostępu do stabilnych źródeł finansowania oraz zdolności do funkcjonowania w rozbudowanych ekosystemach współpracy. Integracja potencjału przedsiębiorstw, jednostek naukowych, administracji publicznej i partnerów zagranicznych sprzyja transferowi wiedzy, przyspiesza procesy innowacyjne oraz zwiększa odporność krajowych łańcuchów dostaw.

Wnioski z analizy surowcowej

Analiza surowcowa wskazuje, że bezpieczeństwo polskiego przemysłu obronnego jest w znacznym stopniu uzależnione od dostępu do surowców krytycznych wykorzystywanych w produkcji nowoczesnych systemów uzbrojenia. W warunkach narastających napięć geopolitycznych bezpieczeństwo surowcowe staje się jednym z podstawowych determinantów odporności krajowych łańcuchów dostaw.

Przeprowadzone badania potwierdzają potrzebę prowadzenia spójnej polityki surowcowej uwzględniającej specyficzne potrzeby sektora obronnego, obejmującej identyfikację surowców krytycznych, rozwój krajowych kompetencji wydobywczych i przetwórczych oraz systematyczne monitorowanie ryzyka dostaw.

Jednocześnie analiza wskazuje, że budowanie bezpieczeństwa surowcowego nie powinno być utożsamiane z pełną samowystarczalnością. W przypadku wielu surowców krytycznych większą odporność zapewnia dywersyfikacja źródeł zaopatrzenia, rozwój współpracy z wiarygodnymi partnerami międzynarodowymi oraz wzmacnianie wspólnej polityki surowcowej Unii Europejskiej.

Istotnym elementem zwiększania odporności pozostaje również wykorzystanie krajowych przewag konkurencyjnych, w szczególności potencjału KGHM, rozwoju technologii odzysku metali krytycznych oraz gospodarki o obiegu zamkniętym. Połączenie tych działań z dywersyfikacją międzynarodowych łańcuchów dostaw stwarza podstawy do budowy bardziej odpornego systemu zaopatrzenia surowcowego dla polskiego przemysłu obronnego.

3. IDENTYFIKACJA I OCENA RYZYKA W ŁAŃCUCHACH DOSTAW W POLSKIM PRZEMYŚLE OBRONNYM

Celem niniejszego rozdziału jest identyfikacja i ocena ryzyka w łańcuchach dostaw wybranych kategorii sprzętu wojskowego: amunicji 155 mm, bojowego wozu piechoty BWP BORSUK, systemu WARMATE oraz armatohaubic AHS KRAB i AHS K9. Analiza służy określeniu, które obszary ryzyka mają największe znaczenie dla ciągłości dostaw, odporności przemysłowej oraz zdolności polskiego przemysłu obronnego do utrzymania, rozwijania i modernizacji kluczowych systemów uzbrojenia. Jej wyniki mają wspierać formułowanie działań wzmacniających bezpieczeństwo państwa, w tym rozwój krajowych zdolności produkcyjnych, dywersyfikację źródeł dostaw oraz ograniczanie zależności od podmiotów zewnętrznych.

Podstawą analizy są literatura przedmiotu, raporty branżowe oraz materiał empiryczny zgromadzony podczas warsztatów z przedstawicielami kluczowych podmiotów krajowego przemysłu obronnego, w tym Polskiej Grupy Zbrojeniowej (PGZ) oraz Grupy WB. W trakcie warsztatów zidentyfikowano główne obszary ryzyka, określono przykładowe zdarzenia prowadzące do ich materializacji oraz oceniono ich prawdopodobieństwo i potencjalny wpływ. Wykorzystano podejście zgodne z logiką zarządzania ryzykiem stosowaną w metodykach NATO i ISO, w którym ryzyko rozumiane jest jako niepewne zdarzenie lub warunek mogący oddziaływać na realizację celów projektu lub organizacji.

Struktura rozdziału odpowiada kolejnym etapom procedury zarządzania ryzykiem. W pierwszej kolejności przedstawiono modele łańcuchów dostaw oraz ich wpływ na profil ryzyka w przemyśle obronnym. Następnie omówiono metodykę identyfikacji i oceny ryzyka, wskazano kluczowe obszary ryzyka wewnętrznego i zewnętrznego oraz przykłady ich materializacji. W dalszej części zaprezentowano ocenę prawdopodobieństwa i wpływu ryzyka na poziomie całej branży, a następnie ocenę znaczenia poszczególnych rodzajów ryzyka dla analizowanych kategorii sprzętu wojskowego. Rozdział zamykają zagadnienia dotyczące zarządzania ryzykiem oraz rekomendacje służące wzmacnianiu odporności łańcuchów dostaw polskiego przemysłu obronnego.

3.1. Modele łańcuchów dostaw a profil ryzyka w polskim przemyśle obronnym

Ocena ryzyka w łańcuchach dostaw przemysłu obronnego wymaga uwzględnienia nie tylko charakteru zagrożeń, lecz także struktury tych łańcuchów. W przypadku uzbrojenia dostarczanego Siłom Zbrojnym RP można wyróżnić trzy podstawowe modele organizacji łańcuchów dostaw, różniące się poziomem kontroli nad technologią, stopniem zależności od zagranicznych dostawców oraz zakresem autonomii strategicznej państwa.

Pierwszy model stanowi **łańcuch dostaw oparty na suwerenności technologicznej**. Jego podstawą jest krajowa kontrola nad własnością intelektualną, *know-how* oraz architekturą systemu uzbrojenia. W tym modelu krajowe przedsiębiorstwo, lider łańcucha dostaw, zachowuje zdolność samodzielnego rozwoju, modernizacji oraz utrzymania produktu przez cały cykl jego życia, a także dąży do pełnej kontroli nad własnością intelektualną w ramach łańcucha dostaw. Zapewnia to najwyższy poziom autonomii strategicznej oraz bezpieczeństwa dostaw, ale jednocześnie wymaga utrzymywania szerokiego zakresu kompetencji badawczo-rozwojowych, produkcyjnych i serwisowych. Kluczowym zasobem staje się własność intelektualna, która pozwala kontrolować rozwój produktu i ograniczać zależność od podmiotów zewnętrznych.

Drugim modelem jest **łańcuch dostaw oparty na zależności licencyjnej**, w którym krajowe przedsiębiorstwa produkują lub integrują

systemy uzbrojenia wykorzystujące technologie pozyskane od partnera zagranicznego. Model ten umożliwia relatywnie szybkie budowanie zdolności przemysłowych i skrócenie czasu wdrożenia nowych systemów, jednak pozostawia istotne obszary zależne od właściciela technologii. Dotyczy to zwłaszcza dostępu do dokumentacji technicznej, praw do modyfikacji systemu, aktualizacji technologicznych oraz części zamiennych. W rezultacie autonomia przemysłowa i operacyjna pozostaje ograniczona.

Trzeci model stanowi **łańcuch dostaw oparty na imporcie z lokalizacją wsparcia**, polegający na zakupie gotowych systemów uzbrojenia za granicą przy jednoczesnym rozwijaniu w kraju zdolności logistycznych, remontowych i serwisowych. Rozwiązanie takie umożliwia szybkie pozyskanie zdolności wojskowych, jednak nie zapewnia pełnej kontroli nad technologią ani nad kluczowymi elementami łańcucha dostaw. W sytuacji kryzysowej lub konfliktu zbrojnego utrzymanie zdolności eksploatacyjnych pozostaje uzależnione od dostaw części zamiennych, wsparcia technicznego oraz decyzji politycznych państwa dostawcy.

Poszczególne modele różnią się nie tylko stopniem autonomii technologicznej, lecz również profilem ryzyka (Tabela 3.1). Oznacza to, że identyczne zdarzenie może wywoływać odmienne skutki w zależności od przyjętej architektury łańcucha dostaw.

Tab. 3.1. Dominujące ryzyka w zależności od modelu łańcucha dostaw

Model łańcucha dostaw	Dominujące źródła ryzyka
Suwerenność technologiczna	niedobór wykwalifikowanych kadr, finansowanie B+R, cyberbezpieczeństwo, ochrona własności intelektualnej, skalowanie produkcji
Zależność licencyjna	ograniczenia transferu technologii, warunki licencyjne, dostęp do dokumentacji, zależność od dostawców komponentów zagranicznych
Import z lokalizacją wsparcia	zakłócenia geopolityczne, embargo, dostępność części zamiennych, ograniczenia serwisowe, zależność od państwa dostawcy

W praktyce większość współczesnych programów zbrojeniowych realizowanych w Polsce nie odpowiada w pełni jednemu modelowi,

lecz stanowi kombinację różnych rozwiązań. Oznacza to, że poszczególne systemy uzbrojenia charakteryzują się zróżnicowaną struk-

turą ryzyka wynikającą z odmiennego stopnia krajowej kontroli nad technologią i produkcją.

Przykładowo, system amunicji krążącej WARMATE jest bliski modelowi suwerenności technologicznej, ponieważ zdecydowana większość jego komponentów powstaje w kraju, a producent ma kontrolę nad kluczowymi technologiami. BWP BORSUK reprezentuje model mieszany, oparty głównie na krajowych kompetencjach, ale wykorzystujący również wybrane komponenty zagraniczne. Armatohaubica KRAB stanowi przykład modelu hybrydowego, łączącego krajową integrację z elementami technologii pozyskanymi za granicą. Z kolei armatohaubica K9 jest przykładem modelu importowego z rozwijanym lokalnym wsparciem eksploatacyjnym. Amunicja artyleryjska kali-

bru 155 mm znajduje się pomiędzy modelem suwerenności produkcyjnej a zależnością od dostaw wybranych komponentów, materiałów i technologii.

Przedstawione modele stanowią punkt wyjścia do dalszej analizy ryzyka. Pozwalają bowiem nie tylko identyfikować potencjalne zagrożenia, lecz także wyjaśniać, dlaczego określone kategorie ryzyka mają większe znaczenie dla niektórych systemów uzbrojenia niż dla innych. W konsekwencji architektura łańcucha dostaw staje się jednym z podstawowych czynników determinujących odporność krajowego przemysłu obronnego oraz zdolność państwa do utrzymania ciągłości dostaw w warunkach kryzysu i konfliktu zbrojnego.

3.2. Metodyka identyfikacji i oceny ryzyka

Przedstawione modele łańcuchów dostaw różnią się poziomem autonomii technologicznej oraz strukturą zależności od dostawców krajowych i zagranicznych. Oznacza to, że generują one odmienne profile ryzyka, które wymagają systematycznej identyfikacji i oceny. Analiza funkcjonowania łańcuchów dostaw w polskim przemyśle obronnym wskazuje na konieczność przyjęcia proaktywnego podejścia do zarządzania ryzykiem oraz równoległego wzmacniania odporności tych łańcuchów (*resilience*). W warunkach rosnącej niepewności geopolitycznej, nasilającej się konkurencji o zasoby oraz presji na szybkie zwiększanie zdolności produkcyjnych, zdolność do przewidywania zakłóceń i przygotowania adekwatnych reakcji staje się czynnikiem krytycznym o porównywalnym znaczeniu ze zdolnością wytwórczą samą w sobie¹²⁸. Z tego względu zarządzanie ryzykiem nie może być ograniczane do działań reaktywnych, uruchamianych dopiero w sy-

tuacji kryzysowej, lecz jest integralnym elementem zarządzania łańcuchami dostaw warunkującym ich ciągłość, elastyczność oraz zdolność do adaptacji. Metodyczne podejście do zarządzania ryzykiem nabiera szczególnego znaczenia w kontekście europejskim, gdzie obserwujemy intensyfikację działań na rzecz wzmocnienia bazy przemysłowo-obronnej¹²⁹. Budowa odpornych łańcuchów dostaw w Polsce wpisuje się w szersze wysiłki na rzecz zwiększania autonomii strategicznej oraz bezpieczeństwa całego regionu.

Zgodnie ze standardami NATO ryzyko definiowane jest jako niepewne zdarzenie lub warunek, który może wywołać skutki pozytywne lub negatywne dla realizacji celów projektu¹³⁰. Ujęcie to jest spójne z podejściem ISO 31000, w którym ryzyko rozumiane jest jako wpływ niepewności na cele organizacji, a zarządzanie nim ma charakter systematyczny, zintegrowany i ciągły¹³¹. W praktyce

128 Loska, D., Hazen, B., Rich, N., Genchev, S., Malik, T. (2025). Military Supply Chain Logistics and Dynamic Capabilities: A Literature Review and Synthesis. *Transportation Journal*, 64(2), e70002. <https://doi.org/10.1002/tjo3.70002>

129 European Commission. (2025). Speech by President von der Leyen on European defence at the Royal Danish Military Academy, https://ec.europa.eu/commission/presscorner/detail/en/speech_25_814

130 NATO. (2012). Risk management guide for acquisition programmes (ARAMP-1). NATO Standardization Office. <https://standards.globalspec.com/std/1497473/aramp-1>

131 ISO. (2018). Risk management - Guidelines (Norma ISO 31000:2018). <https://www.iso.org/standard/65694.html>

oznacza to, że proces zarządzania ryzykiem obejmuje identyfikację, analizę (w tym ocenę prawdopodobieństwa i wpływu), planowanie reakcji oraz monitorowanie ryzyka na każdym etapie cyklu życia systemów uzbrojenia. Jest to proces iteracyjny wspierający podejmowanie decyzji na wszystkich poziomach – od przedsiębiorstwa, przez łańcuch, aż po kraj lub region.

Specyfika łańcuchów dostaw w przemyśle obronnym wymaga analizy ryzyka w dwóch uzupełniających się wymiarach: (i) wewnętrznym, dotyczącym funkcjonowania przedsiębiorstw i relacji pomiędzy uczestnikami łańcucha dostaw oraz (ii) zewnętrznym, wynikającym z otoczenia tych łańcuchów. W obrębie samego łańcucha dostaw

identyfikowane są ryzyka o charakterze strategicznym, operacyjnym i finansowym po stronie przedsiębiorstw, a także ryzyka strukturalne, procesowe i relacyjne, związane m.in. z koncentracją dostawców, złożonością produktów oraz współpracą między podmiotami. Z kolei w otoczeniu łańcuchów dostaw występują ryzyka geopolityczne, ekonomiczne, regulacyjne, technologiczne czy infrastrukturalne, które mogą wpływać na dostępność zasobów, ciągłość produkcji oraz możliwości rozwoju zdolności przemysłowych¹³². W takim ujęciu odporność łańcuchów dostaw jest determinowana zarówno przez czynniki wewnętrzne, jak i przez zdolność adaptacji do dynamicznie zmieniających się warunków zewnętrznych.

3.3. Kluczowe obszary ryzyka

Przeprowadzone warsztaty z przedstawicielami krajowych przedsiębiorstw branży zbrojeniowej potwierdziły, że bezpieczeństwo łańcuchów dostaw w polskim przemyśle obronnym wymaga ciągłego mapowania i aktualizowania obszarów ryzyka. Analiza wypowiedzi uczestników pozwoliła wyróżnić dwanaście kluczowych obszarów ryzyka, które wpływają na ciągłość dostaw, odporność przemysłową oraz zdolność przedsiębiorstw do rozwijania i utrzymania zdolności produkcyjnych. Część z nich ma charakter wewnętrzny i wynika z funkcjonowania przedsiębiorstw oraz relacji między podmiotami tworzącymi łańcuch dostaw. Pozostałe są związane z otoczeniem instytucjonalnym, gospodarczym, technologicznym, regulacyjnym i bezpieczeństwa.

W tabeli 3.2 przedstawiono syntetyczną charakterystykę zidentyfikowanych obszarów ryzyka. Podział na ryzyka wewnętrzne i zewnętrzne ma charakter porządkujący. W praktyce poszczególne obszary ryzyka są ze sobą powiązane. Przykładowo, stabilność finansowa dostawców zależy zarówno od ich kon-

dycji ekonomicznej, jak i od przewidywalności zamówień publicznych, natomiast ryzyka związane z własnością intelektualną, cyberbezpieczeństwem oraz szpiegostwem przemysłowym wzajemnie się wzmacniają. Oznacza to, że skuteczne zarządzanie ryzykiem wymaga jednoczesnego wzmacniania zdolności organizacyjnych przedsiębiorstw oraz tworzenia stabilnego otoczenia instytucjonalnego dla krajowego przemysłu obronnego.

Przedstawiona klasyfikacja wskazuje, że bezpieczeństwo łańcuchów dostaw w polskim przemyśle obronnym nie zależy wyłącznie od dostępności komponentów i surowców. Jest ono determinowane również przez zdolność do utrzymania kompetencji, ochrony własności intelektualnej, zapewnienia finansowania, prowadzenia długofalowej polityki kontraktowania, przeciwdziałania cyberzagrożeniom oraz budowania efektywnych relacji między przemysłem a administracją publiczną. W tym sensie odporność łańcuchów dostaw ma charakter systemowy i wymaga działań zarówno po stronie przedsiębiorstw, jak i po stronie państwa.

¹³² Ocicka, B., Cichosz, M., & Radło, M.J. (2026). Klasyfikacja ryzyka w zarządzaniu łańcuchami dostaw w polskim przemyśle obronnym. [W:] Zamelek, P., Krupnik, D. (red.). Transformacja wojskowych łańcuchów dostaw – teoria i praktyka. Część 5. Wydawnictwo Wojskowej Akademii Technicznej w Warszawie.

Tab. 3.2. Kluczowe obszary ryzyka wewnętrznego i zewnętrznego w łańcuchach dostaw sprzętu wojskowego

Kod	Typ ryzyka	Charakterystyka
Ryzyka wewnętrzne		
R1	Stabilność finansowa	Ryzyko utraty zdolności produkcyjnych lub rozwojowych dostawców przemysłu obronnego wynikające z problemów finansowych, ograniczonego dostępu do kapitału oraz nieregularności zamówień obronnych.
R2	Wykwalifikowane kadry	Ryzyko niedoboru specjalistów posiadających unikalne kompetencje w obszarze technologii obronnych oraz utraty wiedzy krytycznej w realizacji programów zbrojeniowych.
R3	Własność intelektualna i transfer technologii	Ryzyko utraty, przejęcia lub ograniczonego dostępu do technologii, dokumentacji technicznej i praw własności intelektualnej mających znaczenie dla bezpieczeństwa i suwerenności technologicznej państwa.
R4	Polityka kontraktowania	Ryzyko wynikające z nieprzewidywalności programów modernizacji sił zbrojnych, zmian priorytetów zakupowych oraz braku długoterminowych gwarancji zamówień.
Ryzyka zewnętrzne		
R5	Ograniczona liczba dostawców	Ryzyko zakłóceń dostaw wynikające z ograniczonej liczby certyfikowanych dostawców komponentów, materiałów i technologii o znaczeniu obronnym.
R6	Proces certyfikacji	Ryzyko opóźnień w rozwoju i wdrażaniu uzbrojenia wynikające ze złożonych procedur certyfikacyjnych, kwalifikacyjnych i dopuszczeniowych.
R7	Nierówne warunki konkurencji	Ryzyko osłabienia pozycji krajowych przedsiębiorstw obronnych wskutek asymetrii dostępu do informacji, wsparcia politycznego lub preferencji dla zagranicznych dostawców.
R8	Szpiegostwo i sabotaż	Ryzyko pozyskania informacji niejawnych, dokumentacji technicznej lub zakłócenia działalności przedsiębiorstw i łańcuchów dostaw przez podmioty wrogie.
R9	Cyberbezpieczeństwo	Ryzyko cyberataków prowadzących do utraty danych, kompromitacji systemów uzbrojenia lub zakłócenia procesów produkcyjnych i logistycznych.
R10	Relacje z administracją publiczną	Ryzyko wynikające z niewystarczającej komunikacji i koordynacji między przemysłem, administracją publiczną a siłami zbrojnymi w zakresie rozwoju zdolności obronnych.
R11	Sytuacja ekonomiczna	Ryzyko ograniczenia zdolności rozwojowych przemysłu obronnego wskutek zmian sytuacji gospodarczej, kosztów finansowania oraz poziomu wydatków obronnych państwa.
R12	Sytuacja społeczno-ekologiczna	Ryzyko wynikające ze zmian regulacji środowiskowych, dostępności surowców krytycznych oraz uwarunkowań społecznych, które wpływają na funkcjonowanie i konkurencyjność przemysłu obronnego.

Źródło: opracowanie własne na podstawie warsztatów i wywiadów z przedstawicielami przemysłu.

Zidentyfikowane obszary ryzyka stanowią punkt wyjścia do dalszej analizy bezpieczeństwa łańcuchów dostaw w polskim przemyśle obronnym. Sama identyfikacja obszarów ryzyka nie pozwala jednak ocenić ich znaczenia dla funkcjonowania przedsiębiorstw i realizacji programów zbrojeniowych. Dlatego kolejnym etapem analizy jest określenie typowych zdarzeń mogących materializować

poszczególne obszary ryzyka oraz wskazanie ich potencjalnych konsekwencji dla funkcjonowania łańcuchów dostaw. Takie podejście pozwala przejść od ogólnej identyfikacji zagrożeń do bardziej operacyjnej oceny ich wpływu na zdolności produkcyjne, technologiczne i logistyczne krajowego przemysłu obronnego.

Tab. 3.3. Przykłady materializacji ryzyka w różnych obszarach oraz ich potencjalne skutki w łańcuchach dostaw polskiego przemysłu obronnego

Kod	Typ ryzyka	Przykład materializacji ryzyka w polskim przemyśle obronnym	Potencjalny skutek
Ryzyka wewnętrzne			
R1	Stabilność finansowa	Utrata płynności przez dostawcę komponentów elektronicznych Brak finansowania inwestycji zwiększających moce produkcyjne Opóźnienia w płatnościach między uczestnikami łańcucha dostaw.	Opóźnienia dostaw, wzrost kosztów pozyskania komponentów, utrata zdolności produkcyjnych i kompetencji dostawców.
R2	Wykwalifikowane kadry	Odejście ekspertów od systemów bezzałogowych lub radiokomunikacyjnych Niedobór inżynierów materiałów wysokoenergetycznych Trudności w pozyskaniu specjalistów w obszarze cyberbezpieczeństwa i AI.	Utrata know-how, spowolnienie prac B+R, ograniczenie zdolności rozwoju nowych technologii.
R3	Własność intelektualna i transfer technologii	Kradzież dokumentacji technicznej systemu uzbrojenia Ograniczenia licencyjne uniemożliwiające modyfikację produktu Brak zgody na eksport lub modernizację rozwiązania rozwijanego ze środków publicznych.	Utrata kontroli nad rozwojem produktu, wzrost zależności technologicznej, ograniczenie innowacyjności.
R4	Polityka kontraktowania	Opóźnienie decyzji zakupowych MON Zmiana priorytetów programów modernizacyjnych Krótkookresowe kontrakty bez gwarancji kontynuacji produkcji.	Ograniczenie inwestycji, niewykorzystanie mocy produkcyjnych, wzrost niepewności wśród dostawców.
Ryzyka zewnętrzne			
R5	Ograniczona liczba dostawców	Wstrzymanie eksportu krytycznych komponentów przez dostawcę zagranicznego Niedobór półprzewodników lub metali ziem rzadkich Upadłość jedyne kwalifikowanego dostawcy podzespołu.	Przerwanie produkcji, konieczność przeprojektowania produktu, wzrost kosztów i wydłużenie czasu realizacji zamówień.
R6	Proces certyfikacji	Przedłużający się proces certyfikacji nowego systemu uzbrojenia Konieczność ponownej certyfikacji po zmianie komponentu Ograniczony potencjał instytucji wojskowych prowadzących badania i certyfikację.	Opóźnienie wdrożenia sprzętu, utrata przewagi technologicznej, ryzyko utraty kontraktu.
R7	Nierówne warunki konkurencji	Brak transparentnych testów porównawczych sprzętu Asymetryczny dostęp do informacji o postępowaniach zakupowych Naciski polityczne wspierające zagranicznych producentów.	Oslabienie krajowych producentów, wybór mniej efektywnych rozwiązań, zwiększenie zależności od dostaw z zagranicy.
R8	Szpiegostwo i sabotaż	Kradzież dokumentacji technicznej lub danych projektowych Infiltracja personelu przez podmioty obce Celowe uszkodzenie infrastruktury produkcyjnej lub magazynowej.	Utrata przewagi technologicznej, zakłócenie produkcji, zagrożenie bezpieczeństwa państwa.
R9	Cyberbezpieczeństwo	Atak ransomware na zakład produkcyjny Włamanie do systemów projektowych i produkcyjnych Kradzież danych technologicznych lub danych dostawców.	Zatrzymanie procesów operacyjnych, utrata danych, przejęcie własności intelektualnej.
R10	Relacje z administracją publiczną i wojskiem	Niejasne określenie przyszłych potrzeb Sił Zbrojnych RP Opóźnienia w procedurach administracyjnych Ograniczony dialog pomiędzy przemysłem, MON i użytkownikiem wojskowym.	Niepewność inwestycyjna, niedopasowanie projektów B+R do potrzeb wojska oraz opóźnienia w rozwoju zdolności produkcyjnych.

Kod	Typ ryzyka	Przykład materializacji ryzyka w polskim przemyśle obronnym	Potencjalny skutek
R11	Sytuacja ekonomiczna	Wzrost stóp procentowych zwiększający koszt finansowania Wysoka inflacja cen energii i materiałów Ograniczenie finansowania programów obronnych lub B+R.	Wzrost kosztów produkcji, ograniczenie inwestycji, spadek rentowności realizowanych programów.
R12	Sytuacja społeczno-ekologiczna	Zaostrzenie regulacji środowiskowych UE Ograniczenie dostępu do metali ziem rzadkich i innych surowców krytycznych Protesty społeczne utrudniające rozwój infrastruktury przemysłowej.	Wzrost kosztów zgodności regulacyjnej, opóźnienia inwestycji, spadek konkurencyjności wobec producentów spoza UE.

Źródło: opracowanie własne na podstawie warsztatów i wywiadów z przedstawicielami przemysłu.

Analiza przedstawiona w tabeli 3.3 pokazuje, że ryzyko w różnych obszarach może materializować się poprzez różnorodne zdarzenia, których skutki wykraczają poza pojedyncze przedsiębiorstwa i mogą oddziaływać na funkcjonowanie całych łańcuchów dostaw. Szczególnie istotne są ryzyka związane z dostępnością wykwalifikowanych kadr, ochroną własności intelektualnej, cyberbezpieczeństwem oraz ograniczoną liczbą dostawców komponentów krytycznych, ponieważ ich wystąpienie może prowadzić nie tylko do zakłóceń produkcyjnych, lecz także do trwałej utraty zdolności technologicznych i przemysłowych.

Jednocześnie część rodzajów ryzyka ma charakter systemowy i pozostaje poza bezpośrednią kontrolą przedsiębiorstw. Dotyczy to zwłaszcza polityki kontraktowania, procesu certyfikacji, sytuacji makroekonomicznej

oraz relacji z administracją publiczną. Wskazuje to, że budowanie odporności łańcuchów dostaw wymaga działań zarówno na poziomie przedsiębiorstw, jak i instytucji państwowych odpowiedzialnych za politykę przemysłową, obronną i gospodarczą.

Przedstawione w tabeli 3.4 zdarzenia i skutki ryzyka stanowią podstawę kolejnego etapu analizy, polegającego na ocenie prawdopodobieństwa wystąpienia poszczególnych rodzajów ryzyka oraz skali ich oddziaływania na funkcjonowanie polskiego przemysłu obronnego. Dzięki temu możliwe jest określenie, które obszary wymagają najpilniejszych działań zaradczych oraz powinny być traktowane jako priorytetowe z punktu widzenia bezpieczeństwa dostaw i odporności krajowej bazy przemysłowo-obronnej.

3.4. Ocena prawdopodobieństwa i wpływu ryzyka na poziomie branży

Po identyfikacji kluczowych obszarów ryzyka oraz wskazaniu przykładowych zdarzeń i skutków ich materializacji, kolejnym etapem analizy była ocena znaczenia poszczególnych rodzajów ryzyka na poziomie całej branży. Ocena ta została przeprowadzona z perspektywy prawdopodobieństwa wystąpienia danego ryzyka oraz skali jego potencjalnego wpływu na funkcjonowanie łańcuchów dostaw w polskim przemyśle obronnym.

W tabeli 3.4 przedstawiono macierz ryzyka dla polskiego przemysłu obronnego, opracowaną na podstawie wyników warsztatów oraz przy założeniu metodyki zgodnej z podej-

ściem NATO/ISO. Poszczególne ryzyka zostały przyporządkowane do czterech kategorii:

- **krytyczne**, wymagające natychmiastowego działania: R2, R4, R9, R6, R3, R8;
- **wysokie**, wymagające planu redukcji i stałego monitoringu: R1, R5, R10, R7, R11, R12;
- **średnie**, wymagające monitorowania oraz ewentualnych działań ograniczających: w obecnej macierzy nie przypisano ryzyka do tej kategorii;
- **niskie**, dla których działania są podejmowane w zależności od kosztów i potrzeb operacyjnych¹³³.

¹³³ W macierzy opracowanej w wyniku warsztatów z przedstawicielami przemysłu obronnego nie przypisano ryzyka do tej kategorii.

Tab. 3.4 Macierz ryzyka dla polskiego przemysłu obronnego

Skutek Prawdopodobieństwo	Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
Prawie pewne			R9		
Prawdopodobne				R6	R2, R4
Możliwe			R7, R11, R12	R1, R5, R10	R3, R8
Mało prawdopodobne					
Rzadkie					

Źródło: opracowanie własne w oparciu o warsztaty z przedstawicielami przemysłu obronnego.

Wyniki wskazują, że zdecydowana większość zidentyfikowanych rodzajów koncentruje się w strefach krytycznego i wysokiego ryzyka. Szczególnie istotne znaczenie mają ryzyka związane z dostępnością wykwalifikowanych kadr, cyberbezpieczeństwem, ochroną własności intelektualnej, szpiegostwem i sabotażem, procesem certyfikacji oraz przewidywalnością kontraktowania. Są to obszary, które bezpośrednio wpływają na zdolność przedsiębiorstw do utrzymania ciągłości produkcji, rozwoju technologii oraz skalowania zdolności przemysłowych.

Wysoki poziom ryzyka procesu certyfikacyjnego wskazuje, że procedury dopuszczania nowych lub zmodyfikowanych produktów mogą stać się istotnym ograniczeniem elastyczności krajowego przemysłu obronnego. W warunkach szybkiego postępu technologicznego oraz konieczności reagowania

na zmieniające się wymagania pola walki nadmiernie długi proces certyfikacji może prowadzić do opóźnień wdrożeniowych, dezaktualizacji rozwiązań oraz utraty przewagi konkurencyjnej.

Struktura ryzyka przedstawiona w tabeli 3.4 potwierdza również, że odporność łańcuchów dostaw nie zależy wyłącznie od zabezpieczenia przepływu materiałów. Kluczowe znaczenie mają także czynniki technologiczne, organizacyjne, kadrowe, instytucjonalne oraz kwestie bezpieczeństwa. Oznacza to, że działania wzmacniające odporność polskiego przemysłu obronnego powinny obejmować zarówno zabezpieczenie dostępu do komponentów i surowców, jak i rozwój kompetencji, ochronę własności intelektualnej, cyberbezpieczeństwo, stabilizację polityki kontraktowania oraz usprawnienie relacji między przemysłem a administracją publiczną.

3.5. Ocena znaczenia ryzyka dla wybranych kategorii sprzętu wojskowego

Po ocenie prawdopodobieństwa i wpływu ryzyka na poziomie całej branży kolejnym etapem analizy jest określenie znaczenia poszczególnych rodzajów ryzyka dla wybranych kategorii sprzętu wojskowego. Ujęcie branżowe pokazuje ogólną strukturę zagrożeń, ale nie oddaje w pełni różnic wynikających ze specyfiki poszczególnych systemów uzbrojenia. Amunicja artyleryjska 155 mm, BWP BORSUK, system WARMATE, AHS KRAB i AHS K9 różnią się architekturą łańcucha dostaw, poziomem krajowej kontroli nad technologią, zależnością od dostawców za-

granicznych oraz wymaganiami w zakresie utrzymania, serwisu i modernizacji.

Ocena przedstawiona w tabeli 3.5 ma charakter ekspercki i syntetyzuje wnioski z warsztatów oraz charakterystykę modeli łańcuchów dostaw. Nie jest to mechaniczne przeniesienie macierzy ryzyka dla całej branży na poszczególne kategorie sprzętu, lecz wskazuje na względne znaczenie danego obszaru ryzyka dla konkretnego systemu. Zastosowano czterostopniową skalę: niskie, średnie, wysokie i krytyczne znaczenie ryzyka. Niskie oznacza

ryzyko występujące, ale niekluczowe; średnie – ryzyko istotne, lecz możliwe do ograniczenia za pomocą standardowych działań; wysokie – ryzyko mogące poważnie zakłócić produkcję, dostawy, utrzymanie lub modernizację;

krytyczne – ryzyko mogące doprowadzić do przerwania produkcji, opóźnienia programu, utraty zdolności operacyjnej lub trwałego uzależnienia od podmiotu zewnętrznego.

Tab. 3.5. Znaczenie poszczególnych rodzajów ryzyka dla wybranych kategorii sprzętu wojskowego

Obszar ryzyka	Amunicja 155 mm	BWP BORSUK	WARMATE	AHS KRAB	AHS K9
R1: Stabilność finansowa	Wysokie	Wysokie	Średnie	Średnie	Niskie
R2: Wykwalifikowane kadry	Wysokie	Krytyczne	Wysokie	Wysokie	Średnie
R3: Własność intelektualna i transfer technologii	Wysokie	Krytyczne	Wysokie	Wysokie	Krytyczne
R4: Polityka kontraktowania	Krytyczne	Wysokie	Średnie	Wysokie	Średnie
R5: Ograniczona liczba dostawców	Krytyczne	Wysokie	Średnie	Wysokie	Krytyczne
R6: Proces certyfikacji / kwalifikacji	Wysokie	Wysokie	Średnie	Średnie	Niskie
R7: Nierówne warunki konkurowania	Niskie	Średnie	Wysokie	Średnie	Średnie
R8: Szpiegostwo i sabotaż	Wysokie	Wysokie	Wysokie	Wysokie	Wysokie
R9: Cyberbezpieczeństwo	Średnie	Wysokie	Wysokie	Średnie	Średnie
R10: Relacje z władzą administracyjną	Wysokie	Wysokie	Średnie	Wysokie	Średnie
R11: Sytuacja ekonomiczna	Wysokie	Średnie	Średnie	Średnie	Średnie
R12: Sytuacja społeczno-ekologiczna	Wysokie	Średnie	Średnie	Średnie	Średnie

Źródło: opracowanie własne na podstawie warsztatów z przedstawicielami przemysłu obronnego oraz analizy materiałów źródłowych.

W przypadku **amunicji 155 mm** największe znaczenie mają ryzyka związane z polityką kontraktowania, ograniczoną liczbą dostawców, stabilnością finansowania, dostępnością surowców, komponentów i materiałów energetycznych oraz wymaganiami regulacyjno-środowiskowymi. Krytyczne znaczenie R4 wynika z potrzeby podejmowania długoterminowych decyzji zakupowych, stabilnego finansowania oraz przewidywalności zamówień publicznych. Krytyczne znaczenie R5 wiąże się z ograniczoną liczbą dostawców materiałów wysokoenergetycznych, chemikaliów, zapalników, detonatorów i innych elementów niezbędnych do produkcji amunicji na dużą skalę. Wysokie znaczenie mają również ryzyka dotyczące finansów, kadr, transferu technologii, kwalifikacji, relacji z administracją, kosztów oraz regulacji środowiskowych. Niższe znaczenie mają ryzyka cyberbezpieczeństwa i nierówna konkurencja, ponieważ głównym wyzwaniem jest masowa, stabilna i bezpieczna produkcja.

W przypadku **BWP BORSUK** profil ryzyka jest szczególnie złożony, ponieważ jest to projekt rozwojowy i innowacyjny, oparty na krajowych kompetencjach, ale wykorzystujący także wybrane komponenty i technologie z różnych poziomów łańcucha dostaw. Krytyczne znaczenie mają R2 i R3. Ryzyko kadrowe jest krytyczne, ponieważ rozwój, integracja, produkcja, testowanie i modernizacja wymagają utrzymania wyspecjalizowanych zespołów. Ryzyko związane z własnością intelektualną i transferem technologii jest krytyczne ze względu na reżim własności, dokumentację oraz konieczność uzyskiwania zgód na modyfikacje w programach realizowanych przy udziale środków publicznych. Wysokie znaczenie mają także ryzyka finansowe, kontraktowe, dostawcze, certyfikacyjne, cyberbezpieczeństwa, szpiegostwa oraz relacji z administracją. W Borsuku kumulują się zatem ryzyka technologiczne, instytucjonalne i integracyjne.

W przypadku **WARMATE** kluczowe są ryzyka typowe dla systemów opartych na krajowej kontroli technologicznej, własnym *know-how*, szybkim cyklu rozwoju produktu oraz dużym znaczeniu oprogramowania i elektroniki. Wysokie znaczenie mają ryzyka kadrowe, własności intelektualnej, nierównej konkurencji, szpiegostwa, sabotażu i cyberbezpieczeństwa. Przewaga systemu zależy od ochrony rozwiązań konstrukcyjnych, oprogramowania, integracji systemowej i doświadczenia wdrożeniowego. Ryzyka te nie zostały jednak ocenione jako krytyczne, ponieważ system jest już osadzony na rynku, a producent ma relatywnie wysoki poziom kontroli nad kluczowymi elementami produktu. Średnie znaczenie mają ryzyka finansowe, kontraktowe, dostawcze, administracyjne, ekonomiczne i środowiskowo-surowcowe, ponieważ mimo wysokiego poziomu kontroli krajowej nadal występują zależności od wybranych komponentów, w tym elementów napędowych, elektroniki, materiałów i podzespołów.

W przypadku **AHS KRAB** dominują ryzyka właściwe dla programu hybrydowego, łączącego krajową integrację i kompetencje artyleryjskie z elementami technologicznymi oraz komponentami pozyskiwanymi z zewnątrz. Wysokie znaczenie mają ryzyka kadrowe, własności intelektualnej i transferu technologii, polityka kontraktowania, ograniczona liczba dostawców, szpiegostwo i relacje z administracją. Program wymaga utrzymania kompetencji produkcyjnych, integracyjnych i serwisowych, dostępu do komponentów, stabilnych zamówień oraz sprawnej koordynacji między przemysłem a administracją. Średnie znaczenie mają ryzyka certyfikacyjne, cyberbezpieczeństwa, ekonomiczne i społeczno-ekologiczne, które mogą wpływać na tempo i koszty realizacji programu, ale nie stanowią zasadniczego źródła zależności w takim stopniu jak technologie, dostawcy, kontraktowanie i relacje instytucjonalne.

W przypadku **AHS K9** dominują ryzyka wynikające z modelu importu z lokalizacją wsparcia. Krytyczne znaczenie mają R3 i R5, ponieważ zdolność eksploatacji, modernizacji, remontów i rozwoju systemu zależy od zakresu transferu technologii, dostępu do

dokumentacji, zgód licencyjnych, części zamiennych oraz wsparcia ze strony zagranicznego producenta. Jeżeli licencje i umowy nie obejmują szerokich możliwości modyfikacji oraz obsługi technicznej, krajowa autonomia w całym cyklu życia sprzętu pozostaje ograniczona. Wysokie znaczenie ma także ryzyko szpiegostwa i sabotażu, ponieważ infrastruktura serwisowa, magazyny części i procesy logistyczne mogą stać się celem działań przeciwnika. Pozostałe ryzyka mają najczęściej znaczenie średnie lub niskie, gdyż część ryzyka produkcyjnego, rozwojowego i certyfikacyjnego pozostaje po stronie producenta zagranicznego, a po stronie krajowej koncentrują się ryzyka utrzymania, dostępności części i zależności technologicznej.

Porównanie pięciu kategorii sprzętu pokazuje, że profil ryzyka jest silnie powiązany z architekturą łańcucha dostaw. Systemy oparte na krajowej kontroli technologicznej są bardziej wrażliwe na ryzyka związane z kadrami, ochroną wiedzy, cyberbezpieczeństwem, szpiegostwem przemysłowym i możliwością szybkiego rozwoju produktu. Systemy bazujące na zagranicznych technologiach wykazują większą podatność na ryzyka związane z transferem technologii, licencji, dokumentacji, części zamiennych oraz decyzjami państw dostawców. Środki bojowe o wysokim wolumenie zużycia, takie jak amunicja 155 mm, generują natomiast przede wszystkim ryzyka związane ze skalowaniem produkcji, dostępnością surowców, stabilnością zamówień i bezpieczeństwem dostaw.

Wyniki przedstawione wyżej potwierdzają, że odporność polskiego przemysłu obronnego nie może być oceniana wyłącznie przez pryzmat krajowej produkcji końcowej. Kluczowe znaczenie ma również poziom kontroli nad technologią, dostęp do komponentów krytycznych, zdolność serwisowa, stabilność zamówień, bezpieczeństwo informacji, ochrona własności intelektualnej oraz możliwość szybkiej adaptacji produktów do zmieniających się warunków pola walki.

3.6. Zarządzanie ryzykiem

Przedsiębiorstwa polskiego przemysłu obronnego dostrzegają rosnącą ekspozycję na ryzyko i integrują zarządzanie nim w sferach strategicznej, taktycznej i operacyjnej. Celem działań jest budowa odporności na zagrożenia oraz wykorzystanie szans rozwojowych. Podejście wpisuje się w normę ISO 31000:2018, w wymiar przemysłowy „Planu działania na rzecz utrzymania pokoju i gotowości obronnej do 2030 r.” w UE oraz w standardy NATO dotyczące zarządzania ryzykiem. Liderzy łańcuchów dostaw adaptują strategie zalecane w praktykach państw NATO, tj. **unikanie ryzyka** poprzez eliminowanie jego przyczyn, **zmniejszanie** prawdopodobieństwa lub skutków ryzyka, **transfer** odpowiedzialności, **współdzielenie ryzyka** oraz **akceptację ryzyka**. Ważne, że jedna strategia zwykle oddziałuje na więcej niż jeden rodzaj ryzyka.

Przedsiębiorstwa dokonują doboru strategii i metod do specyfiki poszczególnych obszarów ryzyka. Ich przegląd prezentuje tabela 3.6. Zidentyfikowano zarówno metody już stosowane, jak i pożądane do zastosowania w celu wzmocnienia bezpieczeństwa i odporności polskiego przemysłu obronnego. Ich skuteczność w dużej mierze zależy od współpracy oraz synergii decyzji i działań między interesariuszami przemysłu obronnego – przede wszystkim między organami władzy państwowej, siłami zbrojnymi oraz uczestnikami łańcuchów dostaw. Warto również odnotować, że rośnie znaczenie podejścia proaktywnego wobec podejścia reaktywnego – ograniczonego do minimalizacji skutków po wystąpieniu zagrożenia.

Tab. 3.6. Strategie i metody zarządzania ryzykiem w polskim przemyśle obronnym według obszarów

Kod	Obszar ryzyka	Strategia	Metoda
R1	Stabilność finansowa	Zmniejszanie, współdzielenie	• Długoterminowe planowanie rozwoju przemysłu obronnego • Komunikacja z przedsiębiorstwami • Promesa zakupowa państwa • Udział państwa w finansowaniu zapasów krytycznych
R2	Wykwalifikowane kadry	Zmniejszanie	• Rozwój kapitału ludzkiego: <i>reskilling</i> i <i>upskilling</i> • Pozyskiwanie specjalistów z innych branż • Współpraca z uczelniami i szkołami zawodowymi
R3	Własność intelektualna i transfer technologii	Unikanie, zmniejszanie	• Własna działalność badawczo-rozwojowa (<i>in-house</i>), „ucieczka do przodu”, suwerenność technologiczna • Procedury i praktyki zarządzania projektami B+R • Ochrona danych i kontrola dostępu do informacji • Edukacja pracowników • Kultura organizacyjna zorientowana na bezpieczeństwo informacji
R4	Polityka kontraktowania	Zmniejszanie, współdzielenie	• Planowanie zamówień publicznych przez organy państwowe w średnim i długim horyzoncie • Komunikacja i współpraca z przedsiębiorstwami w procesie planowania
R5	Ograniczona liczba dostawców	Zmniejszanie, akceptacja, współdzielenie	• Dywersyfikacja geograficzna i liczby dostawców • Integracja pionowa w łańcuchu dostaw • Utrzymywanie zapasów krytycznych w kraju • Partnerstwa z dostawcami krytycznych zasobów • Partnerstwa m.in. z instytutami wojskowymi, ośrodkami badawczymi i uczelniami na rzecz tworzenia substytutów lub rozwiązań alternatywnych • Wykorzystywanie potencjału startupów • Negocjacje szerokich warunków licencyjnych umożliwiających adaptację i transfer wiedzy, kompleksową obsługę techniczną
R6	Proces certyfikacji	Zmniejszanie, transfer	• Powołanie niezależnej instytucji certyfikującej • Eliminacja konfliktów interesów • Optymalizacja procedur certyfikacji w skali kraju
R7	Nierówne warunki konkurowania	Zmniejszanie	• Transparentność procesów zakupowych • Jednoznaczne kryteria i należyty sposób porównywania ofert • Testowanie sprzętu w warunkach operacyjnych zbliżonych do bojowych

Kod	Obszar ryzyka	Strategia	Metoda
R8	Szpiegostwo i sabotaż	Zmniejszanie	Podział zadań i odpowiedzialności między uczestnikami projektów B+R
R9	Cyberbezpieczeństwo	Zmniejszanie	- Edukacja pracowników - Własna infrastruktura IT i rozwiązania informatyczne, kontrola <i>in-house</i> - Wydzielona infrastruktura dla AI bez zasilania danymi wewnętrznymi
R10	Relacje z administracją publiczną i wojskiem	Zmniejszanie, współdzielenie	- Dialog między organami rządowymi, siłami zbrojnymi a liderami łańcuchów dostaw - Zarządzanie potencjałem krajowego przemysłu obronnego w partnerstwie z przedsiębiorstwami
R11	Sytuacja ekonomiczna	Współdzielenie	- Długookresowa polityka obronna państwa - Rozwój instrumentów finansowania celów obronnych - Programy wspierające inwestycje, finansowanie z Banku Gospodarstwa Krajowego - Udzielanie promesy zakupowej państwa na zakup sprzętu po zakończeniu projektów B+R - Udział państwa w finansowaniu zapasów krytycznych zasobów - Wspieranie eksportu
R12	Sytuacja społeczno-ekologiczna	Transfer, współdzielenie	- Negocjacje unijne odnośnie regulacji i instrumentów polityki środowiskowej - Komunikowanie społeczeństwu celów i założeń polityki obronnej

Źródło: opracowanie własne na podstawie wyników i wniosków z warsztatów z przedstawicielami przemysłu obronnego.

3.7. Rekomendacje

Na podstawie identyfikacji i oceny ryzyka sformułowano cztery zbiorcze rekomendacje, integrujące działania administracji publicznej i przedsiębiorstw. Ułożono je w logice warstwowej: od fundamentów instytucjonalno-regulacyjnych, które warunkują przewidywalność i czas reakcji branży, przez odporność kompetencyjną kapitału ludzkiego jako zasobu krytycznego, aż po odporność operacyjną i bazy dostawców.

1. Budowa instytucjonalnych i regulacyjnych fundamentów odporności. Po stronie administracji publicznej i polityki państwa wskazuje się na powołanie niezależnej instytucji certyfikującej wyroby obronne, eliminującej konflikt interesów z funkcjami badawczo-rozwojowymi pełnionymi przez te same podmioty wojskowe, a także na optymalizację, skrócenie i uelastycznienie procedur oceny zgodności oraz recertyfikacji — zwłaszcza przy modernizacji, zmianach komponentów i aktualizacjach oprogramowania. Niezbędne jest przejście na wieloletnie plany zakupowe, promesy zamówień i stabilne finansowanie, z cykliczną komunikacją polityki obronnej z przemysłem, co stabilizuje horyzont inwestycyjny, w szczególności dla MŚP. Po stronie przedsiębiorstw wskazuje się proaktywne za-

ządzanie ryzykiem ugruntowane w normie ISO 31000:2018, obejmujące stałe mapowanie ryzyka — dostawców krytycznych, komponentów trudno zastępowalnych, zależności licencyjnych, ryzyka kadrowego, cyberzagrożeń — oraz mechanizmy wczesnego ostrzegania. Licencje technologii wojskowych należy projektować z uwzględnieniem niezależności: z prawem do napraw, modernizacji oraz dostępem do dokumentacji i części zamiennych, co pozwala stopniowo wychodzić z zależności licencyjnych. Fundament ten warunkuje skuteczność pozostałych działań, gdyż determinuje czas reakcji i przewidywalność nakładów inwestycyjnych.

2. Wzmacnianie odporności kompetencyjnej kapitału ludzkiego. Wymaga się integracji polityk przemysłowej, edukacyjnej i bezpieczeństwa państwa, wsparcia kształcenia technicznego i zawodowego oraz stworzenia ram branżowego systemu monitorowania kapitału ludzkiego opartego na ujednoliconych wskaźnikach: struktury wieku i płci, rotacji i odejść, czasu rekrutacji na stanowiska krytyczne, liczby i struktury wakatów, sukcesji oraz udziału personelu badawczo-rozwojowego. Po stronie przedsiębiorstw rekomenduje się systematyczny *reskilling* i *upskilling*,

planowanie sukcesji i transferu wiedzy, zarządzanie retencją specjalistów — ścieżki awansu, mechanizmy ograniczające utratę wiedzy — pozyskiwanie kadr z branż pokrewnych (ICT, lotniczej, motoryzacyjnej, maszynowej) oraz partnerstwa z uczelniami i szkolnictwem zawodowym. Odporność kompetencyjna stanowi warunek utrzymania i rozbudowy zdolności badawczo-rozwojowych oraz produkcyjnych w warunkach rosnącego popytu na pracę i konkurencji międzysektorowej.

3. Budowa odporności bazy dostawców i odporności operacyjnej. Wskazuje się na rozwój polityki przemysłowej wspierającej dywersyfikację i stabilność MŚP oraz rozbudowę krajowych zdolności produkcyjnych komponentów krytycznych — amunicji, materiałów wysokoenergetycznych, zapalników, detonatorów i gazogeneratorów. Rekomenduje się selektywną polonizację komponentów, których brak może zatrzymać produkcję, serwis lub modernizację, podczas gdy pozostałe zabezpiecza się przez dywersyfikację dostaw, a także ułatwianie partnerstw na rzecz innowacji z instytutami i uczelniami, nawiązujących do dobrych praktyk umów Łukasiewicz–PGZ (wrzesień 2025) i Łukasiewicz–Grupa WB (ogłoszona grudzień 2025). Po stronie przedsiębiorstw wskazuje się na dywersyfikację geograficzną i liczbową bazy dostawców (rekomendowana kontraktacja z co najmniej dwoma dostawcami zasobów krytycznych), kwalifikację zamienników i utrzymywanie dostawców rezerwowych, utrzymywanie strategicznych zapasów (elektroniki, materiałów specjalnych, surowców krytycznych i komponentów importowanych o długim czasie dostawy), projektowanie produktów modułowych ułatwiających modernizację i stosowanie zamienników oraz selektywną integrację pionową ograniczającą zależność od zewnętrznego know-how. Niezbędne jest także budowanie serwisu i planów ciągłości działania — dokumentacji, magazynów części, kompetencji remontowych i scenariuszy awaryjnych na wypadek cyberataku, sabotażu lub przerwania dostaw. Pogłębione partnerstwa przyspieszają komercjalizację technologii, w tym w obszarze systemów bezzałogowych, amunicji krążącej rodziny WARMATE, systemu GLADIUS i komponentów elektroniki specjalnej.

4. Zarządzanie ryzykiem, finansowanie i dialog strategiczny. Rekomenduje się rozwój instrumentów współdzielenia ryzyka: promesy zakupowej państwa, współfinansowania zapasów krytycznych, specjalistycznego finansowania przez Bank Gospodarstwa Krajowego, wsparcia eksportu i towarzyszącej dyplomacji gospodarczej oraz rozbudowę filaru badawczo-rozwojowego polityki obronnej obok filaru zakupowego. Stabilny rozwój działalności operacyjnej i inwestycyjnej przedsiębiorstw branży obronnej zależy od rozwoju hybrydowego systemu finansowania z wykorzystaniem różnych instrumentów rozwijanych w rezultacie m.in. programów wsparcia krajowego i międzynarodowego (np. European Defence Agency, European Investment Bank) czy dialogu i współpracy z bankami, inwestorami instytucjonalnymi bądź prywatnymi. Wskazuje się na zwiększenie finansowania badań, prototypowania i szybkich wdrożeń w obszarach systemów bezzałogowych, sensorów, łączności, cyberbezpieczeństwa, sztucznej inteligencji, materiałów i rozpoznania. Po stronie przedsiębiorstw warto budować wiarygodność finansową i zdolność absorpcji kapitału, ochronę własności intelektualnej i know-how (segmentacja wiedzy, kontrola dostępu), cyberbezpieczeństwo łańcucha dostaw (wg standardu NIST SP 800-161) oraz strategię ucieczki do przodu opartą na wysokich nakładach na B+R, prowadzącą do suwerenności technologicznej. Warunkiem spójności tych działań jest instytucjonalizacja dialogu państwo–siły zbrojne–przemysł, traktowanego jako narzędzie bezpieczeństwa państwa, umożliwiające wcześniejsze rozpoznanie potrzeb operacyjnych i dostosowanie kierunków B+R.

4. ANALIZA BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ

W CELU ZAPEWNIENIA CIĄGŁOŚCI DOSTAW DO PRODUKCJI I DYSTRYBUCJI SPRZĘTU WOJSKOWEGO I ŚRODKÓW BOJOWYCH

4.1. Infrastruktura transportowa (drogowa, kolejowa, lotnicza)

Infrastruktura transportowa jest jednym z podstawowych warunków utrzymania ciągłości dostaw na potrzeby produkcji i dystrybucji sprzętu wojskowego, uzbrojenia, środków bojowych, komponentów, części zamiennych oraz materiałów specjalnych. Z perspektywy przemysłu obronnego sama długość sieci drogowej, liczba kilometrów linii kolejowych i liczba portów lotniczych nie stanowią wystarczającej podstawy oceny¹³⁴. Kluczowa **jest zdolność państwa do utrzymania przepływów obronno-przemysłowych po wystąpieniu zakłócenia**, czyli możliwość szybkiego przekierowania dostaw czasu przy zachowaniu wymaganych parametrów technicznych, zasad bezpieczeństwa, wymogów dokumentacyjnych oraz terminów realizacji¹³⁵¹³⁶.

W przypadku Polski szczególne znaczenie ma położenie na wschodniej flance NATO, funkcja państwa tranzytowego oraz przebieg trzech europejskich korytarzy TEN-T: Bałtyk–Adriatyk, Morze Północne–Bałtyk oraz Bałtyk–Morze Czarne–Morze Egejskie. Korytarze te tworzą zasadniczy układ transportowy dla przepływów cywilnych i potencjalnych przepływów obronnych¹³⁷. Ich znaczenie nie wynika jednak wyłącznie z przebiegu głównych autostrad, dróg ekspresowych i magistral kolejowych, lecz również z parametrów obiektów inżynierskich, przejść granicznych, terminali, bocznic, ramp, systemów sterowania ruchem, dostępności operatorów oraz możliwości wykorzystania tras alternatywnych¹³⁸.

¹³⁴ Parlament Europejski i Rada, Dyrektywa (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych (CER).

¹³⁵ Ministerstwo Infrastruktury, Strategia Zrównoważonego Rozwoju Transportu do 2030 roku, 2019.

¹³⁶ Komisja Europejska i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa, Action Plan on Military Mobility 2.0, JOIN(2022) 48 final, 10 listopada 2022 r.

¹³⁷ ibidem

¹³⁸ Parlament Europejski i Rada, Rozporządzenie (UE) 2024/1679 z dnia 13 czerwca 2024 r. w sprawie unijnych wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej.

Transport drogowy zapewnia elastyczność oraz umożliwia dystrybucję regionalną, realizację przewozów pilnych oraz pierwszą i obsługę pierwszej oraz ostatniej mili między zakładami produkcyjnymi, magazynami, centrami logistycznymi, terminalami i odbiorcami wojskowymi. Transport kolejowy ma podstawowe znaczenie dla przewozów masowych, ciężkich, powtarzalnych i kontenerowych, zwłaszcza materiałów, amunicji, sprzętu ciężkiego i komponentów przemysłowych. Transport lotniczy nie służy przewozom masowym, lecz może mieć znaczenie krytyczne dla dostaw pilnych, wysokowartościowych i wrażliwych technologicznie, takich jak elektronika, optoelektronika, sensory, części zamienne, komponenty systemów łączności i elementy zaplecza obsługowo-naprawczego.

W praktyce o wykonalności przepływu rozstrzyga łączne spełnienie wymagań dotyczących nośności, skrajni, nacisków osi, klasyfikacji obciążenia (Military Load Classification, MLC), długości składów, dostępności ramp i bocznic, parametrów terminali, stanowisk cargo, systemów sterowania, cyberodporności, paliwa, energii oraz procedur administracyjnych¹³⁹. Szczegółowe dane techniczne, lokalizacyjne i operacyjne mogą być przechowywane w kontrolowanej warstwie informacyjnej dostępnej uprawnionym instytucjom, natomiast raport jawny może posługiwać się klasami ograniczeń i zagregowanymi wskaźnikami^{140 141142}.

4.1.1 Kluczowe ryzyka i luki odporności

Ryzyko w zakresie infrastruktury transportowej oznacza możliwość wystąpienia zdarzenia lub ograniczenia o charakterze technicznym, organizacyjnym, środowiskowym lub cyfrowym, które może spowodować przerwanie, opóźnienie lub utratę przewidywalności dostaw sprzętu wojskowego, środków bojowych, komponentów, części zamiennych lub materiałów specjalnych. Ryzyka transportowe przedstawione w tabeli 4.1 mają charakter wielowarstwowy: obejmują nie tylko drogi, linie kolejowe i lotniska, ale również węzły, terminale, obiekty inżynieryjne, systemy sterowania, dane, energię, paliwa, operatorów i procedury administracyjne.

Powódź z września 2024 r. objęła obszar, przez który przebiegało około 2016 km dróg wojewódzkich, 704 km dróg krajowych i 425 km szlaków kolejowych. Przykład ten pokazuje możliwość jednoczesnego ograniczenia funkcjonowania kilku gałęzi i przeniesienia skutków zakłócenia na węzły zastępcze. Podobny efekt systemowy mogą wywołać awarie zasilania, niedobory paliwa, cyberataki, niedobór operatorów lub przeciążenie terminali. Odporność jest zatem cechą całego układu: infrastruktury, energii, teleinformatyki, operatorów, administracji i procedur pracy w trybie ograniczonym.

Tab. 4.1. Najważniejsze grupy ryzyka i możliwe kierunki jego ograniczania

Grupa ryzyka	Mechanizm lub wąskie gardło	Potencjalny skutek	Kierunek ograniczania ryzyka
Przepustowość i redundancja korytarzy	Przeciążenie sieci, niekompletność ciągów, pojedyncze przeprawy i ograniczona liczba równoważnych tras, zwłaszcza na ostatniej mili	Opóźnienia, rozległe objazdy i kaskadowe przeciążenie sąsiednich węzłów	Analizy wariantów zakłóceńowych; kwalifikacja tras alternatywnych; ukierunkowane usuwanie wąskich gardeł

139 NATO, STANAG 2021. Military Load Classification of Bridges, Ferries, Rafts and Vehicles, Edition 6, NATO/PFP Unclassified, 6 January 2003.

140 International Air Transport Association, Dangerous Goods Regulations, 67. wyd., 2026;

141 Parlament Europejski i Rada, Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2).

142 Parlament Europejski i Rada, dyrektywa (UE) 2022/2557 (CER), dz. cyt.

Grupa ryzyka	Mechanizm lub wąskie gardło	Potencjalny skutek	Kierunek ograniczania ryzyka
Parametry techniczne	Niewystarczająca nośność, skrajnia, nacisk osi, klasa MLC lub parametry dróg startowych i płyt	Brak możliwości realizacji przewozu ciężkiego lub obsługi wymaganego typu statku powietrznego	Kontrolowany rejestr parametrów; audyty MLC; selektywne wzmacnianie obiektów i infrastruktury lotniskowej
Węzły, terminale i ostatnia mila	Niedobór ramp, bocznic, torów ładunkowych, placów, stanowisk obsługi ładunków lotniczych i okien operacyjnych	Kolejki, wydłużenie obsługi i brak możliwości zmiany gałęzi transportu	Ocena rezerwy przepustowości; kwalifikacja węzłów zapasowych; rezerwacja zdolności i modernizacja dostępu
Dane i informacja	Rozproszenie danych, zróżnicowany stopień ich aktualności i brak wspólnych formatów danych o ograniczeniach	Błędna ocena wariantów oraz wydłużenie planowania przewozu specjalnego	Wspólny model danych, właściciel danych, rejestr aktualności danych i poziomu ich wiarygodności
Sterowanie ruchem i cyberbezpieczeństwo	Awarie lub ataki na ITS, systemy sterowania ruchem kolejowym, ERTMS/ETCS, GSM-R i systemy lotnicze	Spadek przepustowości, utrata widoczności i dezorganizacja operacji	Segmentacja sieci; ośrodki rezerwowe; procedury pracy w trybie ograniczonym i ćwiczenia odtworzeniowe
Energia i paliwa	Przerwy zasilania, niedobory paliwa i brak awaryjnych źródeł energii	Zatrzymanie pracy terminali, trakcji, lotnisk lub systemów sterowania mimo sprawnej infrastruktury liniowej	Zasilanie rezerwowe; zapasy paliwa; priorytety przywracania funkcji i warianty pracy w trybie ograniczonym
Pogoda i uszkodzenia fizyczne	Powódź, śnieg, upał, silny wiatr, awaria mostu lub tunelu, sabotaż	Długotrwałe wyłączenie obiektu i przeniesienie zakłócenia na inne gałęzie transportu	Monitorowanie stanu; wcześnie ostrzeganie; procedury szybkiego odtwarzania i testy scenariuszowe
Operatorzy, tabor i ograniczenia transgraniczne	Niedobór kierowców, maszynistów, taboru specjalistycznego, obsługi naziemnej lub kontrolerów; ograniczenia graniczne i zależność od ciężkiego transportu sojuszniczego	Brak możliwości szybkiego zwiększenia przewozów i zależność od dostępności partnerów	Umowy ramowe; rezerwa zdolności; dostęp do zasobów sojusznicznych; wspólne ćwiczenia procesu przewozowego
Awarie infrastruktury krytycznej	Uszkodzenie mostów, przepraw, terminali, lotnisk, centrów sterowania lub innych kluczowych obiektów	Czasowa utrata zdolności operacyjnych i ograniczenie ciągłości dostaw	Monitorowanie stanu infrastruktury (SHM), modernizacja obiektów oraz przygotowanie procedur szybkiego odtwarzania zdolności operacyjnych

Zestawienie wskazuje, że przepływ obronno-przemysłowy może zostać przerwany nie tylko przez uszkodzenie trasy, ale także przez most o niewystarczającej nośności, brak rampy lub przydziału trasy kolejowej, awarię systemu sterowania, brak energii, paliwa, operatora albo aktualnych danych. Z punktu widzenia odporności ważniejszym miernikiem niż nominalna przejezdność jest czas przełączenia na wariant alternatywny o porównywalnych parametrach technicznych i operacyjnych.

4.1.2 Wymagania dotyczące infrastruktury transportowej dual-use

Rozporządzenie wykonawcze Komisji (UE) 2021/1328 określa parametry techniczne i operacyjne infrastruktury transportowej po-

dwójnego zastosowania. W Polsce nie funkcjonuje obecnie jedna spójna baza pozwalająca kompleksowo potwierdzić spełnienie tych wymagań. Dane są częściowo dostępne w otwartych źródłach, w tym w AIP Polska, materiałach PKP PLK i UTK oraz zasobach GDDKiA, GPR i BDOT10k, lecz różnią się szczegółowością, aktualnością i sposobem zapisu. Największym źródłem niepewności planistycznej są braki w danych dotyczących faktycznej nośności mostów, ograniczeń wysokościowych i szerokościowych, gotowości bocznic i torów ładunkowych, zasilania rezerwowego, zdolności do pracy całodobowej oraz rzeczywistej przepustowości terminali i obsługi ładunków lotniczych. Część wymagań z rozporządzenia ma charakter projektowy i powinna być traktowana jako standard przy budowie lub

modernizacji nowych elementów infrastruktury. W odniesieniu do infrastruktury istniejącej możliwe jest natomiast opracowanie wskaźników oceny stopnia spełnienia wymagań, np. udziału długości linii lub odcinków dróg spełniających dany parametr, udziału

portów lotniczych spełniających wymagany próg techniczny albo liczby terminali dysponujących określoną zdolnością operacyjną. Sugerowane wskaźniki oceny stanu infrastruktury podwójnego zastosowania przedstawiono w tabeli 4.2.

Tab. 4.2. Syntetyczna macierz oceny infrastruktury podwójnego zastosowania

Gałąź	Parametry rozstrzygające	Luki w danych i przykładowe wskaźniki
Drogowa	Ciągłość trasy o wymaganej nośności i klasie MLC; skrajnia; dopuszczalne gabaryty; promienie skrętu; parametry mostów; równoważny objazd	Luki dotyczą w szczególności danych o mostach na drogach wojewódzkich i powiatowych oraz ograniczeniach ostatniej mili. Wskaźniki: udział relacji spełniających parametry, liczba ograniczeń krytycznych, czas przełączenia na objazd.
Kolejowa	Nacisk osi, skrajnia, długość pociągu, elektryfikacja, ERTMS, tory ładunkowe, bocznicę, całodobowa praca terminala i zasilanie rezerwowe	Luki dotyczą danych o gotowości bocznic i terminali, dostępności okien oraz rezerwie przepustowości. Wskaźniki: udział linii spełniających parametry, liczba terminali gotowych 24/7, czas zmiany wariantu.
Lotnicza	Długość, szerokość i nośność drogi startowej oraz płyty; stanowiska dla statków powietrznych kodu D–F; terminal ładunkowy; obsługa naziemna; kontrola ruchu, paliwo i ratownictwo	Lukę stanowi brak danych o rzeczywistej zdolności obsługi ciężkich ładunków lotniczych w określonym czasie. Wskaźniki: liczba lotnisk spełniających parametry, liczba dobowych zdolności obsługi, czas odtworzenia operacji.

4.1.3 Modele ruchu jako narzędzie oceny odporności infrastruktury transportowej

Krajowe modele ruchu powinny być wykorzystywane jako narzędzie analizy zdolności i odporności infrastruktury transportowej. Ich podstawową funkcją jest ocena obciążenia sieci, przepustowości, zależności międzygałęziowych, podatności na zamknięcia odcinków oraz skutków przekierowania potoków ruchu. W takim ujęciu model ruchu pozwala sprawdzić, czy infrastruktura posiada wystarczającą zdolność do równoczesnej obsługi ruchu pasażerskiego, towarowego oraz dodatkowych przepływów generowanych przez potrzeby obronne.

W Polsce funkcjonuje kilka krajowych narzędzi o częściowo pokrywających się zakresach, lecz odmiennych funkcjach i zastosowaniach instytucjonalnych. Należą do nich Zintegrowany Model Ruchu (ZMR), rozwijany przez CUPT¹⁴³, Intermodalny Krajowy Model Ruchu (IKMR), wykorzystywany przez GDDKiA¹⁴⁴, oraz

modele rozwijane przez Port Polska: Pasażerski Model Transportowy (PMT)¹⁴⁵ i Towarowy Model Transportowy (TMT)¹⁴⁶. ZMR obejmuje warstwę pasażerską i towarową, IKMR służy m.in. analizie potoków na sieci drogowej, kolejowej i lotniczej, natomiast PMT koncentruje się na ruchu pasażerskim i konkurencyjności gałęzi transportu. Rozwijany TMT ma z kolei odwzorowywać międzygałęziowe przepływy towarowe oraz pełne łańcuchy logistyczne.

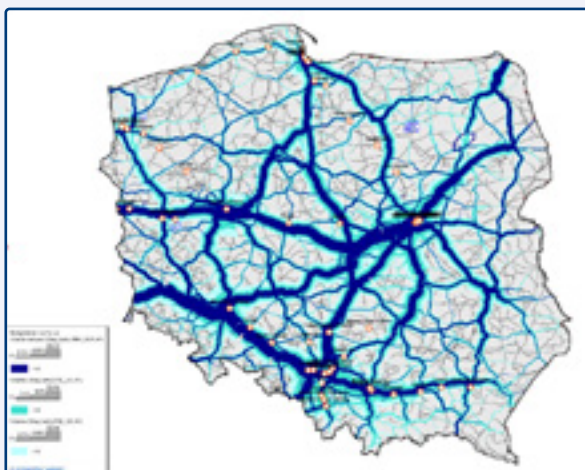
Zakresy tych narzędzi częściowo się pokrywają, dzięki czemu mogą one wzajemnie uzupełniać i weryfikować wyniki (rys. 4.1). Jednocześnie stosowanie odmiennych danych bazowych, założeń prognostycznych, odwzorowania sieci oraz zasad kalibracji może prowadzić do wykonywania podobnych analiz równolegle i uzyskiwania nie w pełni porównywalnych rezultatów. Problemem nie jest zatem samo istnienie kilku modeli, lecz brak wspólnej warstwy referencyjnej i procedur pozwalających wyjaśnić rozbieżności między ich wynikami.

¹⁴³ CUPT – Centrum Unijnych Projektów Transportowych, Zintegrowany Model Ruchu, 2021.

¹⁴⁴ Generalna Dyrekcja Dróg Krajowych i Autostrad, Model Ruchu i Ekonomia, 6.09.2023.

¹⁴⁵ Port Polska, Kolejowy Model Mikrosymulacyjny (KMM).

¹⁴⁶ Port Polska, Pasażerski Model Transportowy,



Rys. 4.1. Rozkład ruchu na autostradach, drogach ekspresowych, krajowych i wojewódzkich – modele PMT oraz IKMR.

Źródło: opracowanie własne na podstawie IKMR oraz PMT

Celem nie powinno być zastąpienie istniejących narzędzi jednym monolitycznym modelem. Poszczególne modele realizują odmienne funkcje i mogą zachować swoją specjalizację, powinny jednak działać w ramach wspólnego krajowego środowiska modelowania. Środowisko to powinno zapewniać jednolite standardy danych, słowniki pojęć, katalog scenariuszy, zasady aktualizacji, kalibracji i walidacji oraz możliwość porównywania wyników. Pozwoliłoby to stosować w różnych modelach te same scenariusze wzrostu przewozów obronnych lub zakłóceń i uzyskiwać porównywalne wskaźniki dotyczące przeciążenia, opóźnień, redundancji oraz zdolności przekierowania ruchu.

Modele te nie zastępują planowania wojskowego ani planowania konkretnych przewozów specjalnych. Tworzą natomiast warstwę odniesienia dla ruchu cywilnego i towarowego: pokazują, gdzie sieć jest przeciążona, które relacje mają ograniczoną redundancję, gdzie mogą wystąpić konflikty między ruchem cywilnym, gospodarczym i obronnym oraz gdzie dodatkowy popyt transportowy może spowodować istotny wzrost opóźnień. Ich wyniki powinny być następnie uzupełniane o dane dotyczące nośności, skrajni, dostępności taboru i operatorów, terminali, bocznicy, procedur oraz ograniczeń właściwych dla przewozów wojskowych.

4.1.4 Ocena odporności i główne ograniczenia

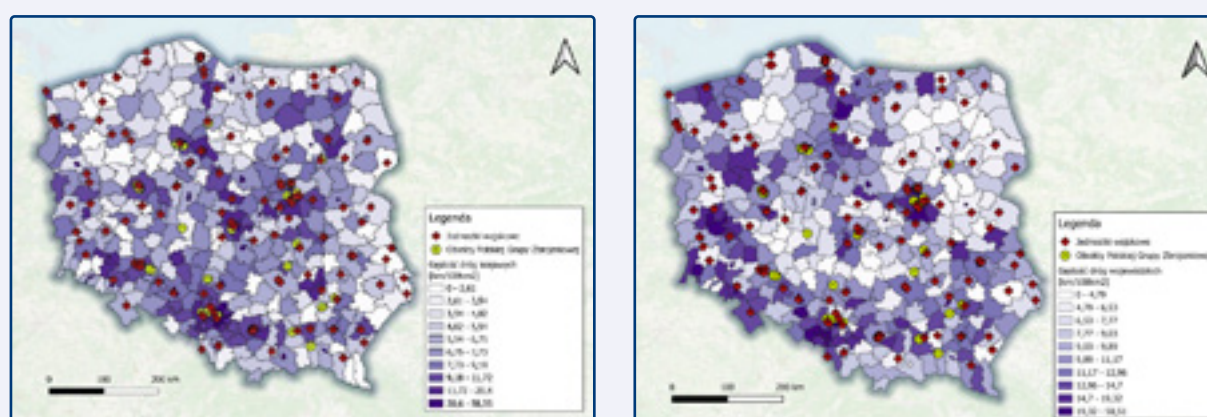
1. Odporność transportowa Polski zależy od głównych korytarzy TEN-T, ale także od węzłów, przejść granicznych i ostatniej mili. Przez Polskę przebiegają trzy kluczowe korytarze TEN-T: Bałtyk–Adriatyk, Morze Północne–Bałtyk oraz Bałtyk–Morze Czarne–Morze Egejskie. Ich znaczenie dla mobilności wojskowej i przemysłu obronnego jest wysokie, ale o skuteczności dostaw decydują również węzły aglomeracyjne, przeprawy przez Wisłę i Odrę, terminale, bocznice, rampy, lotniska cargo, przejścia graniczne oraz drogi dojazdowe do zakładów, magazynów i jednostek wojskowych¹⁴⁷. W praktyce ograniczenie na ostatniej mili może unieważnić dobre parametry głównego korytarza.

2. Największe ryzyko drogowe dotyczy przeciążonych korytarzy, niekompletnych ciągów i ograniczonej redundancji. W 2025 r. autostrady i drogi ekspresowe przenosiły 61% pracy przewozowej na sieci dróg krajowych, natomiast ciągi A4, A1, S8, S7 i A2 odpowiadały łącznie za prawie 40% tej pracy. Sama autostrada A4 odpowiadała za 10,7% pracy przewozowej i pełniła funkcję poprzecznego łącznika trzech korytarzy TEN-T. Z tego powodu szczególnie wrażliwe są relacje, w których kumuluje się ruch cywilny, towarowy, wojskowy i logistyczny albo gdzie brakuje alternatyw o porównywalnych parametrach technicznych. Największe ryzyka dotyczą przeciążenia

¹⁴⁷ Parlament Europejski i Rada, rozporządzenie (UE) 2024/1679, dz. cyt.

korytarzy A1, A2, A4, S8 i S19, w tym odcinków A2 Łódź–Warszawa, A1 w rejonie Piotrkowa Trybunalskiego, S8 Warszawa–Wyszaków, A4 Katowice–Kraków, A4 Katowice–Wrocław oraz A4 Rzeszów–Korczowa. Wrażliwe są również aglomeracje warszawska, krakowska i górnośląska, Węzeł Sośnica, rejon Szczecina oraz przeprawy przez Wisłę i Odrę. Szczegółnej uwagi wymaga północno-wschodnia Polska, w tym Podlasie, Warmia i Mazury, gdzie niższa gęstość dróg wysokich klas nakłada się na strategiczne znaczenie kierunku prowadzącego w rejon przesmyku suwalskiego. W warunkach wzrostu przewozów obronnych lub

skumulowania ruchu cywilnego, wojskowego i towarowego takie braki mogą prowadzić do koncentracji przepływów w pojedynczych punktach sieci. Z tego względu użytecznym miernikiem odporności drogowej jest nie tylko czas przejazdu w warunkach normalnych, lecz także czas przełączenia na trasę alternatywną o porównywalnych parametrach technicznych^{148 149}. Należy także podkreślić, że gęstość dróg krajowych i wojewódzkich (rysunek 4.2) w poszczególnych powiatach kraju jest bardzo zróżnicowana i często nie pokrywa się z rozmieszczeniem jednostek wojskowych oraz obiektów Polskiej Grupy Zbrojeniowej.



Rys. 4.2. Gęstość dróg krajowych i wojewódzkich w powiatach [km/100 km²]

Źródło: opracowanie własne na podstawie BDOT10k

3. Rozproszenie danych o parametrach infrastruktury i zróżnicowany stopień ich aktualności. Mosty, wiadukty, tunele, przeprawy promowe, skrajnia i nośność dróg mogą stać się wąskim gardłem nawet wtedy, gdy główny korytarz jest formalnie przejezdny. Problem dotyczy zwłaszcza infrastruktury położonej poza siecią dróg krajowych, dla której dane o rzeczywistej nośności i stanie obiektów inżynierskich są fragmentaryczne albo prowadzone w różnych systemach. Ograniczeniu tej niepewności może służyć kontrolowany rejestr parametrów infrastruktury podwójnego zastosowania, obejmujący m.in. wojskową klasyfikację obciążenia MLC zgodną ze STANAG 2021, skrajnię, stan techniczny obiektów, ograniczenia oraz wykonalne warianty objazdów¹⁵⁰. Warstwa jawna takiego rejestru mo-

głaby przedstawiać klasy infrastruktury, kryteria oceny i zagregowane wskaźniki, natomiast warstwa operacyjna, dostępna uprawnionym instytucjom, mogłaby zawierać szczegółowe parametry obiektów, poziom pewności i aktualności danych oraz możliwe warianty przekierowania przewozów.

4. Transport kolejowy powinien stanowić podstawową warstwę odporności w przypadku przewozów masowych i ciężkich ładunków, ale wymaga oceny całego procesu przewozowego. Polska dysponuje siecią kolejową liczącą około 20 tys. km linii, z czego około 71,9% znajduje się w stanie dobrym, 20,5% w stanie dostatecznym, a 7,5% w stanie niezadowolającym^{151 152}. Dla przemysłu obronnego szczególne znaczenie mają ma-

148 Generalna Dyrekcja Dróg Krajowych i Autostrad, Generalny Pomiar Ruchu 2025, 2025.

149 Ministerstwo Infrastruktury, Strategia Zrównoważonego Rozwoju Transportu do 2030 roku, dz. cyt.

150 NATO, STANAG 2021, dz. cyt.

151 PKP Polskie Linie Kolejowe S.A., Raport Roczny 2024, 2025.

152 Urząd Transportu Kolejowego, Sprawozdanie z funkcjonowania rynku transportu kolejowego w 2024 r., 2025.

gistrale E20, E30, E59, E65 i E75, łączące główne ośrodki przemysłowe, terminale, przejścia graniczne i porty lotnicze lub morskie. Sama dostępność linii nie przesądza jednak o zdolności wykonania dostawy. Znaczenie mają również terminale, bocznice, rampy, stacje rozrządowe, dostępność lokomotyw i wagonów, przydzielone trasy pociągów, zasilanie oraz systemy sterowania ruchem. Średnia prędkość handlowa przewozów intermodalnych wynosiła w 2024 r. 37,4 km/h wobec około 50 km/h w Unii Europejskiej, co wskazuje, że rezerwy czasowe zależą zarówno od parametrów infrastruktury, jak i od organizacji ruchu oraz obsługi terminalowej¹⁵³.

5. Potencjalna podatność kolei koncentruje się na głównych magistralach, węzłach, liniach jednotorowych, terminalach i obiektach inżynieryjnych. Ryzyka dotyczą m.in. odcinków Warszawa–Poznań na E20, Warszawa–Gdańsk na E65, Katowice–Kraków–Rzeszów na E30, Poznań–Wrocław na E59 oraz Warszawskiego Węzła Kolejowego. Istotne są również połączenia do terminala w Małaszewiczach, odcinki Rail Baltica, kierunki do przejść granicznych z Ukrainą, zwłaszcza Medyka–Przemyśl i Hrubieszów–Izow, oraz terminale w Małaszewiczach, Sławkowie, Kutnie, Poznaniu i Gdańsku. Wysoki udział linii jednotorowych, sięgający około 54%, powoduje, że awaria, wykolejenie lub prace utrzymaniowe mogą całkowicie zatrzymać ruch na wybranych relacjach. Szczególnej uwagi wymagają także mosty kolejowe przez Wisłę w Warszawie, Tczewie, Dęblinie i Krakowie, przeprawy przez Odrę w rejonie Wrocławia, tunel średnicowy w Warszawie, Centralna Magistrala Kolejowa oraz główne stacje rozrządowe^{154 155}.

6. Transport lotniczy powinien być traktowany jako kanał realizacji pilnych dostaw wybranych kategorii ładunków, a nie przewozów masowych. Lotnicze przewozy towarowe mają znaczenie przede wszystkim dla dostaw wysokowartościowych i wymagają-

cych szybkiej realizacji: elektroniki, optoelektroniki, sensorów, komponentów systemów łączności, części zamiennych oraz elementów zaplecza obsługowo-naprawczego. Kluczowe są parametry nośności i wymiary dróg startowych, dróg kołowania i płyt postojowych, dostępność stanowisk dla samolotów klas D, E i F, przepustowość terminali towarowych, paliwo, energia, obsługa naziemna oraz procedury bezpieczeństwa¹⁵⁶. W przypadku ciężkiego transportu lotniczego Polska pozostaje w znacznym stopniu zależna od zdolności sojuszników¹⁵⁷. Obsługa największych statków powietrznych, takich jak C-17 Globemaster III lub C-5M Super Galaxy, wymaga odpowiednio przygotowanych lotnisk, takich jak Rzeszów-Jasionka, Lotnisko Chopina w Warszawie lub Katowice-Pyrzowice.

7. Odporność transportowa zależy od czynników przekrojowych: energii, paliw, cyberbezpieczeństwa, warunków klimatycznych, kadr i kosztów. Zakłócenie systemów sterowania ruchem, awaria zasilania, brak paliwa, cyberatak, powódź, oblodzenie, silny wiatr, niedobór operatorów albo skokowy wzrost kosztów transportu mogą zatrzymać przepływ mimo istnienia infrastruktury fizycznej. Szczególnie narażone są obszary południowej i południowo-zachodniej Polski, w tym województwa dolnośląskie, opolskie, śląskie, małopolskie i podkarpackie, przez które przebiegają strategiczne korytarze, w tym A4, S7 i S19. Podobny skutek mogą mieć przerwy w zasilaniu, niedobory paliwa, awarie systemów sterowania ruchem, cyberataki na systemy ITS, urządzenia sterowania ruchem kolejowym, ERTMS/ETCS, GSM-R, systemy lotnicze oraz bazy danych. Dlatego infrastruktura transportowa powinna być planowana jako system współzależny z energetyką, teleinformatyką, administracją, operatorami i procedurami pracy w trybie ograniczonym.

¹⁵³ Ibidem.

¹⁵⁴ Ibidem.

¹⁵⁵ PKP Polskie Linie Kolejowe S.A., Raport Roczny 2024, dz. cyt.;

¹⁵⁶ International Civil Aviation Organization, Annex 14 to the Convention on International Civil Aviation: Aerodromes. Volume I: Aerodrome Design and Operations, 9th ed., 2022.

¹⁵⁷ Strategic Airlift Capability, Member Nations – Poland, b.r. (dostęp: 17.08.2026).

4.2. Infrastruktura logistyczna

Infrastruktura logistyczna polskiego przemysłu obronnego nie powinna być rozumiana wyłącznie jako zbiór magazynów, centrów dystrybucyjnych, placów, ramp, bocznic i środków transportu¹⁵⁸. Z perspektywy MON i Sił Zbrojnych RP jest to **system zdolności dual-use**, który ma zapewnić dostarczenie komponentów, części, materiałów, wyrobów gotowych i usług serwisowych w wymaganym czasie, jakości, ilości i reżimie bezpieczeństwa^{159 160}.

Kluczowy problem decyzyjny polega na tym, że Polska posiada znaczący potencjał cywilnej i przemysłowej infrastruktury logistycznej, lecz nie jest on automatycznie gotową zdolnością obronną. Magazyn, operator logistyczny, terminal lub system zarządzania magazynem, transportem i zasobami przedsiębiorstwa mają wartość dla obronności dopiero po rozpoznaniu, kwalifikacji, zabezpieczeniu kontraktowym i informacyjnym oraz praktycznym przetestowaniu^{161 162}.

Logistyka nie jest funkcją pomocniczą wobec produkcji, lecz warunkiem realnej zdolności produkcyjnej, dystrybucyjnej i serwisowej^{163 164}. Wzrost mocy w produkcji amunicji, pojazdów, elektroniki, optoelektroniki, systemów łączności, systemów bezzałogowych oraz w obsłudze, naprawach i remontach ma wartość operacyjną tylko wtedy, gdy równolegle dostępne są zapasy krytyczne, opakowania, dokumentacja, kontrola jakości, obsługa materiałów specjalnych, kompletacja, operatorzy, okna przeładunkowe, dane, personel i wariant działania po zakłóceniu^{165 166}.

Z perspektywy decyzyjnej użyteczniejszym przedmiotem zarządzania niż pojedyncza usługa magazynowa lub przewozowa jest gotowość całego przepływu. Obejmuje ona właściciela procesu, katalog zdolności podwójnego zastosowania, dostęp do operatorów, logistyczny wykaz materiałowo-procesowy dla produktów krytycznych, zdolności serwisowe oraz regularne testowanie wariantów dostawy. Infrastruktura logistyczna obejmuje sześć funkcji krytycznych: zaopatrzenie produkcji, magazynowanie i buforowanie, transport i przeładunek, widoczność danych, obsługę, naprawy i remonty oraz regulacje i bezpieczeństwo..

4.2.1 Skala potencjału i warstwy wykorzystania

Na koniec marca 2026 r. zasoby nowoczesnej powierzchni magazynowej w Polsce osiągnęły około 37,4 mln m², a w pierwszym kwartale oddano ponad 653 tys. m². Przy wskaźniku pustostanów 7,3% teoretycznie dostępne było około 2,73 mln m², jednak podaż była silnie zróżnicowana regionalnie¹⁶⁷. Największe skupiska tworzyły obszary Warszawy, Górnego Śląska, Polski Centralnej, Wrocławia i Poznania. Dane potwierdzają dużą skalę zasobu cywilnego, ale nie przesądzają o dostępności konkretnego obiektu, jego profilu technicznym, poziomie ochrony ani możliwości nadania dostawom obronnym priorytetu^{168 169}. Dostępność infrastruktury magazynowej na tle jednostek wojskowych w Polsce przedstawiono na rysunku 4.3.

158 NATO, NATO's role in logistics, 2025.

159 NATO, Resilience, Civil Preparedness and Article 3, 2024.

160 Rządowe Centrum Bezpieczeństwa, Systemy infrastruktury krytycznej, 2024 (dostęp: 09.07.2026).

161 UK Ministry of Defence, Defence Supply Chain Strategy, 2022.

162 RAND Corporation, Toward Defense Supply Chain Disruption Management, 2024.

163 European Commission, White Paper for European Defence Readiness 2030, European Union, 2025.

164 European Commission, European Defence Readiness Roadmap 2030, European Union, 2025.

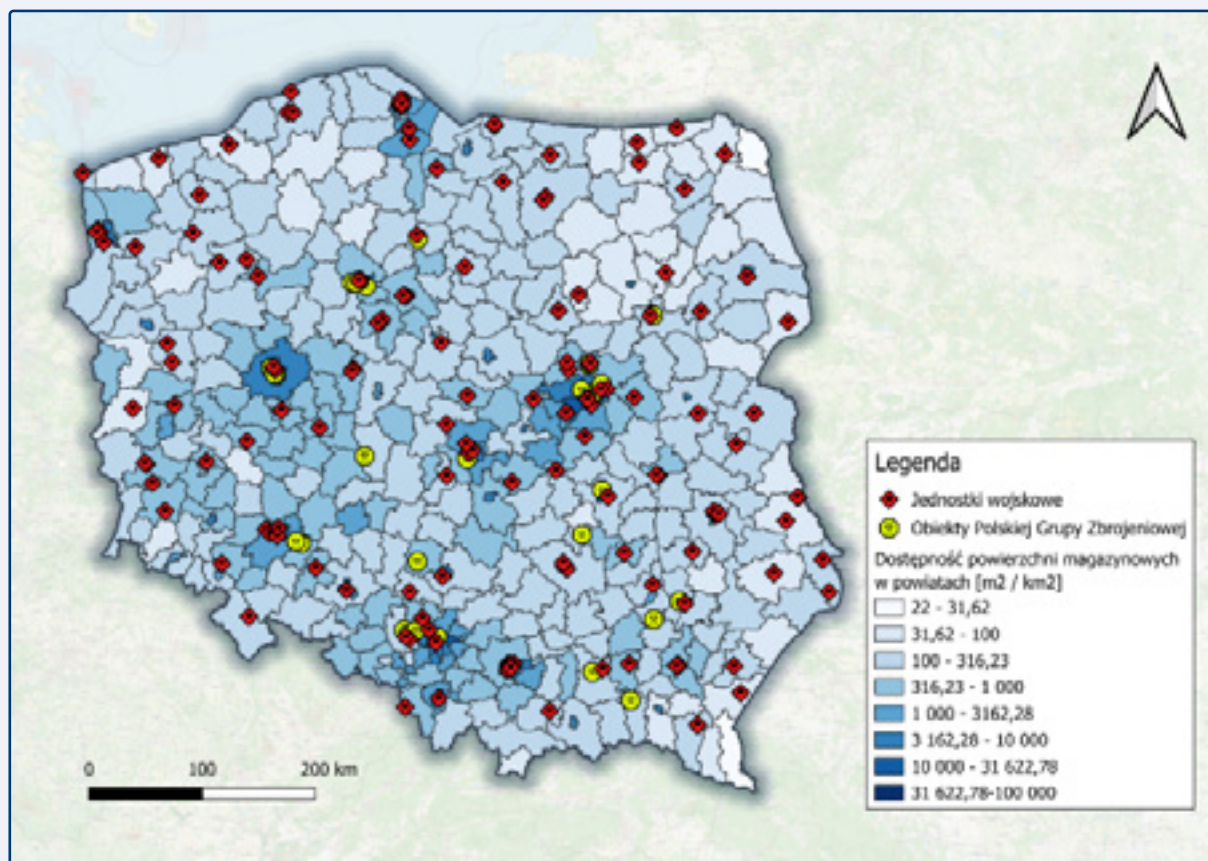
165 NATO, Defence-Critical Supply Chain Security Roadmap, 2024.

166 U.S. Defense Business Board, Supply Chain Illumination in the Department of Defense, 2025.

167 <https://ceo.com.pl/en/strong-start-to-the-year-on-the-industrial-market-in-poland-with-a-clear-increase-in-new-leases-and-expansions-12768/> (dostęp: 03.07.2026).

168 <https://www.axiimm.com/raporty-i-publikacje/pozytywne-otwarcie-roku-na-rynku-magazynowym-wyrazny-wzrost-nowych-umow-najmu-i-ekspansji/> (dostęp: 03.07.2026).

169 <https://www.cushmanwakefield.com/en/poland/insights/industrial-marketbeat> (dostęp: 03.07.2026).



Rys. 4.3. Dostępność infrastruktury magazynowej na tle jednostek wojskowych w Polsce

Z perspektywy wsparcia przemysłu obronnego najważniejszy jest nie tylko rozmiar rynku, ale także jego funkcjonalna różnorodność. Polska ma zarówno duże magazyny klasy A i parki regionalne dla masowego składowania i dystrybucji, jak i parki miejskie, obiekty budowane pod konkretnego użytkownika, platformy kompletacyjne, terminale przeładunkowe, magazyny chłodnicze czy obiekty przygotowane do obsługi produktów chemicznych i towarów podlegającym

szczególnym wymagom. To oznacza, że cywilna infrastruktura może wspierać odporność logistyczną państwa, ale nie jako prosty zamiennik infrastruktury wojskowej. Jej wartość polega raczej na tworzeniu rozproszonej, kontraktowo zabezpieczonej warstwy wsparcia dla części zamiennych, komponentów, opakowań, materiałów utrzymaniowych, wyrobów medycznych, dostaw o wysokiej rotacji i zapasów buforowych.

Równolegle rośnie zapotrzebowanie logistyczne przemysłu obronnego. Jawne decyzje inwestycyjne pokazują, że rozbudowa przemysłu obronnego nie ogranicza się do nowych hal i linii produkcyjnych. Huta Stalowa Wola realizuje program o wartości 1,37 mld zł, zwiększający zdolności dostaw m.in. dla Borsuka oraz programów Wisła i Narew, co oznacza większe przepływy podzespołów wielkogabarytowych, części i wyrobów gotowych¹⁷⁰. W MESKO uruchomienie hali o powierzchni ponad 4 tys. m² zwiększyło zdolność produkcji amunicji małokalibrowej z 50 do 250 mln sztuk rocznie, podnosząc wymagania wobec składowania, kontroli partii, dokumentacji i wysyłki¹⁷¹. Z kolei program rozwoju produkcji amunicji 155 mm obejmuje równolegle Dezamet, MESKO, Nitro-Chem i Gamrat, dlatego jego powodzenie zależy od synchronizacji przepływów między zakładami¹⁷². Najbardziej bezpośrednim przykładem jest spółka Rosomak S.A., gdzie nową linię produkcyjną powiązano z modernizacją magazynu centralnego, cyfrowym planowaniem zasobów i integracją logistyki z produkcją¹⁷³. Przykłady te potwierdzają, że bez równoległego rozwoju zaplecza logistycznego wzrost produkcji może jedynie przenieść wąskie gardło z hali do magazynu, kompletacji lub wysyłki.

Dla polskiego przemysłu obronnego zasadne jest przyjęcie modelu warstwowego przedstawionego w tabeli 4.3. Nie każdy zapas musi być utrzymywany w obiekcie wojskowym, nie każdy magazyn przemysłowy musi być przygotowany do obsługi materiałów

specjalnych i nie każda powierzchnia cywilna może zostać użyta do celów obronnych. Wartość systemu wynika z dopasowania rodzaju zasobu do właściwej warstwy infrastruktury, poziomu ochrony, reżimu prawnego i wymaganego czasu reakcji.

Tab. 4.3. Warstwowy model infrastruktury logistycznej dla łańcuchów dostaw obronności

Warstwa	Główna rola	Typowe zasoby	Warunek użyteczności dla obronności
Zakładowa i przy-produkcyjna	Zasilanie produkcji i stabilizacja rytmu montażu	Materiały, półprodukty, produkcja w toku, komponenty i elementy wielkogabarytowe	Integracja z planowaniem produkcji, kontrola jakości, dokładna ewidencja stanów i szybkie wydanie
Specjalistyczna	Bezpieczne składowanie zasobów wymagających odrębnego reżimu	Materiały wybuchowe, chemia, paliwa, baterie, sensory, optyka i elektronika wrażliwa	Zgodność regulacyjna, ochrona fizyczna i przeciwpożarowa oraz kontrolowane warunki
Centra serwisowe i części	Utrzymanie sprawności sprzętu i skrócenie czasu napraw	Części, narzędzia specjalne, dokumentacja i zestawy obsługowe	Dostępność i śladowość części, personel, narzędzia i powiązanie z producentem
Cywilni operatorzy logistyczni	Bufory, kompletacja, przeładunek, dystrybucja i obsługa celna	Komponenty podwójnego zastosowania, opakowania, części niewrażliwe i zapasy rotacyjne	Umowy ramowe, audyt bezpieczeństwa, priorytet dostępu, zgodność danych i plan ciągłości działania
Publiczna i wojskowa	Rezerwy strategiczne oraz przyjęcie i dystrybucja po stronie odbiorcy	Zasoby rezerwowe, sprzęt, środki bojowe i materiały eksploatacyjne	Zasady uruchomienia i rotacji oraz zgodność z procedurami odbioru i planami przemieszczeń
Cyfrowa - przekrojowa	Widoczność zapasów, partii, dokumentów i zdolności wydania	Systemy magazynowe, transportowe i produkcyjne, ewidencja partii, sensory i raporty	Segmentacja dostępu, cyberbezpieczeństwo, aktualność danych i tryb awaryjny

Model warstwowy ogranicza dwa uproszczenia: utożsamianie całego rynku cywilnego z gotową zdolnością obronną oraz kierowanie wszystkich klas zasobów do infrastruktury specjalistycznej. Wartość systemu wynika z dopasowania rodzaju zasobu do właściwej warstwy, operatora, poziomu ochrony i wymaganego czasu reakcji.

170 <https://www.hsw.pl/inwestycje-wspolfinansowane-ze-srodkow-funduszu-inwestycji-kapitalowych/> (dostęp: 03.07.2026).

171 <https://www.mesko.com.pl/aktualnosci/mesko-sa-pieciokrotnie-zwiekszylo-moce-produkcyjne-amunicji-malokalibrowej> (dostęp: 03.07.2026)

172 <https://www.gov.pl/web/aktywa-panstwowe/24-mld-zl-dla-pgz-na-dofinansowanie-produkcji-amunicji-155-mm> (dostęp: 03.07.2026)

173 <https://www.slaskie.pl/content/wsparcie-ksse-dla-inwestycji-w-rosomaku> (dostęp: 03.07.2026).

4.2.2 Ryzyka systemowe i możliwe kierunki ograniczania

Ryzyka infrastruktury logistycznej należy ujmować jako ryzyka całego przepływu: od dostępności komponentu lub części, przez magazynowanie, dokumentację, dostępność operatora, transport, przeładunek, dane, MRO, energię i odbiór, aż po utrzymanie sprzętu w cyklu życia. Dla decydenta

kluczowe są nie pojedyncze zdarzenia, lecz grupy ryzyk, które mogą zatrzymać produkcję, opóźnić dostawę albo obniżyć gotowość techniczną Sił Zbrojnych RP. Najważniejsze ryzyka oraz kierunki ich ograniczania przedstawiono w tabeli 4.4.

Tab. 4.4. Rejestr ryzyk w zakresie zapewnienia mobilności strategicznej i dostaw sprzętu wojskowego oraz kierunki optymalizacji

Ryzyko strategiczne	Mechanizm	Potencjalny skutek	Kierunek ograniczania
Cywilne zasoby bez gwarancji dostępu	Brak operatora, miejsca, floty lub okien w chwili skokowego popytu	Opóźnienie dostaw, konkurencja z rynkiem komercyjnym	Umowy ramowe, rezerwacja zdolności, portfel wielowarstwowy, ćwiczenia aktywacyjne
Brak widoczności pod-dostawców	Brak wiedzy o krytycznych dostawcach, materiałach i zamiennikach	Zatrzymanie produkcji wyrobu z powodu braku nawet niewielkiego komponentu	Logistyczny BOM/SBOM, lista elementów krytycznych, mapa ryzyk dostawców, kwalifikacja zamienników
Niesynchronizowany wzrost mocy	Nowe hale, linie produkcyjne, magazyny, zakładowe, dokumentacja, jakość, wysyłka	Wzrost mocy produkcyjnych nie przekłada się na realne dostawy	Obowiązkowy plan logistyczny dla każdej inwestycji produkcyjnej
Obsługa materiałów specjalnych i niebezpiecznych	Brak certyfikowanych obiektów, przewoźników lub dokumentacji	Blokada przewozu, niezgodność regulacyjna, ryzyko BHP i bezpieczeństwa	Katalog zdolności ADR/RID, katalog certyfikowanych obiektów, przewoźników i procedur dla towarów specjalnych
Przepustowość transportowa i parametry infrastruktury	Niedobór taboru, okien obsługowych, terminali, placów, bocznic lub kłosew. Niska nośność mostów w klasyfikacji MLC dla ciężkich pojazdów	Wydłużony czas przewozu, kolejki i utrata priorytetu, konieczność stosowania długich tras objazdowych dla ciężkiego sprzętu	Warianty multimodalne, rezerwacja okien obsługowych, umowy z przewoźnikami, monitorowanie rynku, audyt i wzmacnianie obiektów inżynierskich na trasach strategicznych
Brak wspólnego obrazu danych i cyberodporności	Systemy ERP/WMS/TMS, API/EDI, śledzenie przesyłek, chmura, GNSS, systemy operatorów	Opóźniona reakcja, utrata poufności, ryzyko cybernetyczne, brak możliwości śledzenia przesyłek w czasie rzeczywistym	Standard danych, segmentacja informacji, audyty NIS2, Krajowe Centrum Koordynacji Logistycznej
MRO i części zamienne	Brak części, narzędzi, dokumentacji lub serwisantów.	Dostarczony sprzęt pozostaje niesprawny lub długo oczekuje na naprawę.	Dostawa części zamiennych jako osobny łańcuch, zapasy minimalne, regionalny zdolności obsługowo-naprawcze, szybkie przesyłki.
Energia, paliwa, klimat i odporność obiektów	Magazyny, automatyka, terminale, systemy IT, transport, zasilanie	Paraliż systemów informatycznych (WMS/TMS), zatrzymanie pracy suwnic, terminali i automatyki magazynowej, wstrzymanie wysyłek	Zasilanie awaryjne, zapasy paliwa, procedury manualne, zakładowe mikrosieci i magazyny energii
Koncentracja zdolności i pojedyncze punkty awarii	Opieranie kluczowych programów obronnych na pojedynczych fabrykach, liniach produkcyjnych lub magazynach centralnych	Paraliż całego programu zbrojeniowego w wyniku jednej awarii, pożaru lub błędu w pojedynczym obiekcie	Tworzenie równoległych linii produkcyjnych, satelickie magazyny buforowe, budowanie modelu wielu dostawców
Brak właściciela całego przepływu	Podział odpowiedzialności między dostawcą, magazyn, operatora, odbiorcę i administrację	Każdy odcinek działa lokalnie, ale cały przepływ nie osiąga wymaganego czasu	Właściciel przepływu, pulpit monitorowania odchyleń, kluczowe wskaźniki efektywności od zgłoszenia potrzeby do dostawy, procedury eskalacji

Ryzyko strategiczne	Mechanizm	Potencjalny skutek	Kierunek ograniczania
Erozja unikalnych kompetencji kadrowych	Odpływ ekspertów ds. logistyki wojskowej, IT i towarów niebezpiecznych do lepiej płatnego sektora cywilnego; luka pokoleniowa	Zatory operacyjne i proceduralne, brak zdolności do obsługi systemów logistycznych i towarów specjalnych mimo posiadania infrastruktury	Programy sukcesji, konkurencyjne systemy motywacyjne dla kluczowego personelu, specjalistyczne klasy i kierunki kształcenia o profilu podwójnego zastosowania, zarządzanie wiedzą
Zakłócenia GNSS, platform cyfrowych i usług chmurowych	Zagłuszanie (<i>jamming</i>) i fałszowanie (<i>spoofing</i>) sygnałów satelitarnych, cyberataki na chmurowe systemy	Utrata wiarygodności danych lokalizacyjnych i harmonogramów, paraliż floty i aplikacji operacyjnych, utrata synchronizacji czasu	Nawigacja alternatywna, monitorowanie anomalii (RTGMS), chmury hybrydowe, budowa suwerenności rozpoznawczej i logistycznej z PGZ wspólnie z Wojskowymi Zakładami Elektronicznymi S.A. inwestuje także w budowę Centrum Serwisowo-Produkcyjnego pocisków rakietowych CAMM-ER oraz hali produkcyjnej elementów systemu obrony przeciwlotniczej i przeciwrakietowej. wykorzystaniem konstelacji satelitarnej PIAST

Zestawienie potwierdza systemowy charakter ryzyk. Ułatwia ono określenie, które zdolności wymagają bezpośredniej kontroli państwa lub przemysłu, które mogą być kontraktowane, dla których uzasadnione jest utrzymywanie zapasów, a w których wystarczająca może być dywersyfikacja dostawców, operatorów i wariantów działania.

4.2.3 Kluczowe luki zdolności logistycznych

1. Infrastruktura logistyczna jest zdolnością operacyjną, a nie zapleczem administracyjnym. Magazyny, centra logistyczne, rampy, place, bocznice i środki transportu mają znaczenie obronne dopiero wtedy, gdy są powiązane z procedurami, danymi, operatorami, zapasami, dokumentacją, personelem, zabezpieczeniem energetycznym, cyberodpornością i reżimem bezpieczeństwa. Sama dostępność powierzchni magazynowej nie tworzy odporności, jeżeli brakuje możliwości kompletacji, oznakowania, kontroli jakości, obsługi towarów specjalnych, integracji systemów informatycznych lub szybkiego wydania partii.

2. Cywilny potencjał logistyczny Polski jest zasobem, ale nie jest automatycznie zdolnością obronną. Krajowy i międzynarodowy rynek operatorów może wzmacniać odporność przemysłu obronnego, jednak wymaga wcześniejszego przygotowania. Nie chodzi o rezygnację z operatorów globalnych, lecz o budowę portfela obejmującego krajowe podmioty o trwałym zapleczu terytorialnym, operatorów magazynowania i dystrybucji, przewoźników ładunków ciężkich, niebezpiecznych i ponadnormatywnych oraz globalnych integratorów obsługujących dostawy pilnych, wysokowartościowych i międzynarodowych. Portfel ten powinien

być wsparty umowami ramowymi, rezerwacją zdolności, wymogami ochrony informacji, interoperacyjnością danych, procedurami awaryjnymi i ćwiczeniami aktywacyjnymi.

3. Rozbudowa produkcji tworzy ryzyko przeniesienia wąskiego gardła z hali produkcyjnej do logistyki. Jawne decyzje inwestycyjne potwierdzają szybki wzrost krajowych mocy produkcyjnych, natomiast dostępne informacje nie pozwalają ocenić, czy zdolności magazynowe, przeładunkowe, transportowe i wysyłkowe zwiększają się proporcjonalnie. Rozbudowa produkcji uzbrojenia, amunicji, sprzętu wojskowego, elektroniki, optoelektroniki i obsługi technicznej jest strategicznie korzystna, ale jej wpływ na bezpieczeństwo dostaw będzie ograniczony bez równoległego zabezpieczenia logistycznego. Dotyczy to zwłaszcza zapasów krytycznych, opakowań, dokumentacji, kontroli jakości, dostępu do operatorów, obsługi materiałów niebezpiecznych, zdolności przeładunkowych, systemu monitorowania odchyleń i zakłóceń oraz właściciela ryzyka logistycznego dla każdego programu uzbrojenia o krytycznym znaczeniu.

4. O dostępności operacyjnej sprzętu decyduje nie tylko jego dostawa, lecz także zdolność do utrzymania i szybkiego odtworzenia sprawności. Obsługa techniczna, naprawy i remonty (MRO) oraz zaopatrzenie

w części zamienne powinny być traktowane jako krytyczny łańcuch logistyczny obejmujący magazynowanie, wydawanie i dystrybucję części, dostarczanie narzędzi specjalistycznych i zestawów serwisowych, a także obsługę zwrotów elementów uszkodzonych. W przypadku pojazdów, sprzętu ciężkiego, systemów łączności, optoelektroniki i elektroniki wojskowej brak pojedynczej części krytycznej, właściwego narzędzia, dokumentacji lub dostępu do zaplecza naprawczego może wyłączyć sprzęt z użytkowania, mimo że formalnie pozostaje on w zasobie. Ocena zdolności logistycznej powinna zatem obejmować rozmieszczenie i poziom zapasów części krytycznych, czas ich wydania i dostarczenia, dostępność krajowych zdolności naprawczych, personelu technicznego, stanowisk diagnostycznych, dokumentacji oraz oprogramowania serwisowego. Elementy te powinny być uzupełnione rozwiązaniami organizacyjnymi i umownymi zapewniającymi dostęp do niezbędnych danych, narzędzi, ak-

tualizacji i usług serwisowych w całym cyklu życia sprzętu.

5. Ograniczona widoczność poddostawców niższych poziomów łańcucha dostaw i komponentów krytycznych stanowi istotne ryzyko już w czasie pokoju. Informacje jawne pozwalają wskazać kierunki inwestycji i podstawowe rodzaje zagrożeń, lecz nie umożliwiają pełnej oceny odporności bez audytu opartego na danych operacyjnych, częściowo niejawnym. Dla produktów krytycznych konieczny jest logistyczny wykaz materiałowo-procesowy obejmujący komponenty, źródła, czasy dostaw, zamienniki, zapasy minimalne, wymagania transportowe, dokumentację i status jakościowy. Wykaz taki powinien umożliwiać identyfikację elementów, których brak może zatrzymać produkcję, opóźnić dostawę albo uniemożliwić naprawę^{174 175}.

4.3. Krytyczna infrastruktura elektroenergetyczna

Energetyka i paliwa, jako dwa obszary gospodarki, zostały zakwalifikowane do infrastruktury krytycznej państwa (ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym). Analiza przedstawiona w tym rozdziale została ograniczona do jednego z elementów tej infrastruktury, jakim jest energia elektryczna. Energia elektryczna jest wytwarzana z wykorzystaniem paliw kopalnych i źródeł odnawialnych w wielkoskalowych elektrowniach, farmach wiatrowych i fotowoltaicznych, dużych jednostkach rozproszonych (autoprodukcja przemysłowa) oraz instalacjach prosumenckich. Za dostarczanie energii elektrycznej do odbiorców odpowiadają Polskie Sieci Elektroenergetyczne (PSE) i spółki dystrybucyjne działające na poziomie średnich i niskich napięć. Realizacja głównego zadania PSE, jakim jest zapewnienie bezpiecznej, stabilnej i ciągłej pracy Krajowego Systemu Elektroenergetycznego (KSE), nierozłącznie związana jest ze stałą dostęp-

nością do źródeł generujących energię elektryczną, w tym w szczególności do Jednostek Wytwórczych Centralnie Dysponowanych (JWCD) przez operatora. Energia elektryczna w warunkach kryzysowych jest kluczowym zasobem decydującym o zachowaniu podstawowych funkcji bytowych i utrzymania produkcji, w tym również zaspokojenie potrzeb w zakresie obronności kraju.

4.3.1 Ocena krajowych zasobów wytwórczych

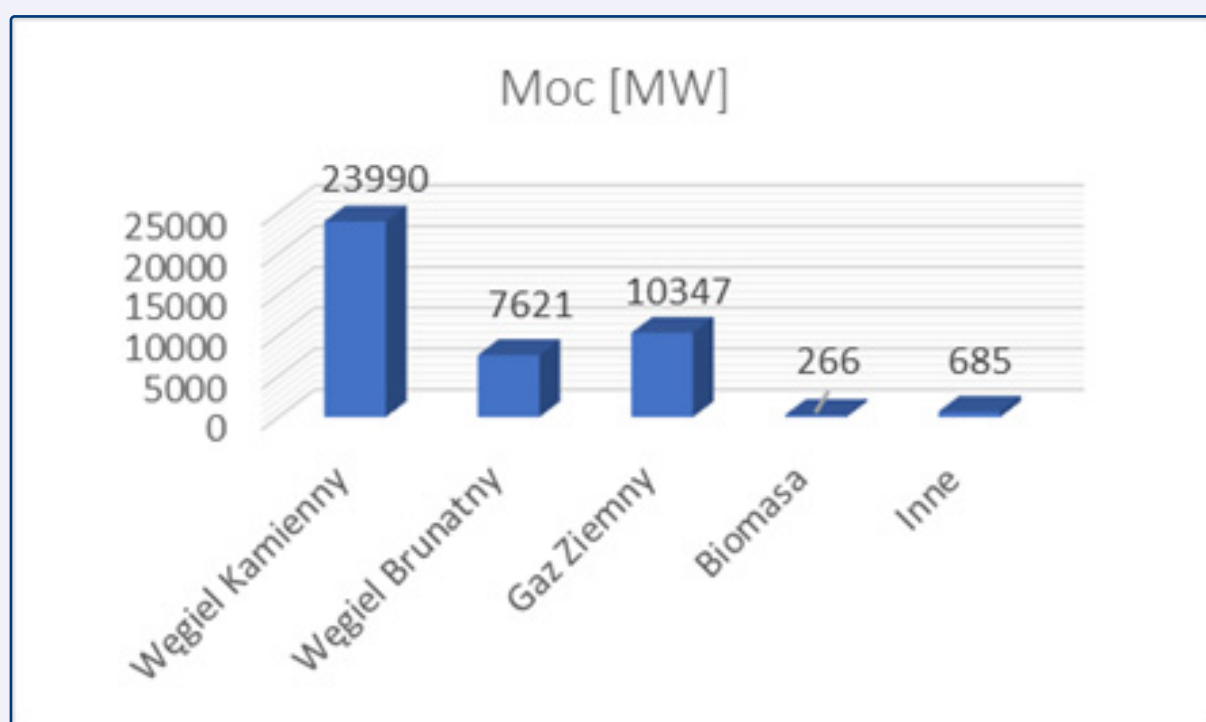
W związku z dynamicznym rozwojem rozproszonych źródeł odnawialnych wielkoskalowych i prosumenckich, głównie słonecznych i wiatrowych, których wielkość generacji uzależniona jest od pogody i pory dnia, coraz większym wyzwaniem dla operatora jest takie bilansowanie systemu, aby z jednej strony wykorzystać jak największą ilość energii ze

¹⁷⁴ Center for Strategic and International Studies, Building Supply Chain Resilience, 2022;

¹⁷⁵ U.S. Defense Business Board, Supply Chain Illumination in the Department of Defense, dz. cyt.

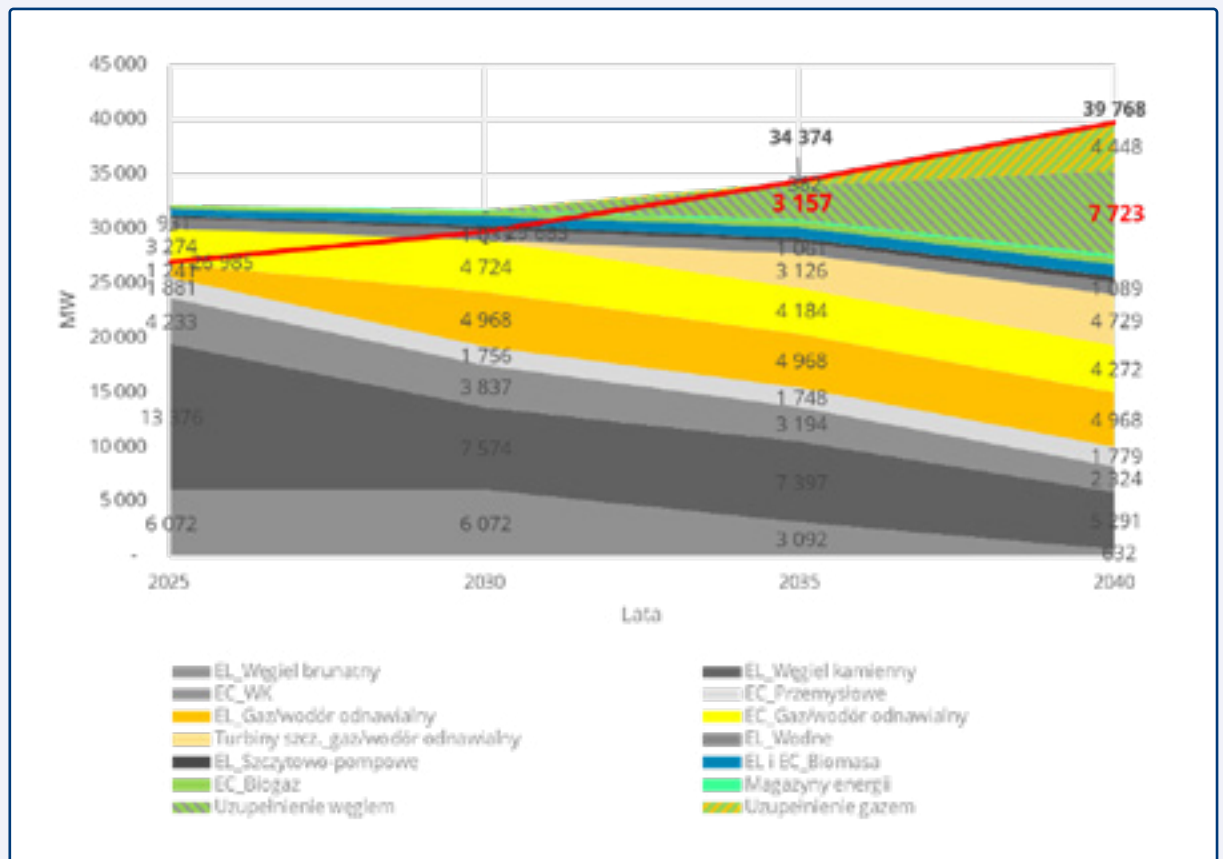
źródeł OZE, a z drugiej dysponować zawsze niezbędnymi mocami w jednostkach regulacyjnych (w polskich warunkach jest to węgiel i gaz). PSE prowadzą ciągłe analizy dostępności zdolności wytwórczych, które publikowane są cyklicznie w Krajowej Ocenie Wystarczalności Zasobów Wytwórczych (NRAA - obowiązuje dokument z listopada 2024 r.). W lutym PSE opublikowały projekt planu na lata 2027–2036, zakładający dynamiczny wzrost zapotrzebowania na moc systemu do 40 GW w 2040 r. oraz inwestycje w infrastrukturę sieciową umożliwiającą przesył energii z elektrowni jądrowej i morskich farm

wiatrowych na południe kraju. Moc zainstalowana w KSE na koniec 2025 r. przekroczyła 76 GW, ale w wielkości tej ok. 37 GW stanowią źródła pogodowo zależne, których dyspozycyjność jest ograniczona. Kluczowym problemem w zapewnieniu wystarczających zdolności wytwórczych jest przedłużenie żywotności lub zastąpienie mocy odstawianych elektrowni węglowych innymi jednostkami, w tym gazowymi. Obecnie elektrownie węglowe stanowią prawie 74 % mocy zainstalowanej, nie uwzględniając odnawialnych źródeł energii (Rys.4.4.).



Rys. 4.4. Zainstalowana moc obecnie eksploatowanych konwencjonalnych źródeł wytwórczych

Przeprowadzone analizy wskazują na ryzyko wystąpienia luki mocy sterowalnych w KSE, która może wynieść ok. 3,5 GW w 2035 r. i 12 GW w 2040 r. (przy założeniu pełnej dostępności pierwszej elektrowni jądrowej w 2040 r.). Na rysunku 4.5 przedstawiono prognozę luki mocy sterowalnych w KSE oraz propozycję jej wypełnienia poprzez przedłużenie żywotności elektrowni węglowych (7,7 GW) i budowę jednostek gazowych (4,5 GW). Czerwona linia wyznacza prognozowane zapotrzebowanie na moc. Pierwszy możliwy okres wystąpienia luki mocy sterowalnych przypada na lata 2032–2033.



Rys. 4.5. Prognoza luki mocy sterowalnych w KSE.

4.3.2 Analiza dostępności infrastruktury sieciowej (przesyłowej i dystrybucyjnej) i jej odporności na zakłócenia i uszkodzenia fizyczne, pod kątem niezawodności dostaw

Dynamika wyzwań stawianych elektroenergetyce sieciowej odsłania jej zasadniczą słabość, polegającą na korzystaniu z przestarzałej i znacznie zdekapitalizowanej infrastruktury, zaprojektowanej głównie z myślą o energetyce węglowej i przystosowanej do „jednokierunkowego przepływu energii”, tj. od źródła do odbiorcy. Wynikłe w tym czasie potrzeby przyłączeniowe oraz konieczność utworzenia efektywnej technicznie i ekonomicznie, elastycznej i zdecentralizowanej struktury sieci potwierdziły pilną konieczność jej ulepszenia. I choć w wielu dostępnych dokumentach strategicznych ten problem jest dostrzegany, to jednak nie można uznać stopnia rozwoju sieci elektroenergetycznych dystrybucyjnych w minionym okresie jako w pełni zadowalający. Z perspektywy lat minionej dekady wynika jednoznacznie, że tempo budowy nowej i modernizacja istniejącej infrastruktury sieciowej oraz utrzymanie użytkowanych aktywów sieciowych

wymagają zasobów finansowych. Stojąc przed wyzwaniem przyłączenia do sieci kolejnych kilkudziesięciu gigawatów generacji odnawialnej, poprawy parametrów jakości energii elektrycznej oraz zapewnienia bezpieczeństwa funkcjonowania sieci, powinniśmy dołożyć wszelkich starań, aby tworzyć realne możliwości finansowania zidentyfikowanych i na bieżąco urealnianych potrzeb sieciowych, m.in. związanych z zakładami strategicznymi z punktu widzenia obronności państwa.

W dobie podejmowania w grupach energetycznych m.in., słusznego w założeniach, zielonego kierunku transformacji polegającego na wejściu w posiadanie aktywów OZE, zachwiano konieczną do utrzymania w tego rodzaju działaniach autonomii i transparentności finansowania rozwoju tej energetyki, zważywszy na to, że uczestnikiem bilansowym grup byli także operatorzy sieci dystry-

bucyjnych, borykający się z ograniczaniem wydatków na rozwój i utrzymanie sieci elektroenergetycznych.

W minionym dziesięcioleciu znacząco obniżyła się również wartość wskaźnika odtworzenia majątku (WOM). W dokumentach uzupełniających i analitycznych powiązanych z PEP2040, takich jak Karta Efektywnej Transformacji Sieci Dystrybucyjnych (KET), przyjęto dla niego poziom 1,5%, podczas gdy w rzeczywistości osiągał on wartość poniżej 1%.

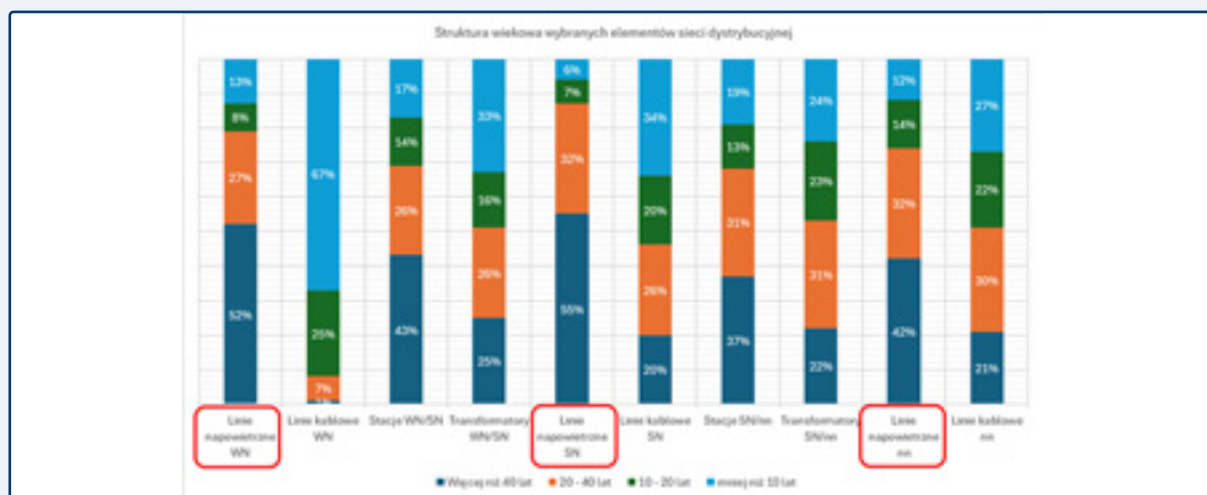
Kolejnym istotnym elementem procesu planistycznego jest zapewnienie odpowiedniego udziału wydatków na utrzymanie istniejącej infrastruktury sieciowej. W minionej dekadzie wydatki na ten obszar działalności operatorskiej – z wyłączeniem nakładów na rozwój i modernizację sieci związanych z przyłączaniem nowych odbiorców i źródeł – stanowiły jedynie kilka lub kilkanaście procent łącznych wydatków inwestycyjnych.

W perspektywie najbliższych lat nadal należy spodziewać się:

- dalszego wzrostu wytwarzania energii ze źródeł odnawialnych, zarówno w instalacjach prosumenckich, jak i w farmach fotowoltaicznych i wiatrowych; wzrastać będzie także udział energii z OZE w krajowym miksie energetycznym, co będzie stanowiło wyzwanie dla bieżącego bilansowania systemu elektroenergetycznego;
- gwałtownego wzrostu zapotrzebowania na magazyny energii (mikro i wielkoskalowe magazyny elektrochemiczne, elektrownie szczytowo-pompowe, magazynowanie energii w postaci skroplonych lub sprężonych gazów, magazynowanie energii z pośrednią konwersją do energii chemicznej wodoru i in.), co wynika z przyrostu w krajowym systemie elektroenergetycznym energii pochodzącej z generacji OZE;
- rozwoju indywidualnych i zorganizowanych form lokalnej samodzielności energetycznej (miejskiej, gminnej lub powiatowej), w tym klastrów i wspólnot energetycznych oraz inicjatyw indywidualnych inwestorów (przybliżenie generacji OZE do odbiorców, m.in. poprzez autokonsumpcję); inicjatywy te stanowią

szansę na tworzenie nowych obszarów aktywności dla lokalnych przedsiębiorców oraz na szybszy wzrost gospodarczy na terenach ich działania;

- okresowo występujących nadpodaży energii elektrycznej w systemie elektroenergetycznym, szczególnie w okresach wietrznych i dużego nasłonecznienia. To z kolei przełoży się na konieczność ograniczania produkcji tych źródeł celem zapewnienia stabilnej pracy KSE albo alternatywnie wypracowania metod w celu zagospodarowania ich nadmiarowej energii, konieczności rozwoju cyfrowych systemów zrównoważonego zarządzania energią w stopniu gwarantującym zarówno sprawne funkcjonowanie instalacji OZE i magazynów energii, jak i stabilizację potrzeb systemu elektroenergetycznego i utrzymanie standardów jakości obsługi klientów;
- wzrostu znaczenia systemu elektroenergetycznego (sieci elektroenergetycznych), czemu sprzyjać będą rosnące w dłuższej perspektywie zapotrzebowanie na zdolności przyłączeniowe i energię elektryczną oraz rozwój usług elastyczności; zidentyfikowane potrzeby wskazują na pilną konieczność dokapitalizowania sieci elektroenergetycznych zarówno w zakresie ich rozwoju, jak i utrzymania istniejących aktywów. Około 50% linii napowietrznych ma ponad 40 lat (rys. 4.6), natomiast na rysunku 4.7 przedstawiono prognozowany wzrost nakładów OSD na inwestycje konieczne – łącznie oraz w podziale na główne kategorie – w perspektywie do 2030 r.



Rys. 4.6. Struktura wiekowa wybranych elementów sieci dystrybucyjnej; stan na koniec 2025 r.

Źródło: Energetyka, Dystrybucja, Przesył. (Raport PTPIREE za rok 2025)

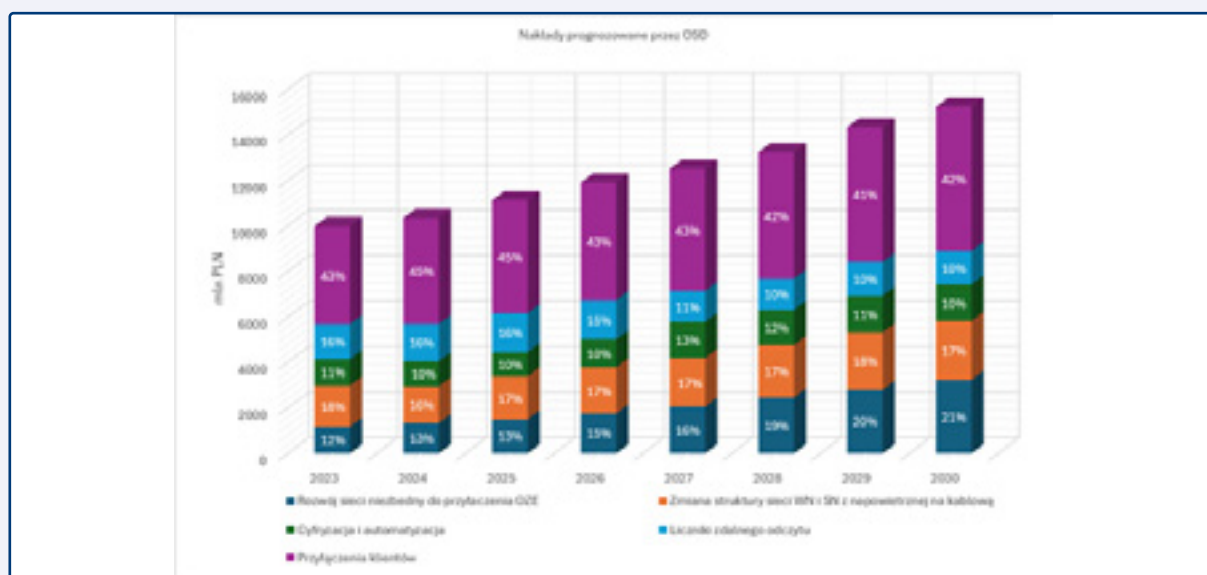
Rozwój i utrzymanie sieci są istotne z punktu widzenia przyłączania nowych zakładów o strategicznym znaczeniu do istniejącej in-

frastruktury elektroenergetycznej. Planowany wzrost nakładów w 2030 r. w stosunku do 2023 r. wynosi 50%.

a)

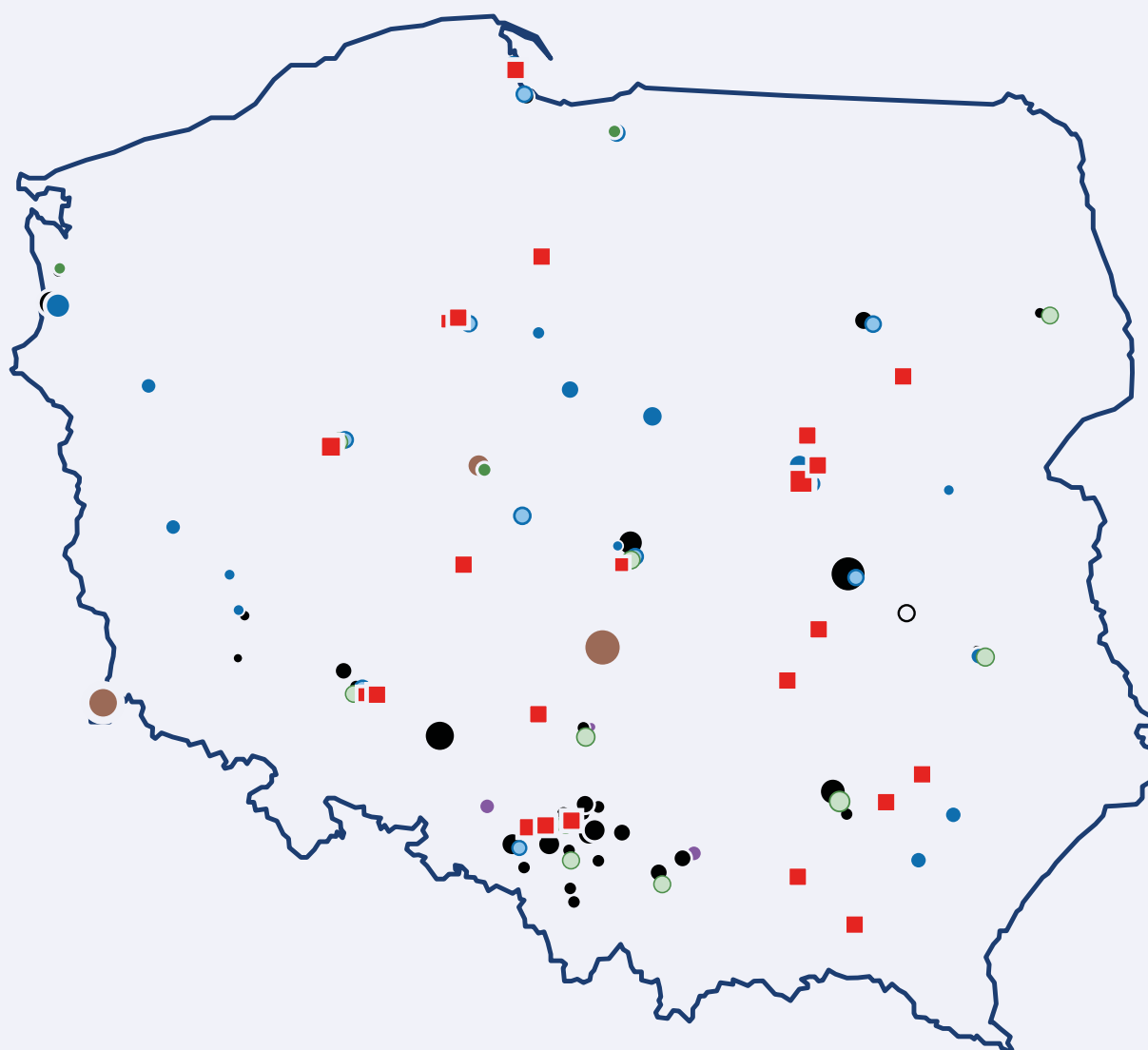


b)



Rys. 4.7. Nakłady prognozowane do realizacji przez OSD w kategorii inwestycje konieczne w ujęciu łącznym (a) oraz w podziale na główne kategorie inwestycyjne (b); perspektywa realizacji to 2030 r.

Źródło: Karta Efektywnej Transformacji Sieci Dystrybucyjnych Polskiej Elektroenergetyki, 2022 r.



OBIEKTY

■ Zakład zbrojeniowy PGZ

● Elektrownia istniejąca

○ W budowie lub planowana

RODZAJ PALIWA

● Węgiel kamienny

● Węgiel brunatny

● Gaz ziemny

● Biomasa

● Współspalanie biomasy

● Inne paliwa

Mapa 4.1. Lokalizacja zakładów zbrojeniowych PGZ i dostępnych konwencjonalnych źródeł energii w Polsce

4.3.3 Analiza zasobów w obszarze autoprodukcji, magazynowania i lokalnego bilansowania energii w zakładach przemysłu obronnego jako sposobów zwiększania odporności

Z uwagi na znaczący udział konwencjonalnych źródeł wytwórczych, analizowano położenie zakładów PGZ w odniesieniu do lokalizacji tych elektrowni. W obecnych uwarunkowaniach sąsiedztwo dużego, stabilnego źródła wytwórczego może sprzyjać zapewnieniu odpowiedniej pewności zasilania zakładów przemysłowych. Analiza wzajemnego rozmieszczenia zakładów PGZ i konwencjonalnych źródeł wytwórczych wskazuje jednak, że znaczenie tego czynnika będzie zmieniało się wraz z transformacją krajowego systemu elektroenergetycznego. Współczesne strategie rozwojowe zakładają bowiem zwiększanie udziału odnawialnych źródeł energii, rozwój technologii przemysłowego, wielkoskalowego magazynowania energii oraz funkcjonowanie źródeł OZE w strukturze coraz bardziej rozproszonej. Obecnie trwająca transformacja energetyki w znacznym stopniu przestawiła koncentrację procesu z produkcji energii (energię należy traktować jako produkt), na zarządzanie tym produktem, a co za tym idzie, w ciągu ostatnich kilku lat tworzenia nowego modelu krajowej energetyki. Na obecnym etapie solarne i wiatrowe źródła energii nie mogą efektywnie funkcjonować samodzielnie i wymagają elastycznego wsparcia ze strony innowacyjnych instalacji energetycznych, opartych na technologiach zdolnych zrównoważyć wahania w czasie produkcji energii generowanej przez te źródła. Tym samym, dostrzeżono także potrzebę systemowej integracji różnych technologicznie instalacji OZE i magazynowania energii, co wiąże się ze wzrostem poziomu skomplikowania zarządzania siecią elektroenergetyczną. Aby uniknąć chaosu w tworzeniu krajowej energetyki rozproszonej, w której generacja odnawialna, magazynowanie energii oraz spełnienie potrzeb bilansowych są objęte priorytetem, należy wdrażać rozwiązania oparte na lokalnych społecznościach energetycznych, takich jak klastry energii, spółdzielnie energetyczne i inne, prawem dopuszczone, autonomię i sa-

modzielności energetyczne. Skoordynowane prawnie, technicznie i ekonomicznie lokalnie sterowalne społeczności energetyczne mogą odegrać w kraju kluczową rolę zarówno w ograniczeniu kosztów energii i usługi dystrybucyjnej, jak i w poprawie ciągłości dostaw. Ma to bezpośredni związek z ukształtowaniem lokalnych rozpyłów energii, jednak nie należy utożsamiać tego z generalnym zapewnieniem bezpieczeństwa energetycznego kraju. Zatem, istotność i słuszność tworzenia lokalnych inicjatyw energetycznych, począwszy od budowy własnej infrastruktury energetycznej, operatywnego zarządzania tą infrastrukturą, po lokalne bilansowanie energii należy uznać za właściwy kierunek rozwoju nowoczesnej energetyki. Jest to jednak warunkowane utrzymaniem odpowiedniego zaplecza stabilizującego krajowy system elektroenergetyczny wobec nadal postępującego gigantycznego przyrostu mocy zainstalowanej pogodowo zależnej generacji odnawialnej. Brak właściwego zrównoważenia generacji OZE źródłami zdolnymi do stabilizacji pracy systemu elektroenergetycznego może prowadzić do zwiększenia ryzyka awarii systemowych, skrajnie nie wykluczając zdarzeń typu blackout.

4.3.4 Zidentyfikowane ryzyka i kierunki ich ograniczania

W polityce, a następnie w procedurach i przepisach dotyczących pewności i ciągłości zasilania zakładów o znaczeniu strategicznym, a także przy podejmowaniu długofalowych działań systemowych należy uwzględnić następujące ryzyka i podjąć próby ich minimalizacji poprzez zastosowanie zaleceń podanych poniżej. Zidentyfikowane najważniejsze ryzyka:

- w KSE w perspektywie 2035 i 2040 r. istnieje ryzyko wystąpienia luki mocy sterowalnych, a co za tym idzie dostępności energii elektrycznej w żądanej wielkości w każdym czasie, co oznacza ograniczenia w dostępie do energii elektrycznej i brak możliwości przyłączenia kolejnych odbiorców, może oznaczać czasowy brak dostępności części, elementów lub całych komponentów;

- znaczący przyrost produkcji energii z wiatru i słońca, który osiągnął 31,2% produkcji energii, co może wpłynąć na możliwości bilansowania w systemie;
 - spadek udziału węgla w krajowym miksie energetycznym do poziomu 52,8% produkcji energii, co zmniejszy bezpieczeństwo energetyczne kraju z uwagi na zmniejszenie wykorzystania surowca dostępnego lokalnie;
 - wzrost udziału gazu ziemnego w krajowym miksie energetycznym do poziomu 14,2 % produkcji energii, co w przypadku zaburzeń dostaw gazu z rejonów objętych konfliktami lokalnymi, zaburzeń importu LNG, przerw w dostawach rurociągami dedykowanymi (np. Baltic Pipe) wpłynie niekorzystnie na pewność zasilania;
 - gwałtowny wzrost nierynkowego redysponowania jednostek wytwórczych (ograniczenie produkcji OZE w roku ubiegłym o 1,4 TWh; a kolejne lata będą obciążone progresem tego negatywnego zjawiska), praca systemu w oparciu o źródła OZE nie jest możliwa z uwagi na brak możliwości stabilizacji jego pracy, dlatego też jednostki tego typu są odłączane, aby w to miejsce wprowadzić generację ze stabilnych, konwencjonalnych źródeł;
 - ograniczenie zdolności przyłączeniowych do sieci dystrybucyjnej;
 - postępujący proces dekapitalizacji majątku generacji węglowej (jednostki wytwórcze, w których następuje spalanie paliw kopalnych w wieku 40 lat i więcej stanowią blisko 60 % aktywów) oraz sieci przesyłowej i dystrybucyjnej;
 - lokalizacja dużych elektrowni, w pobliżu których lokowane były energochłonne zakłady, w tym obronne, w perspektywie 2040 r. przestanie być atutem i przekształci się w ryzyko dostępności do zasobów wytwórczych, wyłączenie elektrowni węglowych spowoduje, że pewność zasilania zostanie obniżona poprzez zmniejszenie dostępności źródeł, więc należy w to miejsce już obecnie przewidzieć źródła o mocy odpowiedniej dla zasilania zakładów o znaczeniu strategicznym;
 - niespójne regulacje prawne uniemożliwiają prowadzenie inwestycji zapewniających poprawność zasilania i odpowiedni poziom jego bezpieczeństwa;
 - brak wysokosprawnych i wielkoskalowych systemów magazynowania energii powoduje brak możliwości prowadzenia produkcji przy wykorzystaniu OZE jako jedyne źródła energii.
- Natomiast kierunkami ograniczania ryzyka mogą być:
- wykorzystanie paliw i zasobów dostępnych w kraju, w tym lokalnie (w krajowych uwarunkowaniach oznacza to wykorzystanie węgla, głównie kamiennego, w określonych ilościach), dla zapewnienia ciągłości produkcji kluczowych zakładów przemysłu obronnego;
 - zapewnienie zapasów surowców energetycznych, składowanych na terenie zakładów i odnawiane cyklicznie, w ramach działania Rządowej Agencji Rezerw Strategicznych, dla zapewnienia ciągłości produkcji kluczowych zakładów przemysłu obronnego;
 - lokowanie zakładów przemysłu obronnego w sąsiedztwie elektrowni energetyki zawodowej, należy tutaj zwrócić uwagę na konieczność analiz w kierunku lokowania mniejszych jednostek wytwórczych (np. SMR) w sąsiedztwie już istniejących zakładów o znaczeniu strategicznym;
 - modernizacja sieci przesyłowych w zakresie podnoszącym pewność zasilania zakładów o strategicznym znaczeniu;
 - zapewnienie odpowiedniego poziomu zapasów materiałów i części zamiennych infrastruktury energetycznej (w zakresie wytwarzania i dystrybucji) oraz odpowiednio przygotowanego personelu technicznego,
 - zabezpieczenie i przechowywanie elementów likwidowanych zakładów jako rezerwa na wypadek kryzysów i awarii (rekomendacja w kierunku likwidowanych węglowych jednostek wytwórczych - likwidowane bloki węglowych elektrowni, można zabezpieczyć i przechować, a w przypadku zwiększonych potrzeb ponownie wykorzystać),

- zmiana organizacji produkcji w zakładach, aby była ona maksymalizowana w okresach zwiększonej generacji energii ze źródeł odnawialnych;
- budowa mikrostruktur obejmujących małe źródła i magazyny energii, zdolnych również do pracy w trybie wyspowym (*off-grid*) w przypadku dłuższych przerw w zasilaniu zewnętrznym; rozwiązania te powinny zapewniać podstawowe funkcje bytowe i zdolność przywrócenia produkcji niezależnie od zasilania z KSE i dużych źródeł zewnętrznych (autoprodukcja);
- rozwój innych form magazynowania energii; obecnie dostępne technologie nie zapewniają zasobów wystarczających do utrzymania ciągłości produkcji w przypadku braku bieżącej generacji, a sprawność magazynowania i dostępne pojemności nie gwarantują wystarczającego poziomu bezpieczeństwa przy zasilaniu zakładu wyłącznie ze źródeł pogodowo zależnych;
- poszukiwanie i rozwój nowych technologii wytwarzania energii (np. z wykorzystaniem wodoru);
- opracowanie spójnych zasad dotyczących zapewnienia odpowiedniego poziomu odporności układów zasilania zakładów zbrojeniowych. Zasady te powinny obowiązywać dla nowopowstających zakładów, a zakłady funkcjonujące powinny zostać zobligowane do jak najszybszego dostosowania się do zaleceń. Procedury przyłączenia zakładów o znaczeniu strategicznym powinny zostać objęte dedykowaną procedurą umożliwiającą możliwie szybkie przyłączenie do sieci dystrybucyjnej lub zwiększenie dostępnej mocy, przy zwiększaniu mocy produkcyjnych. Wymaga to współdziałania operatorów systemu z podmiotami przemysłu zbrojeniowego w planowaniu rozbudowy infrastruktury energetycznej i dostępnych mocy.

4.4. Infrastruktura informatyczna

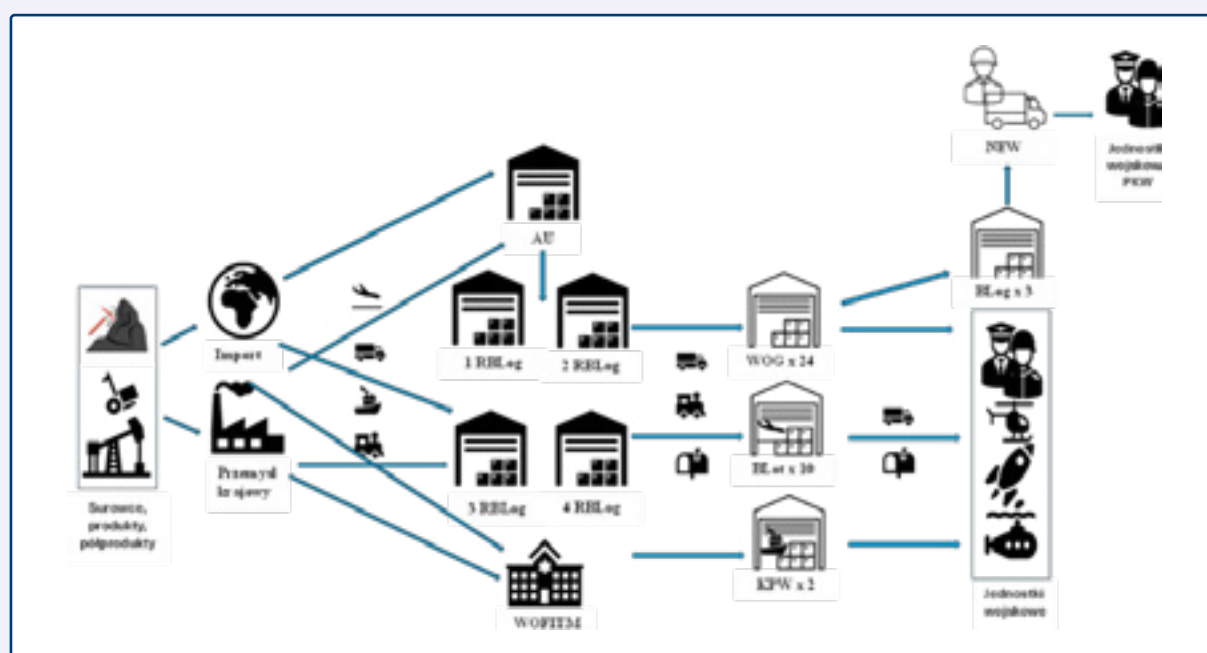
Ocena rozwiązań technicznych i technologicznych w zakresie przepływu informacji na potrzeby budowy widoczności (*visibility*) w łańcuchu dostaw jest złożona i wielowymiarowa, gdyż polega na sprawdzeniu, w jakim stopniu konkretne systemy i technologie zapewniają wiarygodny, spójny i terminowy obraz zasobów, procesów i ryzyk. W przedsiębiorstwach cywilnych i w logistyce Sił Zbrojnych RP zasada jest podobna, natomiast różne są priorytety, np. bezpieczeństwo informacji czy stosowana w wojsku interoperacyjność sojusznicza. Analizowany łańcuch dostaw dla SZ RP obejmuje część cywilną i wojskową, które tworzą jedną całość, lecz nie są powiązane współdziałającymi, jednorodnymi systemami umożliwiającymi zapewnienie widoczności łańcucha dostaw w całym jego zakresie. Charakterystyczną cechą wojskowego łańcucha dostaw jest jego struktura wielopoziomowa, odpowiadająca różnym szczeblom dowodzenia i kierowania

działaniami logistycznymi. Na poziomie strategicznym prowadzi się planowanie i zarządzanie zasobami w wymiarze narodowym oraz w ramach struktur sojuszniczych. Poziom operacyjny odpowiada za organizację i koordynację przepływu środków materiałowo-technicznych pomiędzy oddziałami gospodarczymi (OG) a związkami taktycznymi. Na najniższym szczeblu funkcjonuje natomiast poziom taktyczny, bezpośrednio realizujący dostawy do żołnierzy znajdujących się w rejonach działań operacyjnych lub szkoleniowych. Poziom ten odpowiada za terminowe i precyzyjne dostarczenie środków niezbędnych do wykonania zadania. Model współpracy między uczestnikami wojskowego i cywilnego systemu logistycznego powinien uwzględniać kluczowe zależności oraz zapewniać ciągłość i bezpieczeństwo dostaw – zarówno w warunkach pokojowych, jak i operacyjnych, szczególnie w sytuacjach o podwyższonym poziomie ryzyka¹⁷⁶. Oma-

¹⁷⁶ D. Nagrabski, D. Żuchowski, Bezpieczeństwo wojskowego łańcucha dostaw w terytorialnym systemie zabezpieczenia logistycznego, Transformacja wojskowych łańcuchów dostaw – teoria i praktyka cz. 2, Warszawa 2026 r.

wiana współpraca cywilno-wojskowa ma znaczenie strategiczne, gdyż jej prawidłowe funkcjonowanie zapewnia sprawny przepływ aktualnej informacji logistycznej o posiadanych lub możliwych do pozyskania zasobach. Zgodnie z literaturą przedmiotu¹⁷⁷ informacja jest czynnikiem integrującym i warunkującym prawidłowe funkcjonowanie łańcucha dostaw. Optymalny obieg informacji, uwzględniający specyfikę łańcucha dostaw sił zbrojnych, mogą zapewnić jedynie wdrożone i kompatybilne systemy informacyjne. System informacyjny jest przy tym rozumiany jako organizacja i sposób posługiwania się informacją, obejmujące jej wytwarza-

nie, zapisywanie, odczytywanie, przechowywanie, przetwarzanie i przesyłanie, a także jako zbiór technik i technologii wykorzystywanych w jego organizacji i wspierających jego funkcjonowanie.¹⁷⁸ Ważnym aspektem analizy omawianego obszaru powinien być zatem obieg informacji uwzględniający wielowymiarowość i specyfikę wojskowego łańcucha dostaw, gdyż funkcjonuje on w różnych konfiguracjach oraz uwarunkowaniach operacyjnych i ekonomicznych charakterystycznych dla określonego środowiska¹⁷⁹. Złożoność analizowanego łańcucha dostaw przedstawiono na poniższym rysunku.



Rysunek 4.8. Łańcuchy dostaw do jednostek i instytucji wojskowych

Łańcuch dostaw, zgodnie z rysunkiem 4.8, obejmuje przepływ produktów od dostawców surowców, produktów, półproduktów i części zamiennych, przez kanały importowe i podmioty krajowe (w tym przedsiębiorstwa przemysłu obronnego oraz cywilnych dostawców), do Agencji Uzbrojenia, regionalnych baz logistycznych i Wojskowego Ośrodka Farmacji i Techniki Medycznej. Podmioty te integrują dostawy z obu tych źródeł, realizując procedury przetargowe i zakupy mające zagwarantować ciągłość wsparcia oraz zabezpieczenia logistycznego jedno-

stek wojskowych na terytorium kraju. Realizacja zadań poza granicami kraju odbywa się za pośrednictwem brygad logistycznych, które są kluczowym ogniwem systemu zabezpieczenia Polskich Kontyngentów Wojskowych (PKW). Brygady logistyczne prowadzą gospodarkę materiałową dla PKW we wszystkich działach zaopatrzenia i wydzielają Narodowy Element Wsparcia (NEW/NSE), działający w rejonie operacji jako „przedłużenie” krajowego systemu zaopatrzenia.

177 R. Fuchner, Zarządzanie łańcuchem dostaw, Wyższa Szkoła Logistyki, Poznań 2007

178 Tamże, str. 127

179 D. Grala, Bezpieczeństwo wojskowych łańcuchów dostaw, ASzWoj, Warszawa 2024, str.129

Jak wspomniano wcześniej, w omawianym łańcuchu dostaw można wyodrębnić część cywilną i część wojskową. Każda z nich wykorzystuje specjalistyczne rozwiązania technologiczne umożliwiające sprawny przepływ informacji, jednak rozwiązania te funkcjonują wyłącznie w obrębie części cywilnej albo wojskowej i nie są wzajemnie kompatybilne. Upoważnia to do postawienia tezy, że wąskim gardłem informacyjnym w łańcuchu dostaw dla Sił Zbrojnych RP jest styk sektora cywilnego i logistyki wojskowej.

Istotą omawianego łańcucha dostaw jest zatem widoczność przepływu informacji w całym jego zakresie. Widoczność oznacza zdolność do uzyskania aktualnej i wiarygodnej informacji o położeniu, stanie, dostępności i historii zasobów (materiałów, uzbrojenia i usług) w całym łańcuchu dostaw, a nie tylko w pojedynczej organizacji. W praktyce oznacza to integrację danych z wielu źródeł (systemów magazynowych, transportowych i produkcyjnych, czujników IoT oraz wojskowych systemów ewidencyjnych) w jeden spójny obraz, co wspiera planowanie, prognozowanie i reagowanie na zakłócenia, a docelowo umożliwia automatyzację i zwiększanie autonomii procesów logistycznych. W SZ RP widoczność jest dodatkowo warunkiem utrzymania gotowości bojowej, gdyż umożliwia powiązanie informacji o zasobach logistycznych ze stanem sił i środków w operacji¹⁸⁰. Widoczność łańcucha dostaw definiuje się najczęściej jako zdolność do pozyskiwania aktualnych, dokładnych i kompletnych informacji o stanie, lokalizacji i historii przepływu zasobów w całym łańcuchu, a nie tylko w jednej organizacji. W literaturze podkreśla się, że widoczność obejmuje zarówno fizyczny przepływ dóbr, jak i przepływ informacji o zamówieniach, zapasach, zdolnościach produkcyjnych oraz zdarzeniach zakłócających, takich jak opóźnienia i awarie, a także o związanych z nimi ryzykach. W ujęciu systemowym widoczność tworzy się dzięki sprzężeniu zwrotnemu między zdarzeniami fizycznymi a warstwą informacyjną, co wymaga standaryzacji danych, automatyzacji pozyskiwania informacji (AIDC, IoT) oraz integracji systemów informatycznych.

Przy ocenie rozwiązań techniczno-technologicznych w zakresie przepływu informacji należy przyjąć zestaw kryteriów, które można stosować zarówno w sektorze cywilnym, jak i wojskowym. Typowy zestaw powinien obejmować między innymi:

- zakres widoczności, czyli liczbę ogniw łańcucha objętych systemem (dostawców, poddostawców, transport, magazyny i użytkownika końcowego, a w wojsku – poszczególne szczeble dowodzenia i rodzaje wojsk);
 - jakość danych: dokładność, kompletność, aktualność oraz jednoznaczność identyfikację zasobów (np. z wykorzystaniem kodów EPC/RFID);
 - terminowość informacji: opóźnienie między zdarzeniem fizycznym a jego odzwierciedleniem w systemie (w czasie rzeczywistym lub zbliżonym do rzeczywistego);
 - integrację systemową: zdolność łączenia różnych systemów cywilnych (WMS, TMS, ERP) i wojskowych oraz wymiany informacji między nimi;
 - bezpieczeństwo i poufność: szyfrowanie, kontrolę dostępu i odporność na cyberatak, a w wojsku także zgodność z wymaganiami bezpieczeństwa narodowego i sojuszniczego;
 - skalowalność i elastyczność, a więc możliwość obejmowania systemem nowych obszarów operacji, teatrów działań i partnerów oraz jego szybkiej rekonfiguracji;
 - wsparcie decyzji: dostępność narzędzi analitycznych, takich jak analityka biznesowa (BI), sztuczna inteligencja (AI) i narzędzia prognostyczne, przekształcających dane w rekomendacje dla planistów i dowódców.
- Uwzględniając powyższe, rozwiązania techniczne i technologiczne można pogrupować w kilka kategorii, zarówno w logistyce cywilnej, jak i wojskowej.
- identyfikacja i śledzenie: kody kreskowe, RFID, EPC, inteligentne etykiety, GPS oraz rozwiązania IoT stosowane w kontenerach, pojazdach i sprzęcie;

¹⁸⁰ Z. Malinowski, *The Impact of New Technologies on Supply Chain Management in the Armed Forces*, „Journal of Science of the Military Academy of Land Forces” 2017, vol. 49, nr 4(186).

- sensory i telematyka: czujniki temperatury, wilgotności i wstrząsów oraz urządzenia ELD w pojazdach, umożliwiające monitorowanie warunków transportu i eksploatacji;
- systemy ewidencyjne i wykonawcze: WMS, TMS, systemy SCM, platformy zapewniające widoczność całego łańcucha dostaw oraz wojskowe systemy oparte na standardach danych i jednolitej ewidencji;
- integracja danych: platformy integracyjne, hurtownie danych i oprogramowanie pośredniczące łączące rozproszone systemy, także w rozproszonych, nieliniowych wojskowych sieciach zaopatrzenia;
- rozwiązania zaawansowane: analityka predykcyjna, narzędzia sztucznej inteligencji do prognozowania zakłóceń oraz technologia łańcucha bloków (blockchain) służąca do śledzenia pochodzenia i autentyczności dóbr, szczególnie w łańcuchach o krytycznym znaczeniu.

Należy jednak podkreślić, że choć technologie są w dużej mierze wspólne, sposób ich oceny w sektorze cywilnym i wojskowym różni się ze względu na odmienne cele i uwarunkowania. W cywilnym łańcuchu dostaw nacisk kładzie się na efektywność kosztową, obsługę klienta, skrócenie czasu realizacji oraz elastyczne reagowanie na potrzeby rynku. W wojskowym łańcuchu dostaw priorytetem jest natomiast gotowość bojowa, a więc pewność dostaw w warunkach zakłóceń i działań przeciwnika, interoperacyjność sojuszników oraz bezpieczeństwo informacji.

Podsumowując, sektor cywilny funkcjonuje głównie w środowisku regulowanym i stabilnym, natomiast logistyka wojskowa musi uwzględniać degradację infrastruktury, brak łączności, zagrożenia cybernetyczne oraz konieczność działania w ramach koalicji. W efekcie w środowisku wojskowym większy nacisk kładzie się na kryteria bezpieczeństwa, odporności i interoperacyjności, nawet kosztem efektywności ekonomicznej rozwiązań.

Warunki integracji przepływu informacji w łańcuchu dostaw

Zapewnienie kompatybilnego przepływu informacji w całym łańcuchu – od dostawcy surowców, przez logistykę cywilną, aż po wydanie materiału w jednostce wojskowej na podstawie złożonego zapotrzebowania – wymaga równoczesnego ustanowienia rozwiązań w trzech warstwach, uwzględniających hybrydowość informacji na poszczególnych poziomach łańcucha dostaw. Przykładowo RFID może stanowić tanią „warstwę masową” identyfikacji w punktach, a pozostałe systemy – „warstwę ciągłej widoczności” dla wybranych klas zasobów krytycznych. **Warstwy te obejmują przede wszystkim wspólne standardy danych, zintegrowane systemy informatyczne oraz spójne reguły organizacyjno-prawne.** W praktyce oznacza to, że wojsko i podmioty cywilne muszą posługiwać się tym samym „językiem danych”, korzystać z architektury umożliwiającej bezstratne przenoszenie danych między systemami oraz stosować procedury zapewniające kompletność, terminowość i poprawność informacji od momentu zakupu surowca aż po przyjęcie go do ewidencji w zaopatrywanym pododdziale.

W warstwie danych punktem wyjścia jest ustanowienie jednolitego sposobu identyfikacji tego, co przemieszcza się w łańcuchu, a więc produktów, jednostek logistycznych i lokalizacji. Po stronie cywilnej naturalną bazą są standardy GSI (GTIN, SSCC, GLN) oraz oparte na nich nośniki, takie jak kody kreskowe GSI-128, DataMatrix i EPC/RFID, które pozwalają jednoznacznie wskazać, „jaki to produkt, jaka to jednostka ładunkowa oraz skąd i dokąd się przemieszcza”. Po stronie wojskowej ten „język” musi zostać powiązany z Jednolitym Indekssem Materiałowym (JIM) i Zintegrowanym Wieloszczeblowym Systemem Informatycznym Resortu Obrony Narodowej (ZWSI RON), tak aby każde cywilne oznaczenie można było automatycznie przyporządkować do pozycji w wojskowym katalogu zaopatrzenia, bez ręcznego przepisywania danych i ich uznaniowej interpretacji. Wymaga to opracowania powiązań między słownikami GSI a wojskowym Jednolitym Indekssem Materiałowym, a następnie konsekwentnego stosowania ich w dokumentach zakupu i dostawy oraz podczas przyjmowania do ewidencji logistyki wojskowej.

Kolejnym krokiem jest uporządkowanie informacji o zdarzeniach w łańcuchu dostaw, a więc nie tylko o tym, „co”, ale także „kiedy, gdzie, w jakiej ilości i dlaczego się wydarzyło”. Po stronie cywilnej tę rolę pełni standard EPCIS, który pozwala partnerom łańcucha wymieniać informacje o zdarzeniach typu „przyjęto do magazynu”, „wysłano”, „skonfekcjonowano” czy „zutilizowano” w sposób zrozumiały dla wszystkich uczestników, bez względu na to, jaki system WMS lub ERP stosują. Po stronie wojskowej taki sam paradygmat powinien zostać wdrożony w zintegrowanym systemie resortowym ZWSI RON, tak aby każde zdarzenie logistyczne wygenerowane w porcie cywilnym, centrum dystrybucji operatora czy bazie wojskowej było reprezentowane przez taki sam, ustandaryzowany rekord zdarzenia i bezpośrednio trafiało do wojskowych systemów planowania i ewidencji, umożliwiając automatyczne budowanie spójnego obrazu zapasów i przepływów w czasie zbliżonym do rzeczywistego. Na tej podstawie można budować architekturę systemową, która łączy cywilnych i wojskowych uczestników łańcucha w jedną sieć informacyjną, zamiast tworzyć „zestaw izolowanych wysp”. Po stronie przemysłu i operatorów logistycznych oznacza to korzystanie z systemów klasy ERP, WMS i TMS oraz platform transportowych, które mogą generować standardowe komunikaty EDI lub API oparte na GS1/eCom i EPCIS, a tym samym automatycznie informować o przyjęciu, wysyłce i statusie przesyłki. Po stronie wojskowej konieczne jest wyposażenie zintegrowanego systemu resortowego w bramy komunikacyjne między siecią jawną a niejawną. Bramy te powinny odbierać i walidować takie komunikaty, przekazywać je do odpowiednich modułów Zintegrowanego Wieloszczęblowego Systemu Informatycznego Resortu Obrony Narodowej, a jednocześnie generować analogiczne komunikaty kierowane do partnerów cywilnych i sojuszników. Bez tego łączność między środowiskiem cywilnym a wojskowym sprowadza się do wymiany dokumentów wymagających ponownego wprowadzenia do systemów, co z natury powoduje opóźnienia.

Ostatnim, równie ważnym elementem jest sfera organizacyjna i kompetencyjna, która decyduje o tym, czy nawet najlepiej zaprojektowany strumień danych będzie wykorzystywany w praktyce. Zarówno w wojsku, jak i w logistyce cywilnej należy zmienić sposób pracy z informacją. Trzeba odejść od ręcznego raportowania i „przepisywania” danych na rzecz automatycznego pozyskiwania ich z urządzeń AIDC/IoT oraz standardowych komunikatów systemowych, a także przenieść ciężar pracy logistyków z wypełniania dokumentów na analizę wskaźników i podejmowanie właściwych decyzji logistycznych. Wymaga to przede wszystkim zastosowania narzędzia umożliwiającego komunikację między systemami cywilnymi funkcjonującymi w sieciach jawnych a wojskowymi systemami logistycznymi działającymi w sieciach niejawnych. Dzięki temu każde złożone zapotrzebowanie nie będzie jedynie dokumentem logistycznym, lecz początkiem śledzonego cyfrowo „wątku” w systemie – od dostawcy surowca aż po magazyn logistyczny lub żołnierza jako końcowego odbiorcę. Dopiero wówczas kompatybilny przepływ informacji stanie się trwałą cechą całego łańcucha dostaw, a nie efektem pojedynczych, punktowych inicjatyw informatycznych. Szybka reakcja na zmieniające się potrzeby stanowi bowiem w XXI wieku atut strategiczny, możliwy do wykorzystania dzięki zintegrowanym systemom informacyjnym, które są podstawą rozbudowanych systemów logistycznych i łańcuchów dostaw.¹⁸¹

181 A. Szymonik, I. Nowak Współczesna logistyka, Dyfin S.A. Warszawa 2008 r. str.186

4.5. Wnioski i rekomendacje

Analiza infrastruktury transportowej, logistycznej, elektroenergetycznej i informatycznej wskazuje, że ciągłość produkcji, dostaw oraz utrzymania sprawności sprzętu wojskowego i środków bojowych nie może być zapewniana oddzielnie przez poszczególne sektory. Przedmiotem zarządzania powinien być pełny przepływ obronno-przemysłowy – od pozyskania materiałów i komponentów, przez produkcję, magazynowanie i transport, po dostarczenie wyrobu odbiorcy oraz utrzymanie lub odtworzenie jego sprawności. Zdolność ta musi być zachowana również po wystąpieniu zakłócenia jednej lub kilku współzależnych warstw infrastruktury.

4.5.1. Wnioski

- 1. Ciągłość dostaw jest właściwością całego systemu, a nie pojedynczego rodzaju infrastruktury.** Przejezdna droga, dostępna linia kolejowa, czynne lotnisko, wolna powierzchnia magazynowa, odpowiednia moc przyłączeniowa lub działający system informatyczny nie gwarantują wykonania zadania, jeżeli zawiedzie inny element przepływu. O jego odporności decydują łącznie: infrastruktura, operatorzy, tabor, zapasy, dokumentacja, personel, energia, paliwo, systemy sterowania, dane, procedury bezpieczeństwa i gotowość odbiorcy. Zakłócenie jednego z tych elementów może wywołać skutki kaskadowe i zatrzymać cały przepływ.
- 2. Nominalny potencjał infrastrukturalny nie jest równoznaczny z gotowością operacyjną.** Istnienie trasy, magazynu, terminala, operatora, przyłącza energetycznego lub systemu informatycznego nie przesądza o możliwości ich wykorzystania na potrzeby obronne. Zasób cywilny staje się zdolnością obronną dopiero po zweryfikowaniu jego parametrów, określeniu warunków dostępu i czasu aktywacji, zabezpieczeniu kontraktowym i informacyjnym oraz praktycznym sprawdzeniu. Sama obecność zasobu na rynku nie gwarantuje jego dostępności w warunkach wzrostu zapotrzebowania, konkurencji z przepływami cywilnymi lub zakłócenia infrastruktury.
- 3. Największe ryzyka koncentrują się na styku systemów, obiektów i odpowiedzialności.** Dotyczy to przede wszystkim pierwszej i ostatniej mili, obiektów inżynierskich, terminali, bocznicy, ramp, przeładunków, przekazywania odpowiedzialności między operatorami, przyłączy energetycznych zakładów oraz wymiany informacji między przemysłem, operatorami cywilnymi i logistyką wojskową. Ograniczenie pojedynczego mostu, odcinka jednotorowego, terminala, przyłącza, systemu danych lub procedury może uniemożliwić wykorzystanie pozostałej, sprawnej części infrastruktury. Szczególnie niebezpieczne są pojedyncze punkty awarii, dla których nie przygotowano wykonanego wariantu zastępczego.
- 4. Rozbudowa produkcji bez równoległego zabezpieczenia logistyki i obsługi technicznej może jedynie przenieść wąskie gardło poza halę produkcyjną.** Wzrost mocy produkcyjnych wymaga równoczesnego zapewnienia dostaw materiałów, widoczności poddostawców niższych poziomów, zapasów, magazynowania, kompletacji, kontroli jakości, dokumentacji, opakowań, operatorów i zdolności wysyłkowych. Analogiczne znaczenie ma zabezpieczenie obsługi technicznej, napraw i remontów. Brak pojedynczego komponentu, części zamiennej, narzędzia, dokumentacji, oprogramowania diagnostycznego, aktualizacji lub kompetencji serwisowych może zatrzymać produkcję albo wyłączyć sprzęt z użytkowania, mimo że formalnie pozostaje on w zasobie.
- 5. Energia elektryczna i informacja są zdolnościami operacyjnymi równorzędnymi transportowi i logistyce.** Wysoka moc w krajowym systemie nie oznacza dostępności wymaganej mocy w każdym czasie i miejscu. O odporności zakładu decydują także stan sieci, możliwości przyłączeniowe, niezależność wariantów zasilania, lokalna autonomia oraz zdolność bezpiecznego zatrzymania i ponownego uruchomienia produkcji. Podobnie cyfryzacja nie zwiększa

odporności, jeżeli utrata pojedynczego systemu, łącza, usługi zewnętrznej lub źródła danych może zatrzymać przepływ. Systemy muszą zachowywać minimalną funkcjonalność w trybie ograniczonym i umożliwiać kontrolowane odtworzenie. Jednym z kluczowych ograniczeń pozostaje brak pełnej interoperacyjności między systemami przemysłowymi, cywilnymi i wojskowymi oraz wspólnego sposobu identyfikacji zasobów i wymiany informacji w całym łańcuchu dostaw.

- 6. Odporność powinna być potwierdzana przez wykonanie zadania po zakłóceniu, a nie przez deklarowane parametry zasobów.** Podstawowymi miernikami powinny być m.in.: minimalny poziom produkcji lub dostaw możliwy do utrzymania, całkowity czas dostawy, czas autonomicznego działania, czas przełączenia na wariant zastępczy, czas odtworzenia funkcji oraz liczba rzeczywiście wykonalnych wariantów alternatywnych. Ocena powinna obejmować cały proces – od dostępności zasobu, przez kompletację, kontrolę jakości, dokumentację, przydzielenie operatora, transport i przeładunek, po przekazanie odbiorcy albo przywrócenie sprawności sprzętu.

4.5.2. Rekomendacje

- 1. Ustanowić międzysektorowy system zarządzania odpornością krytycznych przepływów obronno-przemysłowych.** MON powinno zainicjować stały mechanizm współpracy z resortami właściwymi do spraw transportu, energii i cyfryzacji, Rządowym Centrum Bezpieczeństwa, zarządcami infrastruktury, operatorami systemów elektroenergetycznych, przemysłem oraz operatorami logistycznymi. Dla każdego krytycznego programu lub grupy produktów należy wskazać właściciela przepływu odpowiedzialnego za jego koordynację od źródła zaopatrzenia do odbiorcy, a w przypadku obsługi technicznej – do przywrócenia sprawności sprzętu. Właściciel przepływu nie powinien przejmować ustawowych zadań poszczególnych podmiotów, lecz koordynować całość, monitorować ryzyka, uruchamiać warianty zastępcze i prowadzić eskalację problemów. Pierwszym rezultatem powinny być: lista przepływów krytycznych,

matryca odpowiedzialności, wspólny rejestr ryzyk oraz procedura eskalacji.

- 2. Utworzyć bezpieczną, rozproszoną architekturę informacji o zdolnościach, zależnościach i pojedynczych punktach awarii.** Powinna ona integrować trzy grupy danych: parametry infrastruktury transportowej, zdolności logistyczne podwójnego zastosowania oraz zależności energetyczne i informatyczne krytycznych obiektów. Dla każdej informacji należy określić jej źródło, właściciela, datę weryfikacji, poziom pewności, cykl aktualizacji i zasady dostępu. Warstwa jawna powinna zawierać kryteria oceny i wyniki zagregowane, natomiast szczegółowe trasy, parametry obiektów, lokalizacje zapasów i podatności powinny pozostać w kontrolowanej warstwie operacyjnej. Krajowe modele ruchu i inne narzędzia analityczne powinny korzystać ze wspólnej warstwy referencyjnej, bez zastępowania ich jednym monolitycznym systemem.
- 3. Utworzyć wspólne krajowe środowisko modelowania przepływów obronno-przemysłowych.** Należy zintegrować istniejące krajowe modele ruchu i narzędzia analityczne rozwijane przez CUPT oraz Port Polska w jedno wspólne środowisko planistyczne, bez likwidowania ich odrębnych funkcji. Celem nie powinno być budowanie jednego monolitycznego modelu, lecz zapewnienie wspólnych standardów danych, scenariuszy, słowników pojęć, zasad walidacji wyników oraz możliwości porównywania analiz wykonywanych w różnych modelach. Środowisko to powinno umożliwiać ocenę przepływów obronno-przemysłowych w warunkach normalnych i zakłóconych, w tym wzrostu produkcji, pilnych dostaw, zamknięcia odcinków, przeciążenia terminali, braku dostępności bocznic, ramp lub lotnisk cargo oraz konieczności przekierowania dostawy na inną trasę albo gałąź transportu. W warstwie jawnej należy prezentować wyłącznie założenia, typy scenariuszy, klasy ryzyka i wyniki zagregowane. Dane o rzeczywistych trasach, lokalizacjach, przepustowości, wrażliwych obiektach i wariantach operacyjnych powinny pozostać w warstwie dostępnej wyłącznie dla uprawnionych instytucji.

4. **Priorytetowo wzmacniać obiekty i odcinki, które decydują o przewozie ciężkiego sprzętu i ostatniej mili.** Szczególne znaczenie mają mosty, wiadukty, tunele, przeprawy, drogi dojazdowe do zakładów i magazynów, przejazdy przez aglomeracje, odcinki o dużym natężeniu ruchu oraz trasy prowadzące do terminali, bocznic i lotnisk cargo. Modernizacja powinna uwzględniać wymagania przewozów ponadnormatywnych, nośność, skrajnię, geometrię przejazdu, naciski osi i klasy obciążenia wojskowego. Należy również rozwijać systemy monitoringu stanu technicznego obiektów inżynierskich.
5. **Przygotować i okresowo weryfikować warianty alternatywne dla głównych korytarzy transportowych.** Szczególną uwagę należy poświęcić odcinkom o dużej koncentracji ruchu, obszarom o niskiej gęstości sieci wysokiej klasy, przejściom granicznym, północno-wschodniej Polsce oraz relacjom prowadzącym do zakładów przemysłu obronnego. Wariant alternatywny powinien być nie tylko narysowany na mapie, ale sprawdzony pod kątem parametrów technicznych, dostępności operatora, terminala, taboru i czasu przełączenia.
6. **Zabezpieczyć systemy sterowania ruchem, dane, cyberodporność, energię i paliwa jako warunki utrzymania przepływów.** Należy kontynuować modernizację systemów sterowania ruchem kolejowym, wdrażanie ERTMS/ETCS, rozwój inteligentnych systemów transportowych (w dalszej perspektywie bliźniaki cyberfizyczne), zabezpieczenie systemów lotniczych oraz budowę rezerwowych trybów pracy centrów sterowania. Równolegle należy wdrożyć segmentację systemów, architekturę Zero Trust, procedury manualne i ćwiczenia pracy w trybie zdegradowanym. Celem jest utrzymanie podstawowej koordynacji przewozów także po awarii informatycznej, cyberataku lub utracie części systemów cyfrowych.
7. **Wzmocnić odporność infrastruktury transportowej na zdarzenia pogodowe, klimatyczne, energetyczne i paliwowe.** Modernizacje powinny obejmować odwodnienie dróg i linii kolejowych, stabilizację skarp, wzmocnienie nasypów, podwyższanie niwelety na terenach zalewowych, procedury zimowe, rozwój systemów nawigacji i dozoru lotniczego oraz integrację danych pogodowych z systemami zarządzania ruchem. Dla kluczowych węzłów transportowych, terminali, lotnisk i systemów sterowania należy zapewnić awaryjne źródła zasilania, zapasy paliwa i priorytetowe procedury przywracania funkcji.
8. **Zapewnić odporność zasilania zakładów przemysłu obronnego.** Dla zakładów o znaczeniu strategicznym należy określić minimalne wymagania dotyczące ciągłości i autonomii energetycznej, uwzględniające redundancję zasilania, lokalne źródła i magazyny energii zdolne do pracy w trybie wyspowym, zapasy paliw i materiałów eksploatacyjnych, części zamienne oraz odpowiednio przygotowany personel. Procedury przyłączenia nowych zakładów oraz zwiększania dostępnej mocy dla zakładów istniejących powinny być koordynowane z operatorami systemu elektroenergetycznego i uwzględniać strategiczne znaczenie tych obiektów.
9. **Prowadzić stabilną politykę finansowania inwestycji, zapewnienia długoterminowych źródeł finansowania oraz skutecznej kontroli kosztów realizowanych projektów.** Istotne jest również zwiększanie dostępności wykwalifikowanych kadr poprzez rozwój systemów szkolenia i zachęty do podejmowania pracy w sektorze transportu, a także wzmacnianie potencjału przedsiębiorstw logistycznych i terminali przeładunkowych w celu zwiększenia ich zdolności do obsługi wzmózonych potoków przewozowych. Dodatkowo należy rozwijać mechanizmy współpracy między administracją publiczną, a sektorem prywatnym, tworzyć rezerwy strategicznych zasobów transportowych oraz wdrażać systemy monitorowania ryzyka ekonomicznego i planowania awaryjnego, co pozwoli utrzymać ciągłość funkcjonowania systemu transportowego i zwiększyć jego odporność na zakłócenia.
10. **Zbudować portfel kwalifikowanych operatorów i kontraktować gotowość, a nie**

tylko pojedyncze usługi. Model jednego głównego operatora jest niewystarczający. Należy stworzyć portfel obejmujący krajowych operatorów terytorialnych, operatorów magazynowania i dystrybucji przemysłowej, przewoźników kolejowych, przewoźników ładunków ciężkich, niebezpiecznych i ponadnormatywnych, operatorów cargo lotniczego oraz globalnych integratorów dla dostaw pilnych i międzynarodowych. Umowy powinny obejmować nie tylko cenę usługi, lecz także dostępność powierzchni, taboru, okien przeładunkowych, personelu, obsługi celnej, systemów danych, procedur awaryjnych i czasu uruchomienia zdolności.

- 11. Powiązać każdą inwestycję produkcyjną w przemyśle obronnym z obowiązkowym zabezpieczeniem logistycznym.** Nowe hale, linie technologiczne i centra kompetencyjne powinny być planowane razem z magazynami, kompletacją partii, opakowaniami, kontrolą jakości, dokumentacją, częściami zamiennymi, obsługą techniczną, zdolnościami wysyłkowymi, operatorami i zapasami minimalnymi. Żadna kluczowa inwestycja produkcyjna w przemyśle obronnym nie powinna być zatwierdzana bez planu logistycznego obejmującego magazyny, place, kompletację, dokumentację, kontrolę jakości, opakowania, części zamienne, MRO, zdolność wysyłkową, dane, energię, BCP i właściciela przepływu end-to-end.
- 12. Zbudować warstwowy system zapasów dla pozycji krytycznych.** Należy odejść od jednego modelu zapasu i rozdzielić zapasy na: rezerwy państwowe, zapasy produkcyjne, zapasy operatorów, bufor importowe, zapasy konsygnacyjne, części zamienne i opakowania. Priorytet nadać pozycjom o długim czasie odtworzenia, niskiej zastępowalności i wysokim wpływie na gotowość.
- 13. Ustanowić wspólny standard danych logistycznych i materiałowych oraz bezpieczny system wymiany informacji.** Należy ujednolicić sposób identyfikacji materiałów, komponentów, partii, dokumentacji, zapasów, operatorów i statusów dostaw między przedsiębiorstwami sek-

tora obronnego, resortem obrony narodowej i Siłami Zbrojnymi RP. Standard powinien obejmować właścicieli danych, poziomy jawności, interoperacyjność systemów cywilnych i wojskowych, mapowanie indeksów materiałowych, kontrolę jakości danych, identyfikowalność komponentów, ochronę informacji i cyberbezpieczeństwo. Należy przy tym zapewnić mapowanie pomiędzy stosowanymi w sektorze cywilnym standardami identyfikacji i wymiany danych a wojskowymi indeksami materiałowymi i systemami ewidencyjnymi oraz możliwość bezpiecznej, zautomatyzowanej wymiany informacji pomiędzy systemami funkcjonującymi w środowiskach o różnych poziomach ochrony informacji. Docelowo powinien powstać bezpieczny punkt koordynacji informacji logistycznej, który pokazuje opóźnienia, braki dokumentacyjne, ryzyka dostaw i statusy partii bez ujawniania nadmiarowych danych wrażliwych.

- 14. Zabezpieczyć MRO, prawa serwisowe i części zamienne jako element każdej decyzji zakupowej.** Należy w kontraktach na sprzęt wojskowy wymagać nie tylko dostawy wyrobu, ale także pakietu części krytycznych, narzędzi, dokumentacji technicznej, oprogramowania diagnostycznego, praw do serwisu, stanowisk testowych, szkolenia personelu i krajowej zdolności naprawy.
- 15. Regularnie testować gotowość logistyczną w ćwiczeniach aktywacyjnych i testach odporności.** Najważniejszym sprawdzianem gotowości nie jest deklaracja dostępności magazynu, operatora lub środka transportu, lecz praktyczne uruchomienie zakontraktowanej zdolności. Ćwiczenia powinny obejmować zmianę operatora, uruchomienie dodatkowej powierzchni magazynowej, wykorzystanie alternatywnego terminala, obsługę dokumentacji, odprawę, dostępność taboru, załadunek, przeładunek, wydanie zasobu odbiorcy oraz pracę w warunkach awarii systemu informatycznego, braku zasilania, braku paliwa, zakłócenia pogodowego lub cyberataku. Wyniki ćwiczeń powinny aktualizować katalog zdolności, umowy, procedury i plany awaryjne.

5. SZTUCZNA INTELIGENCJA W BEZPIECZEŃSTWIE ŁAŃCUCHÓW DOSTAW

5.1. Zastosowanie AI i analiza danych w zarządzaniu ryzykiem dostaw – kierunki rozwoju

W przemyśle obronnym, tak jak w wielu innych obszarach, obserwujemy coraz szybszą transformację cyfrową łańcuchów dostaw. Jednym z rezultatów tego procesu jest wytwarzanie dużych wolumenów danych o bardzo wysokim zróżnicowaniu, od specyfikacji inżynierskich, rejestrów produkcyjnych, poprzez manifesty przewozowe, po nieustrukturyzowane raporty wywiadowcze i rynkowe. Z technicznego punktu widzenia, gdyby umiejętnie gromadzić wytwarzane zasoby informacyjne, pozwoliłoby to obecnie na generowanie oglądu sytuacji w czasie rzeczywistym oraz na wyciąganie wniosków na przyszłość, gdzie podstawowym celem jest uzyskanie zdolności do jak najwcześniejszego identyfikowania istotnych problemów i szybkiej rekonfiguracji zasobów zanim kryzys się zmaterializuje. W tym kontekście, kluczową kwestią staje się właściwa analiza tak wielkich zbiorów danych.

Odpowiedzią na ten problem są metody sztucznej inteligencji (AI), których przewaga nad klasycznymi metodami analitycznymi polega przede wszystkim na zdolności do dynamicznego łączenia danych pochodzących z różnych źródeł oraz przetwarzania informacji nieustrukturyzowanych, które stanowią wyzwanie dla tradycyjnych systemów relacyjnych. Podczas gdy klasyczne oprogramowanie często wymaga czasochłonnego, ręcz-

nego ujednolicania danych i działań przede wszystkim reaktywnie, systemy AI mogą w sposób ciągły analizować i syntetyzować bardzo duże wolumeny rozproszonych informacji, skracając czas potrzebny do przygotowania prognoz i ocen sytuacji. Jest to szczególnie istotne w środowiskach o wysokim rygorze bezpieczeństwa, w których informacje mogą być rozproszone, niepełne lub celowo ukrywane. W takich warunkach zaawansowane metody analizy grafowej wspierane przez AI umożliwiają identyfikowanie i mapowanie wielowymiarowych, często nieliniowych relacji pomiędzy podmiotami, zasobami i zdarzeniami. Pozwala to przejść od pasywnej analizy danych historycznych do aktywnego testowania scenariuszy typu „co, jeśli?” oraz formułowania rekomendacji dotyczących możliwych działań. AI może zatem odgrywać kluczową rolę w nowoczesnej analizie danych, oferując narzędzia, które mają potencjał rozwiązania wielu istotnych problemów związanych z zarządzaniem łańcuchami dostaw w przemyśle obronnym, również w warunkach pokoju.

Wyróżnić możemy następujące kluczowe obszary, w których zastosowanie AI wydaje się najbardziej obiecujące: głębokie mapowanie sieci zaopatrzenia, symulacje warunków skrajnych za pomocą technologii cyfrowych bliźniaków oraz utrzymanie predykcyjne.

Głębokie mapowanie sieci dostawców, „friend-shoring” i kształtowanie rynku

Współczesna literatura¹⁸² silnie akcentuje potrzebę geograficznej rekonfiguracji produkcji zbrojeniowej w kierunku tzw. „friend-shoringu”, czyli, w naszej sytuacji, przenoszenia baz produkcyjnych do państw sojuszników w ramach NATO i UE. W tym kontekście, sztuczna inteligencja odgrywa kluczową rolę w zmierzaniu się z trzema kluczowymi wyzwaniami:

- Pierwszym jest analiza posiadanych informacji w celu głębokiego zmapowania sieci dostawców co umożliwi identyfikację wąskich gardeł i priorytetyzację pożądanых zmian, tj. wybranie dostawców, z których należy zrezygnować z powodu zbyt wysokiego ryzyka oraz potencjalnych nowych dostawców.
- Drugim wyzwaniem jest automatyzacja i przyspieszanie rygorystycznego procesu walidacji oraz wdrażania (onboardingu) nowych dostawców, weryfikując ich zgodność z normami wojskowymi.
- Trzecim wyzwaniem jest optymalizacja struktury rynkowej w przemyśle obronnym UE, m.in. przeciwdziałanie nadmiernemu rozdrobnieniu poddostawców.

O ile mapowanie sieci dostawców w przemyśle obronnym jest powszechną praktyką, wyzwaniem jest głębokość z jaką przeprowadza się tego rodzaju analizę. Historycznie robiono ją tylko w stosunku do dostawców pierwszego i drugiego poziomu (P-1 oraz P-2). Tymczasem, wojny i napięcia geopolityczne ostatnich lat pokazały ryzyko związane z tak płytkim podejściem, gdzie brak wglądu w głębsze warstwy – od hut czy kopalń węgla i rudy przez producentów wafli krzemowych po przemysł wydobywczy metali ziem rzadkich – stawał się przyczyną powstawania wąskich gardeł. Deficyt wiedzy dotyczy w szczególności poddostawców poziomu trzeciego i czwartego (P-3 oraz P-4), szczególnie tych odpowiadających za dystrybucję komponentów kluczowych, takich

jak zaawansowane układy półprzewodnikowe czy metale ziem rzadkich, których nie da się zastąpić w procesach technologicznych. Presja na mapowanie tak głębokich struktur wykazuje bezpośrednią analogię do nowych wymogów wprowadzonych przez Unię Europejską w zakresie identyfikacji i odporności podmiotów krytycznych (m.in. dyrektywa CER), gdzie fundamentem bezpieczeństwa staje się drobiazgowo zrozumienie mapy zależności sieciowych, a nie tylko podmiotów z pierwszej linii frontu.

Identyfikacja tych głębszych powiązań jest określana mianem „podświetlania łańcucha dostaw” (*supply chain illumination*). Poprzednie technologie służące temu celowi były nieefektywne gdyż opierały się analizie danych które dostarczali bezpośredni dostawcy. Trudno było w takiej sytuacji zidentyfikować ukryte powiązania lub firmy fasadowe na niższych poziomach. Obecnie analizy tego rodzaju mogą być realizowane z wykorzystaniem wielkich modeli językowych (LLM) oraz zbudowanych na nich autonomicznych agentach. Narzędzia te są w stanie prowadzić zautomatyzowaną agregację i syntezę heterogenicznych, nieustrukturyzowanych zbiorów danych (m.in. manifestów przewozowych, rejestrów korporacyjnych oraz danych wywiadu jawnoźródłowego – OSINT), transformując je w dynamiczne grafy wiedzy. Pozwala to na bardziej efektywne wykrywanie ukrytych zależności, które są trudne do identyfikacji przez analityków używających tradycyjnych podejść. Innymi słowy, AI zwiększa możliwość automatyzacji, skalowania i ciągłej aktualizacji analiz, które wcześniej wymagały większego udziału pracy analitycznej. Oczywiście, wyniki analiz prowadzonych przez modele LLM powinny podlegać weryfikacji zważywszy na ciągle występujące ryzyko halucynacji tych modeli.

W odniesieniu do walidacji oraz wdrażania nowych podmiotów, wskazuje się na sztuczną inteligencję jako na kluczową technologię niwelowania barier operacyjnych¹⁸³. Tradycyjne procedury weryfikacji zgodności z re-

182 Taylor, C. O. (2026). Reshoring, Nearshoring, and North American Supply Chains. Working Paper. Houston, TX: Rice University's Baker Institute for Public Policy.

183 Roberts, A. (2025). Utilization of Artificial Intelligence (AI) to Illuminate Supply Chain Risk. Fort Belvoir, VA: Defense Logistics Agency.

strykcyjnymi specyfikacjami wojskowymi są wysoce zbiurokratyzowane i podatne na wystąpienie wąskich gardeł informacyjnych¹⁸⁴. Tymczasem, wdrożenie zaawansowanych algorytmów przetwarzania języka naturalnego (NLP) oraz dużych modeli językowych (LLM) pozwala na szybką semantyczną analizę i automatyczną walidację rozproszonej, nieustrukturyzowanej dokumentacji technicznej, w tym świadectw badania materiałów oraz certyfikatów zgodności. Taka automatyzacja procesu wdrażania nowych podmiotów nie tylko skraca czas, ale także zmniejsza ryzyko wystąpienia błędu popełnionego przez człowieka. Dodatkowo, daje szansę na zwiększenie integralności i zgodności technicznej wdrażanych komponentów.

Usprawnienie procesu wprowadzania nowych poddostawców na poziomie operacyjnym stanowi bezpośredni punkt wyjścia do realizacji trzeciego wyzwania, jakim jest globalna optymalizacja struktury rynkowej i przeciwdziałanie strukturalnemu rozdrobnieniu europejskiego przemysłu obronnego. Jak jednoznacznie wskazują najnowsze dokumenty strategiczne Komisji Europejskiej – w tym *White Paper for European Defence Readiness 2030* – oraz uzupełniający ją raport instytucjonalny *Defence Readiness Roadmap 2030*¹⁸⁵, fragmentacja popytu i podaży wyraźnie ogranicza unijne zdolności produkcyjne. Dotychczasowa praktyka, w ramach której poszczególne państwa członkowskie zamawiają sprzęt według własnych specyfikacji technicznych, promuje lokalnych narodowych producentów i uniemożliwia wdrożenie produkcji masowej, w której duże firmy specjalizują się w konkretnych rodzajach uzbrojenia. Wszystko to blokuje cel osiągnięcia przynajmniej 40% udziału wspólnych zamówień do 2030 roku¹⁸⁶. W tym kontekście, można oczekiwać, że AI przestanie być jedynie systemem wsparcia, a stanie się kluczowym narzędziem wykorzystywanym w procesie konsolidacji rynku. W szczególności,

wykorzystując modele AI mogą być zdolne do automatycznej ekstrakcji, normalizacji i mapowania semantycznego rozproszonych danych przetargowych w wielu językach unijnych. W przeciwieństwie do tradycyjnych baz danych – które były nieelastyczne i wymagały żmudnego, manualnego ujednolicania przez zespoły eksperckie – współczesne algorytmy AI potrafią samodzielnie powiązać odmienne opisy inżynierskie w jeden spójny profil techniczny. Potencjalnie ułatwia to identyfikowanie punktów wspólnych i wdrażanie unijnych zakupów grupowych i służy konsolidacji rynku dla poszczególnych produktów.

Symulacje warunków skrajnych za pomocą technologii cyfrowych bliźniaków

Głębokie mapowanie sieci dostawców stanowi bezpośredni punkt wyjścia do wdrożenia koncepcji „cyfrowego wątku” (*digital thread*), realizowanej za pomocą technologii cyfrowych bliźniaków łańcucha dostaw¹⁸⁷. Paradygmat ten jest obecnie uznawany za fundament nowoczesnego zarządzania ryzykiem, przewidywania zakłóceń oraz budowania odporności operacyjnej łańcuchów dostaw¹⁸⁸. Cyfrowy wątek to zintegrowany, ciągły i dwukierunkowy model danych, który dzięki architekturze sztucznej inteligencji pozwala na spięcie dotychczas odizolowanych silosów informacyjnych – od systemów zarządzania cyklem życia produktu, przez realizację produkcji, aż po systemy planowania zasobów i logistykę polową (przykładem jest rozwiązanie firmy SIMBA Chain wdrożone w USAF¹⁸⁹). Taka spójna struktura danych może być wykorzystana do śledzenia i analizowania każdego krytycznego komponentu uzbrojenia na całej ścieżce jego istnienia: od fazy projektowej, przez linie montażową, aż po realne zużycie i cykl eksploatacji w warunkach bojowych.

184 Rasmussen, A., Sabic, H., Saha, S. i Nielsen, I. E. (2023). Supplier selection for aerospace & defense industry through MCDM methods. *Cleaner Engineering and Technology*, 12, 100590. <https://doi.org/10.1016/j.clet.2022.100590>

185 [https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782589/EPRS_BRI\(2026\)782589_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782589/EPRS_BRI(2026)782589_EN.pdf)

186 https://defence-industry-space.ec.europa.eu/eu-defence-industry/readiness-roadmap-2030_en

187 Shao, C., Kibira, D. i Frechette, S. (2024). *Digital Twins for Advanced Manufacturing: The Standardized Approach*. W: *Digital Twins, Simulation, and Metaverse*. Washington, DC: Springer Nature.

188 Ivanov, D. i Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning & Control*, 32(9), 775–788. <https://doi.org/10.1080/09537287.2020.1768450>

189 SIMBA Chain (2026). *Digital Thread*. <https://simbachain.com/digital-thread/>

Podczas gdy cyfrowy wątek pełni funkcję „układu nerwowego”, tj. odpowiada za nieprzerwany przepływ danych między systemami, cyfrowy bliźniak stanowi „serce i mózg” tego rodzaju architektury. Jest to dynamiczna replika całego ekosystemu logistycznego i produkcyjnego działająca w czasie rzeczywistym. Rolą cyfrowego bliźniaka jest ciągle pobieranie danych z cyfrowego wątku (np. sygnałów IoT z fabryk, telemetrycznych raportów o stanie maszyn czy danych o lokalizacji transportów) i przekładanie ich na matematyczny model funkcjonowania zaplecza armii. Dzięki temu potrafi on wirtualnie odwzorować fizyczne interakcje, zużycie materiałowe oraz zależności operacyjne pomiędzy podmiotami. Literatura przedmiotu proponuje aby zaawansowane algorytmy AI (w tym uczenie maszynowe i nieliniowe modele predykcyjne) wykorzystać w środowisku cyfrowego bliźniaka do prowadzenia dynamicznych testów warunków skrajnych (*stress testing*) oraz zaawansowanych symulacji scenariuszy typu „co-jeśli”¹⁹⁰. Platformy symulacyjne zintegrowane z cyfrowym bliźniakiem i AI potrafią bardzo szybko przetworzyć miliony zmiennych i obliczyć operacyjne skutki nagłych zakłóceń logistycznych. Przykładowo, symulując nagłą utratę dostępu do strategicznego krytycznego punktu logistycznego, takiego jak port w Gdyni (będącego kluczowym hubem dla stałej obecności wojskowej i rotacji sił NATO na wschodniej flance), możemy za pomocą algorytmów sztucznej inteligencji natychmiastowo przeliczyć wpływ tego zdarzenia na łańcuchy dostaw części zamiennych. Cyfrowy bliźniak może automatycznie prognozować stopień obniżenia gotowości operacyjnej konkretnych platform bojowych. Dzięki temu logistycy i planiści wojskowi uzyskują ilościowo ocenione alternatywne warianty tras, rekomendacje dotyczące relokacji zapasów i optymalne plany awaryjne, zanim nastąpią fizyczne skutki kryzysu.

Warto również wspomnieć, że technologia cyfrowych bliźniaków może przynieść bardzo duże realne oszczędności. Szacuje się, że obecnie koszty operacyjne i wsparcia logistycznego stanowią większość całkowitych kosztów cyklu życia zaawansowanych systemów obronnych. Wieloletnie obciążenia finansowe są determinowane często przez decyzje podejmowane na wczesnych etapach projektów. Szczególnie narażone są projekty wielonarodowe, gdyż opierają się często na niekompatybilnych podejściach, co zwiększa ryzyko przekroczenia budżetu. Stosując algorytmy AI w ramach cyfrowego bliźniaka jesteśmy w stanie w dużym stopniu rozwiązać ten problem budując i analizując dynamiczne scenariusze kosztowe nawet przy niepełnych i niejednorodnych specyfikacjach technicznych i na wczesnym etapie akwizycji uzbrojenia¹⁹¹.

Literatura z zakresu inżynierii systemów bezzałogowych wskazuje, że integracja cyfrowych bliźniaków na liniach montażowych pozwala na bezpośrednie mapowanie zmian komponentów u dostawców na globalne zachowanie całej floty^{192 193}. Przykładem jest tutaj badawcza linia produkcyjna uruchomiona na Chalmers University of Technology, gdzie pokazano, że wirtualizacja procesów produkcyjnych i logistycznych pozwala na natychmiastowe testowanie scenariuszy odpornościowych¹⁹⁴. W warstwie inżynierskiej zaawansowane modele matematyczne – jak cyfrowy bliźniak układu silnika bezszczotkowego i śmigła opracowany przez Gauthiera i in. – pozwalają precyzyjnie symulować nieliniowe zmiany siły ciągu oraz oporu śmigła wywołane zmianą dostawcy komponentu. Pozwala to ocenić dynamikę lotu platformy BSP w środowisku symulacyjnym bez konieczności przeprowadzania testów empirycznych.

190 Liu, C., Wang, Y., Purvis, L. i Potter, A. (2026). Can digital twin technology enhance supply-chain resilience? A systematic literature review. *Sustainability*, 18(5), 2361. <https://doi.org/10.3390/su18052361>

191 Tudosia, M. (2026). Predictive maintenance and life cycle management for armoured vehicles. *European Security & Defence*.

192 Gauthier, D. J., Biederman, N., Gyovai, B. i Wilhelm, J. P. (2024). Digital twin of a DC brushless electric motor-propeller system with application to drone dynamics. *AIAA SCITECH 2024 Forum*, art. 2359. <https://doi.org/10.2514/6.2024-2359>

193 Lopes, P. V., Chen, S., González Sánchez, J. P., Bekar, E. T., Bokrantz, J. i Skoogh, A. (2023). Data-driven smart maintenance decision analysis: A drone factory demonstrator combining digital twins and adapted AHP. W: *Proceedings of the 2023 Winter Simulation Conference, 1996–2007*. <https://doi.org/10.1109/WSC60868.2023.10408351>

194 Ibidem.

Utrzymanie predykcyjne

Sztuczna inteligencja może pełnić niezwykle istotną rolę optymalizując koszty utrzymania uzbrojenia poprzez tzw. utrzymanie predykcyjne (*predictive maintenance*). Algorytmy AI mogą analizować w czasie rzeczywistym strumienie danych z sensorów IoT zainstalowanych na kluczowych platformach bojowych — takich jak czołgi (np. K2 Black Panther) czy samobieżne armatohaubice (np. Krab) — i automatycznie zamawiają komponenty zamiennie dokładnie wtedy, gdy wykazują one pierwsze, niewidoczne dla człowieka symptomy zużycia. Pozwala to na całkowite odejście od kosztownego i nieefektywnego modelu magazynowania zapasów na wypadek awarii na rzecz precyzyjnego planowania logistycznego.

Wdrożenie predykcyjnego zarządzania zasobami zintegrowanego z cyfrowymi bliźniakami pozwala na redukcję całkowitego kosztu posiadania określonego rodzaju uzbrojenia, przy jednoczesnym wzroście gotowości sprzętowej floty. Przejście z reaktywnego utrzymania technicznego na proaktywne, wyprzedzające zapobieganie awariom, nie tylko maksymalizuje bezpośrednią zdolność bojową, ale także stabilizuje łańcuchy dostaw części zamiennych u producentów.

Co istotne w kontekście europejskim, audytowalność prognoz algorytmicznych może być wykorzystany jako instrument zwiększający zaufanie pomiędzy ministerstwami obrony państw członkowskich. Pozwoliłoby to na bardziej precyzyjne, wspólne planowanie budżetów logistycznych i zwiększyłoby szansę na skuteczną kooperację międzynarodową.

Tym niemniej, w kontekście utrzymania predykcyjnego kluczowe jest właściwe wartościowanie celów, jakim służy optymalizacja algorytmiczna. Komercyjny model logistyczny „dokładnie na czas” (ang. „just-in-time”), nastawiony na maksymalną redukcję kosztów, świetnie się sprawdza w rozwiązaniach cywilnych, ale jest nieadekwatny w warunkach kryzysu lub wojny. Doświadczenia z okresu pandemii COVID-19 oraz pełnoskalowej wojny w Ukrainie jednoznacznie dowodzą, że fundamentem odporności łańcuchów dostaw w przemyśle obronnym jest celowe utrzymywanie nadmiarowych zapa-

sów. Zatem sztuczna inteligencja powinna być wykorzystywana do precyzyjnego kalibrowania i optymalizowania poziomów tych rezerw, a nie do ich eliminowania.

Dyskusja, ryzyka i ograniczenia wdrożeniowe

Mimo bezdyskusyjnych korzyści wynikających z implementacji sztucznej inteligencji w wojskowych łańcuchach dostaw, należy podkreślić, że wdrożenie w praktyce opisanych powyżej nowych rozwiązań wiąże się z pokonaniem szeregu trudnych wyzwań. W szczególności:

- Silosowość oraz niska jakość danych wejściowych:** Podstawową barierą nie jest obecnie brak dojrzałości samych technologii obliczeniowych, lecz ograniczona interoperacyjność systemów informacyjnych wśród podmiotów całego ekosystemu. Dane niezbędne do zasilania modeli AI są rozproszone i odizolowane nawet pomiędzy poszczególnymi przedsiębiorstwami wchodzącymi w skład Polskiej Grupy Zbrojeniowej. Ten sam problem występuje w kontekście prywatnych podmiotów przemysłu obronnego a nawet instytucji państwowych. Problemy tego rodzaju występują nie tylko w Polsce, ale właściwie we wszystkich Państwach Członkowskich NATO i wynikają z obiektywnego faktu, że dane związane z produkcją zbrojeniową są niezwykle wrażliwe. Powoduje to, że technologia cyfrowych bliźniaków łańcucha dostaw znajduje się w większości przypadków na etapie pilotażowym lub bardzo ograniczonych wdrożeń dedykowanych. Budowa pełnowymiarowego, działającego w czasie rzeczywistym cyfrowego bliźniaka wymaga wieloletnich, kapitałochłonnych inwestycji infrastrukturalnych, rygorystycznej standaryzacji struktur danych u wszystkich kooperantów oraz stałego dostępu do informacji wejściowych o jak najwyższej jakości. Remedium na problemy rozproszenia i braku integracji źródeł danych jest wypracowanie jednolitych standardów i obowiązków wymiany informacji. Jest to o tyle trudne, że rozwiązania krajowe w tym zakresie muszą współgrać z przepisami międzynarodowymi doty-

czącymi ochrony informacji niejawnych. Tym niemniej, bez tego rodzaju zmian, potencjał analityczny systemów opartych na AI pozostanie drastycznie ograniczony, a technologia nie wyjdzie poza fazę jednostkowych wdrożeń testowych.

- **Cyberbezpieczeństwo i podatność na sabotaż cyfrowy (zatrutowanie danych):** Wdrażanie systemów AI drastycznie zwiększa wachlarz możliwych cyberataków. W czasie pokoju największym zagrożeniem dla AI staje się sabotaż cyfrowy realizowany poprzez ataki kontradiktoryjne, w tym tzw. zatrutowanie danych (*data poisoning*). Na przykład, przy nieadekwatnej ochronie, przeciwnik może celowo i w sposób niezauważalny zmodyfikować dane o stanach magazynowych, parametrach technicznych lub logistyce komponentów do dronów (np. fałszując sygnatury jakościowe materiałów kompozytowych u poddostawcy). Taka manipulacja może doprowadzić do zainstalowania wadliwych komponentów w całej partii produktów i w konsekwencji wywołać systemową awarię wielu bezzałogowców¹⁹⁵.
- **Ryzyko wynikające z łańcucha dostaw oprogramowania:** Wdrażanie zewnętrznych algorytmów AI wymaga rygorystycznego audytowania dostawców kodu pod kątem obecności ukrytych podatności oraz celowo wprowadzonych furtek (*backdoors*). O cyberbezpieczeństwie traktować będą kolejne sekcje niniejszego rozdziału.
- **Brak determinizmu i halucynacje modeli LLM oraz Agentów AI:** Wykorzystanie autonomicznych agentów opartych na dużych modelach językowych (LLM) do analizy raportów rynkowych, dokumentacji przetargowej czy białego wywiadu gospodarczego wiąże się z ryzykiem konfabulacji (halucynacji). W kontekście wojskowego zarządzania ryzykiem, gdzie decyzje logistyczne mogą przekładać się bezpośrednio na gotowość bojową i życie żołnierzy,

wygenerowanie przez AI fałszywego wniosku o statusie dostawcy lub dostępności surowców krytycznych może wygenerować nieakceptowalne, kosztowne błędy.

- **Dylemat suwerenności technologicznej:** Państwa sojusznicze stają przed fundamentalnym dylematem geopolitycznym w obszarze zarządzania technologią. Z jednej strony istnieje możliwość natychmiastowego wdrożenia wysoce efektywnych, gotowych rozwiązań AI dostarczanych przez globalne, prywatne korporacje technologiczne (głównie z USA). Z drugiej strony rodzi to ryzyko utraty kontroli nad wrażliwymi danymi operacyjnymi oraz uzależnienia od zagranicznych podmiotów. Alternatywą jest kosztowna budowa własnych, suwerennych systemów AI, które mogą być początkowo mniej zaawansowane technologicznie, lecz pozostają w pełni kontrolowane, bezpieczne i audytowalne przez państwowe organy bezpieczeństwa¹⁹⁶.
- **Wyjaśnialność modeli (*Explainable AI*):** Decyzje dotyczące relokacji zasobów, priorytetów logistycznych czy rezygnacji z danego dostawcy muszą być, w kontekście zdolności obronnych państwa, w miarę możliwości transparentne i audytowalne. Stosowanie algorytmów typu „czarna skrzynka”, które generują rekomendacje bez możliwości odtworzenia logicznej ścieżki wnioskowania, jest nieakceptowalne dla wojskowych organów decyzyjnych.
- **Zjawisko automatyzacji zaufania (*automation bias*):** Kolejną kwestią jest realne ryzyko związane z uwarunkowaniami psychologicznymi człowieka, w którym użytkownicy systemów wspierania decyzji opartych na AI zaczynają bezkrytycznie przyjmować i zatwierdzać rekomendacje generowane przez te rozwiązania. Brak zdrowego sceptycyzmu oraz rutynowe poleganie na wskazaniach AI może prowadzić nie tylko do złych decyzji, ale do utraty umiejętności analitycznych.

¹⁹⁵ Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X. i Hamin, M. (2025). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations (NIST AI 100-2 E2025). Washington, D.C.: U.S. Department of Commerce. <https://csrc.nist.gov/pubs/ai/100/2/e2025/final>

¹⁹⁶ Johansen, A. i Kruck, A. (2025). The competence–control trade-off in military AI innovation: Autonomous weapons systems and shifting modes of state control over private experts. *European Journal of International Security*. <https://doi.org/10.1017/eis.2025.10020>

Należy podkreślić, że algorytmy AI pozwalają na dużo efektywniejszą analizę danych i wspierają podejmowanie decyzji, ale w same w sobie nie stanowią ostatecznego rozwiązania problemu. Np. mapowanie głębszych poziomów zaopatrzenia (P-3 oraz P-4) pozwala na precyzyjne podświetlenie łańcucha dostaw, jednak samo wskazanie anomalii nie eliminuje fizycznego ryzyka. Kluczowym problemem współczesnego przemysłu zbrojeniowego pozostaje bowiem zbyt duża koncentracja geograficzna produkcji istotnych komponentów – w szczególności zaawansowanych układów półprzewodnikowych, elektroniki oraz materiałów specjalnych. O ile modele AI są w stanie skutecznie zmapować i zasygnalizować te niebezpieczne zależności, o tyle nie zastąpią one twardych instrumentów polityki przemysłowej i zarządczej. Przeciwdziałanie tym podatnościom wymaga równoległego i aktywnego wdrażania strategii dywersyfikacji źródeł zaopatrzenia,

fizycznej budowy państwowych zapasów strategicznych oraz systematycznego rozwoju krajowych zdolności produkcyjnych.

Podsumowując, sztuczna inteligencja powinna być postrzegana wyłącznie jako wysoce zaawansowane narzędzie wspomagające procesy analityczne i zarządcze, a nie jako uniwersalny substytut dla kompetencji ludzkich, struktur organizacyjnych czy polityki suwerennościowej państwa. Odporność i bezpieczeństwo łańcuchów dostaw polskiego przemysłu obronnego nie będą nigdy wynikać z samego wdrożenia nowoczesnego oprogramowania, ale będą rezultatem synergii, tj. przemysłanego połączenia technologii obliczeniowej z dojrzałym zarządzaniem ryzykiem, elastycznością operacyjną przedsiębiorstw oraz długofalową i konsekwentną polityką przemysłową kraju.

5.2. Cyberbezpieczeństwo w łańcuchach dostaw zasadniczego SpW, ŚB, ŚM dla Sił Zbrojnych RP

Polska znajduje się regionie, w którym cyberprzestrzeń stała się jednym z narzędzi oddziaływania geopolitycznego wrogich państw. Oprócz klasycznej cyberprzestępczości nastawionej na zysk coraz częściej obserwujemy incydenty o charakterze zakłócającym i destrukcyjnym, wymierzone w instytucje, sektory strategiczne oraz elementy infrastruktury krytycznej. Dla biznesu, w szczególności polskiego przemysłu zbrojeniowego oznacza to wzrost ryzyka bezpośredniego oraz pośredniego, poprzez łańcuchy dostaw i zależności od dostawców usług cyfrowych.

Równolegle polskie przedsiębiorstwa przechodzą transformację cyfrową, przenosząc dane i procesy do chmury obliczeniowej, integrując systemy ze swoimi partnerami, automatyzując finanse i logistykę, rozwijając modele pracy zdalnej, próbując także wdrażać narzędzia oparte o sztuczną inteligencję. Zmiany te niewątpliwie podnoszą produktywność organizacji, jednakże jednocześnie

zwiększają „powierzchnię ataku” dzięki zwiększonej liczbie kont, urządzeń, punktów zdalnego dostępu i uprawnień. W takim ekosystemie cyberbezpieczeństwo przestaje być kwestią wyłącznie technologiczną, a staje się przede wszystkim elementem zarządzania ryzykiem biznesowym oraz wskaźnikiem odporności operacyjnej danej organizacji.

Niemal w każdym tygodniu, media i organizacje monitorujące naruszenia bezpieczeństwa danych, donoszą o kolejnych cyberatakach, wyciekach danych i coraz nowszych metodach dokonywania przestępstw w sieci. Nie ma żadnych podstaw, aby oczekiwać odwrócenia tego trendu. Z badań przeprowadzonych przez firmę VECTO¹⁹⁷ wynika, że całkowita liczba cyberataków rośnie niezależnie od wielkości organizacji, choć największą intensyfikację odnotowują duże przedsiębiorstwa (55% z nich zauważyło wzrost lub znaczny wzrost w porównaniu do 38% średnich i 40% małych firm).

¹⁹⁷ Raport VECTO - Cyberbezpieczeństwo w polskich firmach -VIII Edycja 2025

O zwiększeniu intensywności ataków świadczy niemal dwukrotny spadek liczby firm, które nie odnotowały żadnego ataku, z 33% do 17%. Oznacza to, że dla dużej części organizacji w Polsce, cyberzagrożenia przestały być hipotezą, a stały się realnym czynnikiem ryzyka.

Typowe zagrożenia cyberbezpieczeństwa w łańcuchach dostaw (obronnych) obejmują ataki złośliwego oprogramowania (*malware*), *ransomware*, *phishing*, zagrożenia

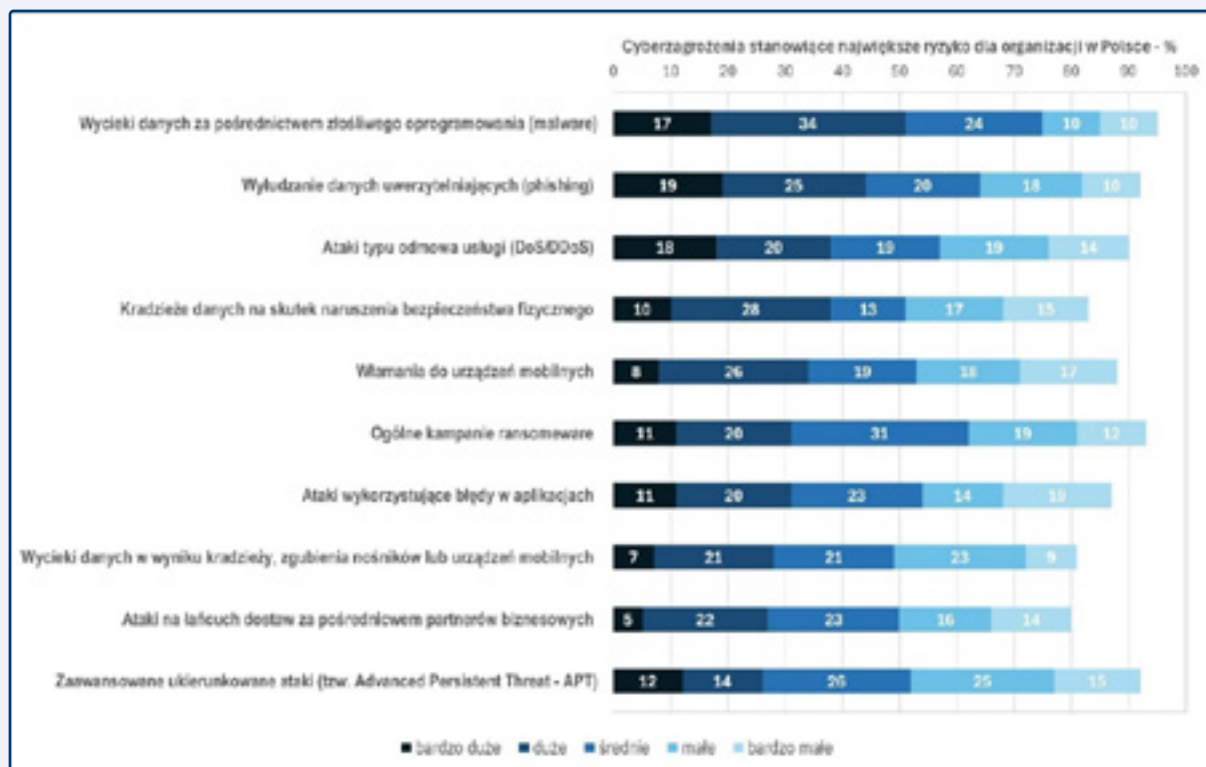
wewnętrzne oraz podatności w oprogramowaniu lub sprzęcie „firm trzecich”. Łańcuch dostaw w polskim przemyśle obronnym jest podatny na te ataki, ponieważ obejmuje on wielu kontrahentów i podwykonawców, o różnym poziomie dojrzałości w obszarze cyberbezpieczeństwa, tworząc jednocześnie otwarte punkty wejścia dla strony atakującej. Ponadto, dane wymieniane między tymi podmiotami, dodatkowo mogą zwiększać ryzyko ich ujawnienia.

Tab. 5.1. Typowe zagrożenia cyberbezpieczeństwa w łańcuchach dostaw

Zagrożenia cyberbezpieczeństwa	Opis
Phishing	polega na podszywaniu się „atakującego” pod całkowicie inną osobę bądź instytucję;
	celem ataku jest nakłonienie użytkownika do podjęcia określonego działania, na przykład kliknięcia w zainfekowany link lub pobrania dokumentu w celu zainfekowania systemu;
	celem jest wyludzenie informacji, np. danych logowania, danych osobistych lub innych, wrażliwych informacji.
Malware (złośliwe oprogramowanie)	oprogramowanie zaprojektowane do uszkodzania, zakłócania lub uzyskiwania nieautoryzowanego dostępu do systemu. Poza <i>ransomware</i> powszechnie znanymi typami są wirusy, robaki, trojany, spyware, adware, rootkity.
Ransomware	większość ataków zaczyna się od złośliwej wiadomości e-mail, której otwarcie powoduje instalację złośliwego oprogramowania w celu przejęcia (kradzieży) zasobów danej firmy;
	celem takiego ataku jest szyfrowanie danych i wymuszenie okupu za odblokowanie lub odzyskanie danych;
	atak wymusza podejmowanie decyzji pod presją czasu oraz bezlitośnie uderza w zdolność firmy do działania;
Podatności (w oprogramowaniu, sprzęcie firm „trzecich”)	najbardziej niebezpieczny rodzaj ataku dla biznesu, który może sparaliżować firmę na dłuższy czas.
	to jedna z najbardziej niebezpiecznych form infiltracji łańcucha dostaw. Atakujący wykorzystują odkryte luki w oprogramowaniu, które pozwalają im przejąć kontrolę nad urządzeniami, aplikacjami, i rozprzestrzeniać złośliwe oprogramowanie. Luki w oprogramowaniu wynikają z błędów programistycznych, niewłaściwej konfiguracji lub braków aktualizacji systemów.
Zagrożenia wewnętrzne	osoby mające dostęp do kluczowych zasobów organizacji stają się źródłem naruszeń bezpieczeństwa. Mogą przybierać one formę celowych działań takich jak: sabotaż, kradzież danych, szpiegostwo lub niecelowych jak błędy ludzkie, które mogą prowadzić do wycieku danych lub naruszenia bezpieczeństwa systemu.

Według badań przeprowadzonych przez firmę KPMG¹⁹⁸ największe ryzyko dla polskich firm stanowią wycieki danych za pośrednictwem złośliwego oprogramowania (**malware**), wyludzenie danych uwierzytelniających (**phishing**) oraz szyfrowanie danych (**ransomware**), gdzie odnotowano wzrost tych incydentów w ciągu ostatniego roku. Za najmniej zagrażające uznano **ataki na łańcuch dostaw za pośrednictwem partnerów biznesowych**, warto jednak podkreślić, że 5% wskazań dla najwyższej skali ryzyka to pięciokrotny wzrost w porównaniu z poprzednim rokiem. Podobne wnioski można wyciągnąć z danych pochodzących z raportów o zakresie globalnym, gdzie zwraca się uwagę na istotny wzrost ataków na łańcuch dostaw z udziałem tzw. „trzeciej strony” czyli partnerów biznesowych (producentów, dostawców, kooperatorów), w których atak *ransomware* pozostaje w dalszym ciągu kluczowym elementem wielu incydentów cybernetycznych.

198 Raport KPMG – Barometr cyberbezpieczeństwa – Luty 2025



Rys. 5.1. Cyberzagrożenia stanowiące największe ryzyko dla firm w Polsce

Źródło: opracowanie własne na podstawie - Raport KPMG Pt. Barometr Cyberbezpieczeństwa. Edycja 2025

Mając na uwadze, że łańcuch dostaw w polskim przemyśle obronnym stanowi sieć wzajemnych powiązań między różnymi podmiotami, obejmującą wszelkie działania związane z pozyskiwaniem surowców, produkcją oraz dystrybucją towarów i usług dla Sił Zbrojnych RP, kluczowym wydaje się być zrozumienie, czym jest cyberatak na łańcuch dostaw, jak on działa, oraz jaki wpływ może on mieć na ciągłość dostaw dla polskiego wojska.

Atak na łańcuch dostaw to zaawansowana technika cyberataku, w której atakujący infekują legalne komponenty oprogramowania poprzez ingerencję na jednym z wcześniejszych etapów ich tworzenia, dystrybucji czy aktualizacji lub infekują procesy dostawcze w celu przeniknięcia do systemu ofiary przez zaufane kanały. Zamiast atakować bezpośrednio dobrze zabezpieczoną organizację na przykład spółkę Polskiej Grupy Zbrojeniowej (PGZ), przestępcy atakują firmę partnerską tej spółki (np. dostawcę oprogramowania, usługodawcę), wstrzykując *złośliwy kod*, który przechodzi niezauważony przez mechanizmy zaufania, aż zostanie automatycznie zainstalowany w całej organizacji.

Schemat działania cyberataku na łańcuch dostaw (obronnych):

- Wybór celu:** atakujący identyfikują wybraną organizację docelową (np. spółkę PGZ);
- Identyfikacja słabszych ogniw:** atakujący przeprowadzają rekonesans w celu wykrycia słabszych ogniw w łańcuchu dostaw celu, w tym mniejszych dostawców, wykonawców, kooperantów, zewnętrznych dostawców oprogramowania i usług, którzy są słabiej zabezpieczeni;
- Początkowy atak:** atakujący włamują się do sieci jednego z tych słabszych ogniw, instalując złośliwe oprogramowanie lub wykorzystując zagrożenia wewnętrzne;
- Uzyskanie dostępu:** po wejściu do łańcuch dostaw atakujący starają się rozszerzyć swój dostęp, poruszając się w systemie zaatakowanego dostawcy, aby zbliżyć się do głównego celu;
- Wstawianie złośliwego kodu lub komponentów:** atakujący modyfikują oprogramowanie lub komponenty sprzętowe przed dostarczeniem ich do głównego celu;

- 6. Zewnętrzna filtracja:** gdy atakujący zdobędą przyczółek w systemach głównego celu, mogą przejść do zewnętrznej filtracji wrażliwych danych lub wprowadzić dalsze złośliwe oprogramowania (np. *ransomware*);
- 7. Pozostanie niewykrytym:** wiele wyrafinowanych ataków na łańcuch dostaw ma na celu pozostanie niewykrytym tak długo, jak to możliwe. Atakujący mogą tworzyć *backdoory*, wdrażać *rootkity* lub wykorzystywać inne techniki dla zachowania dostępu;
- 8. Wyjście:** po osiągnięciu swoich celów atakujący mogą próbować zatrzeć ślady, usuwając dzienniki lub dowody ataków.

Szczególnie niepokojący jest fakt, że średni czas wykrycia takiego ataku wynosi¹⁹⁹ 207 dni, co daje atakującym wystarczająco dużo czasu na przeprowadzenie zaplanowanych i szeroko zakrojonych operacji.

Najgłośniejszym przykładem ataku na łańcuch dostaw, a zarazem najbardziej złożonym i szkodliwym w historii, był atak na amerykańską firmę SolarWinds w 2020 roku. Złośliwy kod został wstrzyknięty do oprogramowania Orion przez atakującą grupę z Rosji. Zainfekowana aktualizacja została rozpowszechniona wśród 18 tysięcy klientów, w tym agencji rządowych w USA oraz dużych korporacji na całym świecie. Atak umożliwił zdalny dostęp i kradzież wrażliwych danych z sieci „ofiar” co miało długofalowe konsekwencje zarówno dla firm, jak również całych państw.

Rosnąca digitalizacja oraz automatyzacja produkcji i procesów dostawczych w polskim przemyśle obronnym zwiększa istotnie ryzyko cyberataków na łańcuch dostaw poprzez partnerów zewnętrznych, co może wpłynąć kaskadowo na ciągłość i efektywność dostaw dla polskiego wojska, przyczyniając się do istotnych opóźnień w zamówieniach i dostawach.

Skutki cyberataków w łańcuchach dostaw możemy podzielić na bezpośrednie i pośrednie. Do pierwszych zaliczamy kradzież da-

nych, zakłócenia operacyjne w bieżącej działalności organizacji oraz straty finansowe. Do drugich zaliczamy konsekwencje prawne naruszenia cyberbezpieczeństwa oraz szkody wizerunkowe organizacji.

- 9. Kradzież danych:** Naruszenie cyberbezpieczeństwa może prowadzić do wycieku danych informacyjnych, w tym tajemnic wojskowych, własności intelektualnych, unikalnych technologii wojskowych oraz innych wrażliwych dla bezpieczeństwa narodowego informacji. Przedsiębiorstwa przemysłu obronnego wydają duże środki na tworzenie tajemnic handlowych, patentów i nowych pomysłów technologicznych. Takie aktywa mają charakter strategiczny zarówno dla bezpieczeństwa Państwa, jak i konkurencyjności firmy na rynku i jej stabilności finansowej. Skradzione dane mogą umożliwić wrogiemu Polsce państwu lub konkurencji rynkowej skopiowanie lub rozwijanie pomysłów i rozwiązań technologicznych, co może spowodować zagrożenie dla bezpieczeństwa Polski lub dla strategicznej pozycji i rentowności przedsiębiorstwa.

- 10. Zakłócenia operacyjne w działalności biznesowej organizacji:** Każdy cyberatak zazwyczaj wpływa na działalność biznesową firmy szybko i w dużym stopniu, naruszając systemy w całej organizacji, uniemożliwiając wykonywanie podstawowych procesów takich jak, komunikacja, transakcje biznesowe czy też przetwarzanie danych. Może to prowadzić do dużych problemów operacyjnych, w których pracownicy nie mogą wykonywać swoich obowiązków efektywnie, co przekłada się na opóźnienie realizacji projektów (zamówień, dostaw) oraz potencjalną utratę dochodów firmy. Ponadto, czas potrzebny na odzyskanie danych po ataku może znacząco się wydłużyć, ponieważ nierzadko istnieje konieczność zakupu nowych systemów, dodatkowych zabezpieczeń i urządzeń, co jeszcze bardziej może nasilić zakłócenia w bieżącej działalności, doprowadzając czasami organizację do jej paraliżu. Przykładem

199 <https://nflo.pl/baza-wiedzy/atak-cybernetyczny-kompendium/>

takim był atak²⁰⁰ *ransomware* na szpital MSWiA w Krakowie w 2025 roku, który uniemożliwił przyjmowanie pacjentów na oddział neurologii, co miało dramatyczne konsekwencje dla zdrowia ludzi.

11. Straty finansowe: Podstawowa strata najbardziej odczuwalna w momencie naruszenia cyberbezpieczeństwa to koszty bezpośrednie, poniesione na odzyskiwanie danych i naprawę systemu. Specjaliści cyberbezpieczeństwa zwykle zlecają ocenę wycieku (kradzieży) danych, odzyskiwanie utraconych informacji i likwidację luk w systemie zaatakowanej organizacji. Czas przestoju, potrzebny na przywrócenie systemu do normalnej pracy wynosi, w przypadku ataku *ransomware*³ średnio 21 dni, podczas których firma nie może wykonywać efektywnie codziennych czynności biznesowych. Te przestoje mogą prowadzić do znacznej utraty przychodów przedsiębiorstwa, dlatego ważne jest aby minimalizować czas reakcji na takie zagrożenia. Średnie koszty naprawy mogą wynieść od milionów do dziesiątek milionów złotych w dużych organizacjach w zależności od skali i rodzaju naruszenia. Pośrednie koszty w dłuższej perspektywie mogą być jeszcze bardziej dotkliwe, ponieważ dana organizacja może już nie zarabiać tak wiele jak przed cyberatakami. W przypadku spółki publicznej notowanej na giełdzie prawdopodobny jest długoterminowy spadek wartości rynkowej, wywołany między innymi utratą zaufania swoich inwestorów.

12. Konsekwencje prawne: Istnieją różne przepisy dotyczące ochrony danych, które firmy muszą przestrzegać. Nieprzestrzeganie tych przepisów może skutkować wysokimi grzywnami, postępowaniami sądowymi i innymi konsekwencjami o charakterze prawnym.

13. Szkody wizerunkowe organizacji: Naruszenie cyberbezpieczeństwa w łańcuchu dostaw obronnych może zagrażać wizerunkowi danej organizacji (np. spółce

PGZ), zaufaniu opinii publicznej, zaufaniu interesariuszy, w szczególności Siłom Zbrojnym, będącym odbiorcą zamówionych dostaw. Interesariusze mogą mieć uzasadnione powody, by sądzić, że dana organizacja jest lekkomyślna i nieodpowiedzialna, co może zmniejszyć ich zaufanie i zaangażowanie, a nawet zakończyć współpracę. Zaufanie, to jeden z najcenniejszych aktywów każdego przedsiębiorstwa, a kiedy zostanie ono utracone w wyniku naruszenia bezpieczeństwa danych, trudno je będzie szybko odzyskać. Stopień utraty reputacji danej organizacji zależy do pewnego stopnia od rodzaju informacji, które wyciekły. Na przykład kradzież danych o stanie zdrowia pacjentów z dokumentacji medycznej, będzie poważniejszą katastrofą wizerunkową dla szpitala, niż kradzież danych osobowych jednej z instytucji finansowej. Dodatkowo należy jeszcze uwzględnić krytyczne reakcje mediów, które współcześnie są szybkie i przekazują informacje bezpośrednio na żywo, co tym skuteczniej kompromituje daną organizację i jej partnerów biznesowych w oczach szerokiej opinii publicznej.

Podsumowując, łańcuch dostaw zasadniczego SpW, ŚB, ŚM dla Sił Zbrojnych RP, kluczowy dla bezpieczeństwa narodowego stoi przed poważnymi wyzwaniami, wynikającymi z realnych, coraz bardziej powszechnych zagrożeń cyberbezpieczeństwa. Zagrożenia te mogą zakłócać (opóźniać) dostawy dla polskiego wojska, powodować wycieki (kradzieże) wrażliwych dla bezpieczeństwa Państwa informacji oraz przyczyniać się do osłabienia zdolności obronnych kraju. Ochrona przed nimi wymaga wdrożenia w przedsiębiorstwach przemysłu obronowego Polsce skutecznych strategii cyberbezpieczeństwa, obejmujących ocenę ryzyka, współpracę z partnerami biznesowymi, zgodność z obowiązującymi przepisami²⁰¹ oraz wdrożenia zaawansowanych technologii i ciągłych innowacji w celu ochrony łańcucha dostaw obronnych przed coraz to nowymi zagrożeniami. Łagodzenie zagrożeń cybernetycznych wymaga holistycznego podejścia, które integruje zaawansowane rozwiązania tech-

200 <https://cyberdefence24.pl/cyberbezpieczenstwo/krakowski-szpital-mswia-zawiadamia-o-naruszeniu-danych>

201 Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw – DZ.U. 2026 POZ. 252

nologiczne, takie jak uwierzytelnianie wieloskładnikowe (MFA), solidne bezpieczeństwo sieci oraz zaawansowane systemy wykrywania zagrożeń, z kluczowymi strategiami skoncentrowanymi na człowieku, takimi jak ciągłe szkolenia pracowników i skuteczne planowanie reagowania na incydenty i odyskiwania danych. Chociaż żadna strategia nie może zagwarantować 100% ochrony, staranne przestrzeganie tych najlepszych praktyk może znacznie zmniejszyć ryzyko.

Regulacje krajowe i unijne, które wpływają na wymogi bezpieczeństwa stawiane dostawcom w sektorze obronnym.

Najistotniejszym aktem prawnym, który kształtuje obowiązki związane z cyberbezpieczeństwem jest Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r., w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dalej: „Dyrektywa NIS2”)[Dyrektywa (UE) 2022/2555]. Rozszerza ona zakres podmiotowy i sektorowy regulacji w porównaniu z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/1148, zwaną dyrektywą NIS1, a ponadto wzmacnia obowiązki dotyczące zarządzania ryzykiem, w tym ryzykiem związanym z łańcuchami dostaw. Wymogi, jakie nakłada Dyrektywa NIS2 dotyczą m.in. obsługi incydentów, ciągłości działania, bezpieczeństwa dostaw, szkoleń, cyberhigieny czy też odpowiednich zabezpieczeń technicznych oraz operacyjnych. W związku z tym, iż reżim dyrektywy unijnej wiąże państwa członkowskie co do celu, polski ustawodawca wprowadzając w życie wymagania przedmiotowej dyrektywy znowelizował ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: „uksc”) poprzez uchwalenie ustawy z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw [Dz.U. 2026 poz. 252]. Podmioty objęte wymogami ustawy podzielone zostały na dwie podstawowe kategorie podmiotów: podmioty kluczowe oraz ważne. Klasyfikacja tych podmiotów odbywa się w oparciu o kryterium sektora, w którym działa podmiot (załączniki do uksc klasyfikują poszczególne sektory na sektory kluczowe lub ważne) oraz kryterium wielkości (co do zasady podmioty średnie i duże, o których mowa w załączniku

I do rozporządzenia Komisji UE nr 651/2014 uznające niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu [Rozporządzenie (UE) 651/2014], działające w sektorach wyszczególnionych w załącznikach do ustawy).

Dostawy sprzętu dla Sił Zbrojnych RP odbywają się przez sieć firm, z których każda ze względu na wielkość oraz charakter działalności może być objęta wymogami przedmiotowej ustawy. Biorąc pod uwagę charakter wyrobów objętych niniejszym raportem, a przede wszystkim poszczególne komponenty, które składają się na uzbrojenie, należy stwierdzić, że producenci tych komponentów mogą być objęci wymogami rzeczzonej ustawy. Załącznik nr 2 do uksc jako sektor ważny, objęty ustawą, wymienia m.in. sektor produkcji – podsektor produkcji komputerów, wyrobów elektronicznych i optycznych. Do tej kategorii mogą należeć podmioty zajmujące się produkcją m.in. elektronicznych obwodów drukowanych, komputerów i urządzeń peryferyjnych, produkcją instrumentów i przyrządów pomiarowych, kontrolnych i nawigacyjnych, które mogą stanowić poszczególne elementy wchodzące w skład przyrządów wykorzystywanych w sprzęcie wojskowym.

W tym miejscu warto podkreślić, że w ustawie wprowadzono szczególne rozwiązanie dotyczące podmiotów podległych oraz nadzorowanych przez Ministra Obrony Narodowej. Zgodnie z art. 5 ust. 10 i 11 uksc ww. podmiotów nie zalicza się automatycznie do podmiotów kluczowych bądź ważnych. MON może jednak, w drodze decyzji niepodlegającej ogłoszeniu, wskazać podległe lub nadzorowane jednostki uznawane za podmioty kluczowe lub ważne. Wyłączenie nie dotyczy jednak automatycznie podmiotów prywatnych, które dostarczają sprzęt lub usługi dla Sił Zbrojnych RP.

Art. 8 ust. 1 pkt. 2 lit. e uksc stanowi, iż podmiot kluczowy lub ważny zobowiązany jest wprowadzić system zarządzania bezpieczeństwem informacji, wdrażający odpowiednie i proporcjonalne środki techniczne i organizacyjne. Środki te powinny uwzględniać m.in. bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględ-

nieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym. Tym samym biorąc pod uwagę tak krytyczne dostawy, jakimi są dostawy dla Sił Zbrojnych RP, nie można skupiać się jedynie na produkcie końcowym. Konieczna jest ocena całego łańcucha dostaw, poczynając od projektowania, po aktualizację, testowanie, utrzymanie, podwykonawstwo, by wreszcie zakończyć na zdolności do raportowania incydentów. Podmioty kluczowe lub ważne nie powinny kierować się wyłącznie ceną, ale powinny również - szczególnie w przypadku dostawców oprogramowania, ocenić, czy dostawca np. w odpowiedni sposób zarządza podatnościami czy też posiada bezpieczne procesy wytwarzania oprogramowania. Z tej perspektywy zasadnym wydaje się wymaganie przy zawieraniu umów z dostawcami uregulowania podstawowych zasad m.in. zapewnienia przez samego dostawcę niezbędnych środków technicznych i organizacyjnych (np. wymagania dotyczące oprogramowania, dostępu, kwalifikacji personelu). W związku z tym należy podkreślić, iż zagrożenie cybernetyczne może powstać w Siłach Zbrojnych w szczególności przez dostawców zewnętrznego oprogramowania, dostawców aktualizacji, czy też usług utrzymania.

Ustawa układa nacisk na ryzyko związane z cyberbezpieczeństwem, natomiast przepisy ustawy Prawo zamówień publicznych z 11 września 2019 r. (dalej: „PZP”) [Dz. U. z 2026 r. poz. 793 ze zm.] dają podmiotom realne możliwości wymagania dokumentacji w zakresie bezpieczeństwa łańcuchów dostaw. W tym przypadku chodzi tu m.in. o art. 408 ust. 1 pkt 3 PZP. Zgodnie z nim: „Zamawiający określa w ogłoszeniu o zamówieniu lub dokumentach zamówienia wymagania związane z realizacją zamówienia w zakresie bezpieczeństwa dostaw. W tym celu zamawiający może żądać złożenia wraz z ofertą dokumentacji gwarantującej, że organizacja i lokalizacja łańcucha dostaw wykonawcy umożliwia mu spełnienie wymagań zamawiającego w zakresie bezpieczeństwa dostaw określonych w ogłoszeniu o zamówieniu lub dokumentach zamówienia, a także zobowiązania do zagwarantowania, że ewentualne zmiany w łańcuchu dostaw w trakcie realizacji zamówienia nie wpłyną negatyw-

nie na zgodność z tymi wymaganiami. PZP nie ustanawia samodzielnych wymagań cyberbezpieczeństwa dla łańcucha dostaw, ale umożliwia ich implementację w postępowaniu zakupowym. Warto w tym miejscu podkreślić również brzmienie art. 417 PZP, który stanowi, iż „w przypadku zamówień w dziedzinach obronności i bezpieczeństwa kryteriami oceny ofert są cena albo cena lub koszt i inne kryteria [...], w szczególności [...] bezpieczeństwo dostaw [...], określone w SWZ. Ustawa PZP daje zatem możliwość wprowadzenia wymogów cyberbezpieczeństwa wobec dostawców dla Sił Zbrojnych RP. Należy przy tym zwrócić uwagę, że PZP w art. 12, przewiduje wyłączenie stosowania ustawy m.in. w przypadku zamówień objętych klauzulą tajności. W takim przypadku ww. mechanizmy nie znajdą zastosowania.

Aktem prawnym, który znacząco wzmacnia wymogi cyberbezpieczeństwa jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi (akt o cyberodporności) (dalej: „CRA”) [Rozporządzenie (UE) 2024/2847]. Omawiana regulacja wymusza uwzględnianie cyberbezpieczeństwa w całym cyklu życia produktów z elementami cyfrowymi, co ma na celu podniesienie standardu oceny dostawców oraz komponentów, które będą wykorzystywane również w łańcuchach dostaw obronnych. CRA ustanawia wymagania dotyczące m.in. projektowania, rozwoju i produkcji produktów z elementami cyfrowymi oraz procesów obsługi podatności w czasie używania produktu, przy czym zasadnicza część jego przepisów będzie stosowana od 11 grudnia 2027 r. W tym miejscu należy pamiętać, iż rozporządzenie przewiduje specjalne wyłączenia z obowiązków dla sektora obronności. Rozporządzenia nie stosuje się do produktów z elementami cyfrowymi opracowanych lub zmodyfikowanych wyłącznie na potrzeby bezpieczeństwa narodowego lub obronności ani do produktów zaprojektowanych specjalnie w celu przetwarzania informacji niejawnych (art. 2 ust. 7 CRA). Oznacza to, że CRA ma znaczenie przede wszystkim dla komponentów komercyjnych, podwójnego zastosowania i produktów ICT włączanych do woj-

skowego łańcucha dostaw, ale niekoniecznie dla każdego zasadniczego sprzętu wojskowego projektowanego wyłącznie dla wojska.

Z perspektywy dostawców zasadniczym postanowieniem jest art. 13 ust. 5 CRA, zgodnie z którym producenci dokładają należytej staranności przy integrowaniu z produktami z elementami cyfrowymi komponentów pochodzących od stron trzecich, aby komponenty takie nie naruszały cyberbezpieczeństwa produktu z elementami cyfrowymi, w tym w przypadku zintegrowania komponentów wolnego i otwartego oprogramowania, które nie zostały udostępnione na rynku w ramach działalności komercyjnej.

Nie mniej istotnym aktem jest ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. [Dz.U. z 2025 r. poz. 1209 ze zm.] Ustawa określa zasady ochrony informacji niejawnych, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkodę dla Rzeczypospolitej Polskiej. W sytuacji, w której konieczne stanie się udostępnienie podmiotowi wykonującemu umowę informacji niejawnych o klauzuli „poufne” lub wyższej będzie musiał on uzyskać świadectwo bezpieczeństwa przemysłowego. Cała procedura w tym zakresie opisana jest w rozdziale 9 – „Bezpieczeństwo Przemysłowe” przedmiotowej ustawy. W związku z wykonywaniem umów dla Sił Zbrojnych RP takie sytuacje mogą mieć wielokrotnie miejsce. Warto podkreślić, że przepisy dotyczące bezpieczeństwa przemysłowego stosowane powinny być także do przedsiębiorców będących podwykonawcami umów. Dostęp do informacji niejawnych o klauzuli „poufne” lub wyższej wiąże się również z wprowadzeniem do umów z podmiotami instrukcji bezpieczeństwa przemysłowego, która określa zasady postępowania z informacjami i materiałami objętymi określoną klauzulą tajności.

Z perspektywy prawa unijnego szczególnym dokumentem jest Rozporządzenie 2021/821 ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania [Rozporządzenie (UE) 2021/821]. Nie jest to dokument ściśle dotyczący cyberbezpieczeństwa, natomiast reguluje on obrót technologiami, oprogramowaniem

i produktami podwójnego zastosowania, które mogą mieć znaczenie dla cyberbezpieczeństwa, kryptografii lub ochrony informacji. Rzeczone rozporządzenie ustanawia system kontroli wywozu, pośrednictwa, pomocy technicznej i transferu produktów podwójnego zastosowania. Produkty podwójnego zastosowania to takie, które mogą mieć zastosowania zarówno cywilne, jak i wojskowe. Załącznik nr I - Rozporządzenie (UE) 2021/821] obejmują m.in. elektronikę, komputery, telekomunikację, czujniki, lasery, nawigację i awionikę. Rozporządzenie wymusza analizę w kontekście tego, co jest przedmiotem obrotu, kto jest odbiorcą, jakie jest końcowe zastosowanie i czy istnieje ryzyko zmiany przeznaczenia produktu.

Przywoływane akty prawne w niniejszej pracy wskazują, że cyberbezpieczeństwo w kontekście łańcuchów dostaw nie może być oceniane wyłącznie przez pryzmat jakości produktu końcowego, ceny lub terminowości zamówienia. Obecnie przepisy prawa coraz silniej akcentują konieczność całościowego, holistycznego zarządzania ryzykiem w łańcuchu dostaw.

Cyberodporność łańcucha dostaw

W tym miejscu warto zwrócić uwagę na perspektywę ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw. Przez to ryzyko należy rozumieć potencjalne szkody, możliwość wystąpienia negatywnych skutków lub naruszenia zasad ochrony danych, które mogą powstać w związku z dostawcami, ich łańcuchami dostaw, a także oferowanymi produktami lub usługami. Rzeczone ryzyko wynika z zagrożeń, które wykorzystują podatności lub luki występujące w produktach, które przemieszczają się w całym łańcuchu dostaw. W praktyce ryzyko cyberbezpieczeństwa materializuje się, gdy zagrożenie — wynikające z działania człowieka lub innych czynników — skutecznie wykorzystuje podatność systemu, produktu, usługi albo elementu ekosystemu łańcucha dostaw [NIST, 2024, str. 71, dostęp 14.07.2026 r.]. Szczególnego znaczenia nabiera zatem właściwe zarządzanie ryzykiem, zwłaszcza w sektorze przemysłu obronnego. O ile bowiem w sektorze komercyjnym zakłócenia w łańcuchu dostaw prowadzą przede wszystkim do strat

finansowych, o tyle w sektorze obronnym mogą bezpośrednio wpływać na zdolności operacyjne państwa, a w konsekwencji stanowić zagrożenie dla jego bezpieczeństwa.

Podmioty sektora przemysłu obronnego powinny zatem identyfikować ryzyka cyberbezpieczeństwa występujące w całym łańcuchu dostaw, uwzględniając zarówno dostawców bezpośrednich, jak i dalszych uczestników tego łańcucha, a następnie włączać rozpoznane ryzyka do ogólnego procesu zarządzania ryzykiem w organizacji. Zgodnie z podejściem określonym w normie NIST SP 800-161r1 Narodowego Instytutu Norm i Technologii Stanów Zjednoczonych [NIST, 2024, str. 449-508, dostęp: 14.07.2026 r.] proces ten obejmuje cztery zasadnicze etapy:

Określanie ram ryzyka – ustalenie kontekstu podejmowania decyzji związanych z ryzykiem, w tym przyjętych założeń i ograniczeń oraz priorytetów organizacji.

Ocena ryzyka – identyfikację i analizę zagrożeń oraz podatności, a także określenie prawdopodobieństwa wystąpienia niepożądanych zdarzeń i ich potencjalnego wpływu na organizację oraz realizację jej zadań.

Postępowanie z ryzykiem – wdrożenie odpowiednich środków zaradczych na podstawie wyników oceny ryzyka.

Monitorowanie ryzyka – ciągłe śledzenie poziomu narażenia organizacji, weryfikację skuteczności zastosowanych zabezpieczeń oraz reagowanie na zmiany zachodzące zarówno w systemach organizacji, jak i w jej łańcuchu dostaw.

Szczególne znaczenia w sektorze przemysłu obronnego nabiera ryzyko wynikające z wykorzystywania zagranicznych komponentów elektronicznych, oprogramowania, firmware'u, usług chmurowych. Łańcuchy dostaw w branży obronnej składają się z wielu poziomów wykonawców. Często główni wykonawcy zlecają produkcję komponentów podwykonawcom, którzy z kolei korzystają z kolejnych dostawców. Stopień skomplikowania jest tak duży, że wiele firm biorących udział w tym procesie może nawet nie mieć świadomości, że są częścią łańcu-

cha dostaw dla wojska [Lucas, R. i inn. (2024)]. Potencjalnym problemem polskiego przemysłu obronnego może być ograniczona widoczność dostawców tzw. drugiego i trzeciego poziomu. Główny wykonawca może formalnie spełniać wymagania zamawiającego, jednak część krytycznych elementów — takich jak komponenty elektroniczne, biblioteki programistyczne, firmware, moduły aktualizacyjne lub usługi chmurowe — może pochodzić od podmiotów, szczególnie z krajów spoza NATO/UE, których poziom bezpieczeństwa nie został realnie zweryfikowany. Rzeczona sytuacja powoduje znaczne trudności w ustaleniu rzeczywistego poziomu bezpieczeństwa produktu końcowego. Wiele organizacji nie ma pełnej kontroli nad systemem dostaw produktów i usług ICT stąd też cyberprzestępcy mogą celowo atakować podwykonawców, aby za ich pośrednictwem uzyskać dostęp do bardziej chronionych organizacji lub infrastruktury krytycznej. W raporcie "EU-NATO Task Force On The Resilience Of Critical Infrastructure" [EU, NATO, 2024, dostęp: 14.07.2026 r.] zaznaczono, iż zagraniczna kontrola nad sektorami technologicznymi, infrastrukturą, materiałami strategicznymi i łańcuchami dostaw może umożliwiać obcym podmiotom pozyskiwanie wrażliwych informacji, zakłócanie dostępu do infrastruktury lub odmowę świadczenia usług.

Stąd też w nowelizacji polskiej ustawy o krajowym systemie cyberbezpieczeństwa znalazły się przepisy o tzw. dostawcach wysokiego ryzyka (art. 67b uksc). W ramach tego mechanizmu minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego może w formie decyzji uznać dostawców konkretnych typów produktów ICT czy rodzajów usług ICT bądź procesów ICT za dostawców wysokiego ryzyka. Skutki takiej decyzji określa art. 67c uksc, który zobowiązuje wskazane w nim podmioty do niewprowadzania objętych decyzją produktów, usług lub procesów do użytkowania oraz do ich wycofania w ustawowych terminach. Ministerstwo Cyfryzacji wskazało, że decyzja wobec dostawcy wysokiego ryzyka ma umożliwiać eliminowanie niebezpiecznego sprzętu lub usług ICT z użycia w podmiotach kluczowych dla funkcjonowania państwa, przy czym de-

cyzja dotyczy dostawcy i określonych produktów, a nie automatycznie wszystkich dostawców z danego państwa [Ministerstwo Cyfryzacji, 2025, dostęp: 14.07.2026 r.]

Wyzwaniem dla polskiego systemu obronnego jest zróżnicowany poziom dojrzałości cyberbezpieczeństwa, w szczególności wśród małych i średnich przedsiębiorstw, będących ogniwami w łańcuchach dostaw. Europejska Agencja Obrony w swoim raporcie „Guidelines for Facilitating SMEs’ Access to the Defence Market” podkreśla, że rola małych przedsiębiorstw w europejskiej bazie technologiczno-przemysłowej sektora obronnego stopniowo wzrastała. Przedsiębiorstwa te działają zarówno jako bezpośredni dostawcy dla ministerstw obrony jak i podwykonawcy w łańcuchu dostaw obronnych [Europejska Agencja Obrony, 2016, str. 3, dostęp: 14.07.2026 r.]. Wśród Małych i średnich przedsiębiorstw występuje najwięcej problemów z zapewnieniem odpowiedniego poziomu cyberbezpieczeństwa. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa ENISA wskazuje, że mierzą się one z niskimi budżetami na cyberbezpieczeństwo, brakiem specjalistycznych kompetencji oraz rosnącą liczbą cyberataków, co może negatywnie wpływać nie na ich konkurencyjność, lecz także na łańcuch dostaw, którego mogą być częścią [ENISA, dostęp 14.07.2026 r.]. W sektorze obronnym taka wada stanowi niebagatelne zagrożenie. Może ona doprowadzić do utraty integralności produktu, opóźnienia dostaw, czy też ujawnienia informacji objętych klauzulą poufności. Stąd też formalna zgodność z przepisami dostawcy końcowego nie daje gwarancji bezpieczeństwa całego łańcucha dostaw. To odbiorca powinien zadbać o to, by podwykonawcy w jak największym stop-

niu ograniczali ryzyko związane z incydentami cyberbezpieczeństwa. W związku z tym w przypadku dostaw krytycznych dla Sił Zbrojnych RP podmioty z sektora obronnego mogłyby wymagać od dostawców m.in.:

- wykazu krytycznych komponentów elektronicznych,
- wykazu wykorzystywanego oprogramowania i bibliotek,
- informacji o kraju pochodzenia komponentów.

Pozwoliłoby to zmapować zamawiającym elementy najbardziej narażone na ewentualny incydent. Jest to podejście promowane przez amerykański Narodowy Instytut Norm i Technologii – NIST. Innym rozwiązaniem mogłoby być pogrupowanie poszczególnych dostawców w zależności od znaczenia – wpływu poszczególnych dostawców towarów lub usług na prawidłowe funkcjonowanie Sił Zbrojnych RP. Dla każdej kategorii podmioty z sektora obronnego mogłyby wymagać innych – mniej lub bardziej restrykcyjnych wymagań dotyczących cyberbezpieczeństwa.

Podsumowując, cyberodporność łańcucha dostaw w sektorze obronnym nie może być utożsamiana wyłącznie ze spełnieniem wymogów regulacyjnych przez wykonawcę końcowego. Wymaga ona całościowego spojrzenia na dostawców, podwykonawców, komponenty elektroniczne, oprogramowanie, usługi ICT oraz zależności od podmiotów zagranicznych. W przypadku dostaw krytycznych dla Sił Zbrojnych RP kluczowe znaczenie ma zdolność do identyfikowania, ograniczania i monitorowania ryzyk występujących na wszystkich poziomach łańcucha dostaw.

5.3. Ocena współzależności infrastruktury fizycznej i cyfrowej

Ocena współzależności infrastruktury fizycznej i cyfrowej w przemyśle obronnym powinna koncentrować się na relacjach między zasobami, a nie na samym katalogu zagrożeń. W polskim systemie ochrony infrastruktury krytycznej chodzi zarówno o systemy rzeczy-

wiste, jak i cybernetyczne oraz funkcjonalnie powiązane obiekty, urządzenia, instalacje i usługi, których zakłócenie może osłabić bezpieczeństwo państwa oraz sprawność administracji i gospodarki. Do tych systemów należą między innymi energetyka, łączność,

sieci teleinformatyczne i transport. Celem ochrony jest nie tylko zapobieganie zakłóceniom, lecz także możliwie szybkie przywrócenie funkcji krytycznych po incydencie.

W realiach polskiego przemysłu obronnego zakład produkcyjny nie jest samodzielnym bytem infrastrukturalnym. Jego zdolność do wytwarzania uzbrojenia, amunicji i komponentów zależy równocześnie od zasilania energetycznego, dostępności łączy telekomunikacyjnych, pracy systemów OT/ICS sterujących procesem technologicznym, działania systemów ERP/MES/WMS, ciągłości magazynowania oraz sprawności transportu drogowego, kolejowego i morskiego. Zależność ta jest wzmacniana przez fakt, że istotna część infrastruktury o znaczeniu krytycznym pozostaje poza bezpośrednią kontrolą resortu obrony, w rękach operatorów cywilnych i podmiotów komercyjnych^{202 203}.

Znaczenie tych powiązań jest szczególnie widoczne w podejściu NATO do odporności. Sojusz uznaje odporność cywilną za warunek wsparcia działań wojskowych i wskazuje siedem bazowych wymagań odporności, obejmujących między innymi energię, łączność i transport. W praktyce oznacza to, że ocena odporności obronnego łańcucha dostaw musi obejmować nie tylko zakłady produkcyjne, lecz także porty, terminale kolejowe, sieci energetyczne, operatorów telekomunikacyjnych, usługi satelitarne, centra danych i dostawców usług cyfrowych, od których zależy ciągłość dowodzenia, logistyki i utrzymania ruchu²⁰⁴.

Najważniejsze współzależności mają charakter krzyżowy. Przerwa w zasilaniu nie zatrzymuje wyłącznie maszyn produkcyjnych, lecz może równocześnie unieruchomić serwerownię, monitoring, system kontroli dostępu, łączność lokalną i część infrastruktury OT. Awaria operatora telekomunikacyjnego albo utrata łączności satelitarnej może odciąć zakład od systemów ERP/MES/WMS, usług chmurowych, zdalnego utrzymania i koor-

dynacji logistycznej. Zakłócenie transportu lub przeładunku nie jest natomiast wyłącznikiem problemem fizycznym, ponieważ bez danych z WMS i ERP magazyn oraz transport tracą wiarygodną informację o stanach, priorytetach i trasach dostaw²⁰⁵.

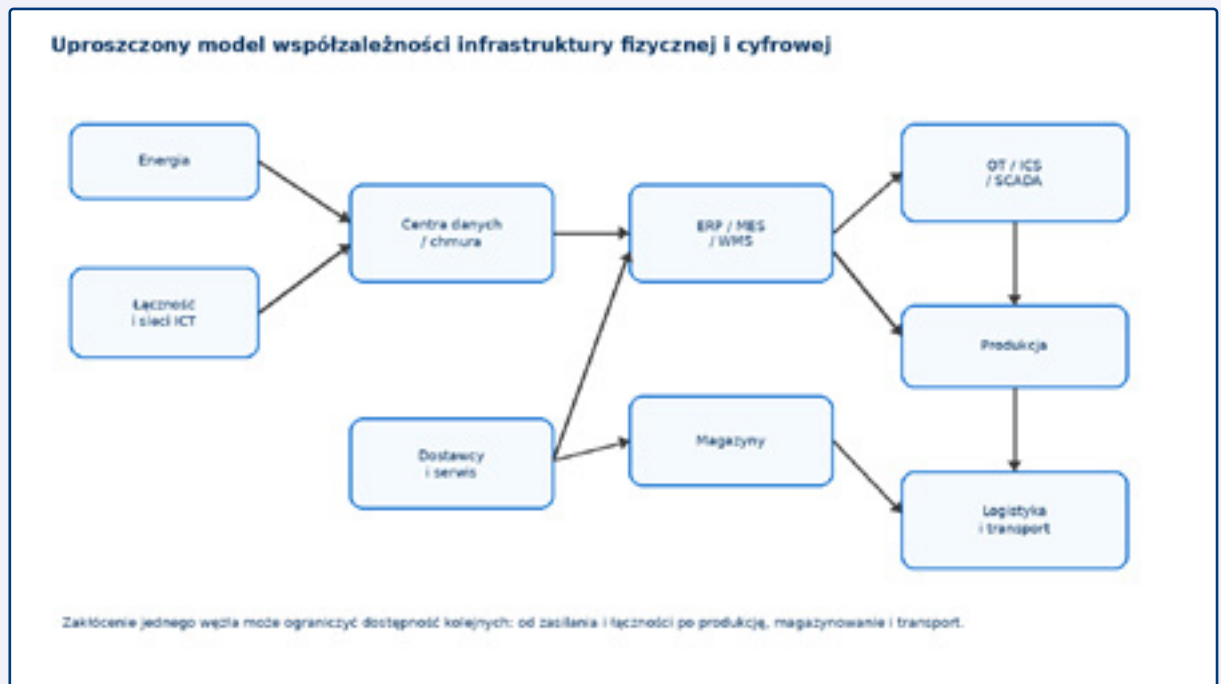
Uproszczony model tych zależności przedstawiono na rysunku poniżej.

202 <https://www.gov.pl/web/rcb/infrastruktura-krytyczna> (dostęp: 02.07.2026 r.).

203 <https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej> (dostęp: 02.07.2026 r.).

204 <https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej> (dostęp: 02.07.2026 r.).

205 https://www.nato.int/cps/en/natohq/topics_132722.htm (dostęp: 02.07.2026 r.).



Rys. 5.2. Uproszczony model współzależności infrastruktury fizycznej i cyfrowej w obronnym łańcuchu dostaw

Identyfikacja ryzyk

Ryzyko w zakresie współzależności infrastruktury fizycznej i cyfrowej oznacza możliwość wystąpienia takiego zakłócenia, które poprzez relacje między energią, telekomunikacją, systemami cyfrowymi, produkcją, magazynami, transportem i dostawcami doprowadzi do utraty ciągłości produkcji, dystrybucji albo serwisu sprzętu wojskowego. W odróżnieniu od klasycznej analizy zagrożeń nie wystarczy wskazać, że istnieje ryzyko cyberataku, awarii zasilania lub sabotażu fizycznego. Konieczne jest wskazanie, przez jakie zależności zakłócenie przenosi się na pozostałe elementy systemu²⁰⁶.

Kluczowe węzły i zależności wymagające oceny odporności przedstawiono w tabeli 5.2. Tabela porządkuje najważniejsze obszary: energię, łączność, systemy ERP/MES/WMS, OT/ICS/SCADA, transport i terminale oraz dostawców krytycznych. Dla każdego węzła wskazano zależności, możliwy efekt kaskadowy i minimalny środek odporności.

²⁰⁶ Yijiang Li, Kibaek Kim, Sven Leyffer, Matt Menickelly, Lawrence Paul Lewis, Joshua Bergerson, Modeling and solving cascading failures across interdependent infrastructure systems, Optimization and Control, 2024

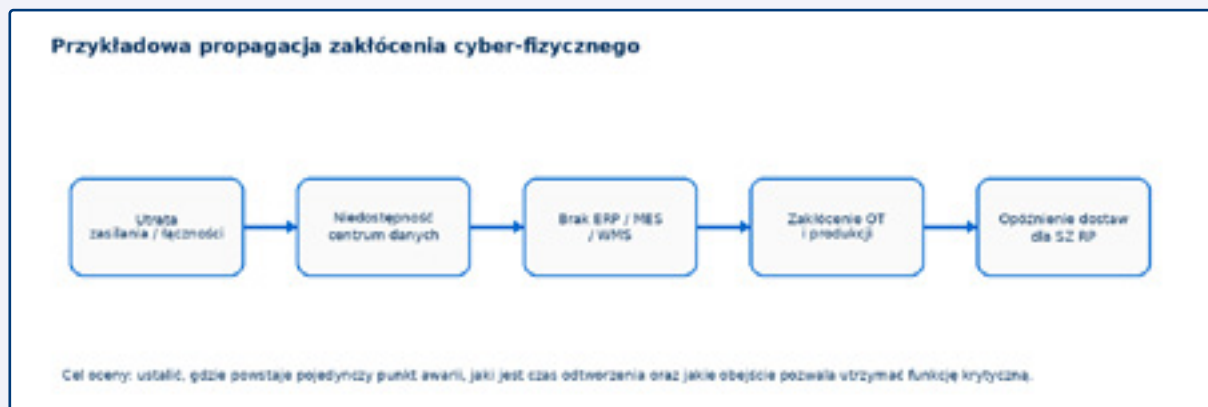
Tab. 5.2. Kluczowe węzły i zależności infrastrukturalne wymagające oceny odporności.

Węzeł krytyczny	Zależności	Możliwy efekt kaskadowy	Minimalny środek odporności
Energia i zasilanie rezerwowe	przylączy, UPS, generatory, paliwo	zatrzymanie produkcji, ICT, OT i ochrony fizycznej	redundancja, testy pracy wyspowej, zapas paliwa
Łączność i sieci ICT	operatorzy telekomunikacyjni, satelita, Internet, VPN	utrata ERP/MES/WMS, zdalnego serwisu i koordynacji logistyki	dwa kanały łączności, procedury offline
ERP/MES/WMS	centra danych, chmura, konta uprzywilejowane	utrata planowania, stanów magazynowych i śledzenia komponentów	kopie offline, procedury ręczne, testy odtworzenia
OT/ICS/SCADA/PLC	sterowanie procesem, sieci przemysłowe, serwis	postój lub produkcja wadliwych partii	segmentacja, tryb manualny, kontrola zmian
Transport i terminale	drogi, kolej, porty, terminale przeładunkowe	opóźnienie dostaw uzbrojenia, amunicji i części	alternatywne trasy, umowy awaryjne, priorytety przewozowe
Dostawcy krytyczni	elektronika, firmware, serwis, komponenty COTS	brak substytutu, przerwanie produkcji lub serwisu	drugi dostawca, zapasy, kwalifikacja bezpieczeństwa

Wnioski z tabeli 5.2 są bezpośrednie: ochrona infrastruktury nie może być ograniczona do ochrony zakładu albo systemu informatycznego. Musi obejmować cały układ zależności, w tym infrastrukturę wspierającą, operatorów zewnętrznych, dostawców usług cyfrowych, transport i serwis. Szczególne znaczenie mają węzły bez realnego obejścia, ponieważ to one decydują o podatności na efekt kaskadowy.

Przykładową propagację zakłócenia cyber-fizycznego przedstawiono na rysunku 5.3. Schemat pokazuje sekwencję: utrata zasilania lub łączności, niedostępność centrum danych, brak ERP/MES/WMS, zakłócenie OT i produkcji, a finalnie opóźnienie dostaw

dla Sił Zbrojnych RP. Taki sposób opisu pozwala odejść od abstrakcyjnego katalogu zagrożeń i przejść do oceny, gdzie powstaje pojedynczy punkt awarii, jaki jest czas odtworzenia i jakie obejście pozwala utrzymać funkcję krytyczną²⁰⁷.



Rys. 5.3. Przykładowa propagacja zakłócenia cyber-fizycznego od infrastruktury wspierającej do dostaw dla Sił Zbrojnych RP

Ocena współzależności powinna obejmować również zagrożenia hybrydowe. Zakłócenie może wynikać z cyberataku, sabotażu fizycznego, długotrwałej przerwy energetycznej, awarii operatora telekomunikacyjnego, katastrofy naturalnej, błędu ludzkiego albo skoordynowanego działania łączącego kilka z tych elementów. Dlatego scenariusze

analityczne powinny obejmować zdarzenia złożone, na przykład jednoczesną utratę zasilania i niedostępność ERP, awarię telekomunikacji połączoną z blokadą transportową, zakłócenie pracy magazynu przy równoczesnym braku dostępu do WMS albo incydent OT występujący w czasie presji na zwiększenie produkcji²⁰⁸.

²⁰⁷ Ibidem.

²⁰⁸ Stouffer, K., Pease, M., Tang, C. Y., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A. i Thompson, M. (2023). Guide to Operational Technology (OT) Security (NIST Special Publication 800-82 Rev. 3). Gaithersburg: National Institute of Standards and Technology.

Minimalny zestaw wskaźników odporności infrastrukturalnej przedstawiono w tabeli 2. Wskaźniki te powinny być wykorzystywane nie jako rozbudowany system sprawozdawczy, lecz jako praktyczne narzędzie priorytetyzacji działań MON, przemysłu i operatorów infrastruktury krytycznej.

Tab. 5.3. Minimalny zestaw wskaźników odporności infrastrukturalnej.

Wskaźnik	Co mierzy	Znaczenie dla MON
Pokrycie mapą zależności	odsetek procesów krytycznych ujętych w mapie	warunek priorytetyzacji ochrony i inwestycji
Liczba pojedynczych punktów awarii	węzły bez realnego obejścia	identyfikacja najbardziej pilnych ryzyk systemowych
Czas odtworzenia funkcji krytycznej	RTO dla energii, ICT, OT, magazynów i transportu	ocena zdolności utrzymania dostaw dla SZ RP
Gotowość pracy degradacyjnej	możliwość działania bez pełnego ERP/WMS/łączności	ograniczenie skutków kaskadowych
Pokrycie testami BCP/DRP	wyniki ćwiczeń odtworzeniowych	weryfikacja, czy procedury działają w praktyce
Ocena dostawców krytycznych	udział dostawców objętych oceną ryzyka	zmniejszenie podatności łańcucha dostaw

Metodyka oceny powinna obejmować pięć działań. Po pierwsze, należy zmapować zależności między zakładami, magazynami, transportem, energetyką, telekomunikacją i systemami cyfrowymi. Po drugie, trzeba wskazać pojedyncze punkty awarii i oszacować ich substytucyjność. Po trzecie, należy zbudować scenariusze kaskadowe dla najważniejszych kombinacji zakłóceń²⁰⁹. Po czwarte, konieczne jest określenie parametrów odtworzenia, w tym czasu przywrócenia funkcji krytycznych, dopuszczalnego okresu pracy w trybie ograniczonym oraz minimalnego poziomu zapasów. Po piąte, należy cyklicznie oceniać dostawców krytycznych oraz zależności od usług komercyjnych²¹⁰.

Narzędzia automatyzacji analitycznej, w tym AI, mogą wspierać wykrywanie anomalii, korelację alertów i budowę obrazu sytuacyjnego, lecz powinny pozostać warstwą pomocniczą. O odporności obronnego łańcucha dostaw decydują przede wszystkim architektura zależności, możliwość pracy degradacyjnej, redundancja, jakość procedur awaryjnych, ćwiczenia oraz zdolność odtworzenia. Wdrożenia AI powinny być stosowane tam, gdzie istnieją wiarygodne dane, jasny proces weryfikacji eksperckiej oraz mechanizm ograniczania fałszywych alarmów²¹¹.

5.4. Wnioski i rekomendacje

Przeprowadzona analiza wskazuje, że bezpieczeństwo łańcuchów dostaw polskiego przemysłu obronnego należy obecnie rozpatrywać jako problem systemowy, obejmujący jednocześnie wymiar technologiczny, organizacyjny, cybernetyczny, przemysłowy i geopolityczny. W warunkach rosnącej cyfryzacji przemysłu obronnego samo zapewnienie bezpieczeństwa produktu końcowego lub bezpośredniego dostawcy nie jest wystarczające. Ryzyko może być generowane na każdym poziomie łańcucha – również przez poddostawców komponentów elektronicznych, oprogramowania, firmware’u, usług ICT, dostawców surowców oraz podmioty znajdujące się na poziomach P3 i P4.

209 Li, Y., Kim, K., Leyffer, S., Menickelly, M., Lewis, L. P. i Bergerson, J. (2024). Modeling and solving cascading failures across interdependent infrastructure systems. arXiv preprint arXiv:2407.16796.
210 Hu, K., Levi, R., Yahalom, R. i Zerhouni, E. G. (2023). Supply Chain Characteristics as Predictors of Cyber Risk: A Machine-Learning Assessment. arXiv preprint arXiv:2210.15785.
International Electrotechnical Commission (2019). IEC 31010:2019 Risk management — Risk assessment techniques. Geneva: IEC.
211 <https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej> (dostęp: 02.07.2026 r.).

Po pierwsze, sztuczna inteligencja może zasadniczo zmienić sposób zarządzania ryzykiem łańcuchów dostaw, ale nie może być traktowana jako samodzielne rozwiązanie problemu odporności. Największy potencjał AI występuje w trzech obszarach: głębokim mapowaniu sieci dostawców, analizie scenariuszy kryzysowych z wykorzystaniem cyfrowych bliźniaków oraz utrzymaniu predykcyjnym. AI może umożliwić przejście od analizy reaktywnej do predykcyjnej, a tym samym wcześniejsze identyfikowanie zagrożeń i przygotowanie wariantów działania.

Po drugie, kluczowym warunkiem wykorzystania AI jest jakość, dostępność i interoperacyjność danych. Obecna silosowość systemów informacyjnych, rozproszenie danych pomiędzy przedsiębiorstwami oraz ograniczona wymiana informacji powodują, że potencjał technologii AI może pozostać niewykorzystany. W praktyce oznacza to, że pierwszym etapem cyfryzacji zarządzania ryzykiem nie powinno być kupowanie zaawansowanych modeli AI, lecz budowa odpowiedniej architektury danych i zasad ich wymiany.

Po trzecie, cyfrowy bliźniak łańcucha dostaw powinien być traktowany jako narzędzie planowania odporności, a nie wyłącznie jako narzędzie informatyczne. Integracja danych produkcyjnych, logistycznych, magazynowych i eksploatacyjnych umożliwia prowadzenie testów typu „co-jeśli” oraz ocenę konsekwencji utraty określonego dostawcy, infrastruktury, komponentu lub szlaku logistycznego. Pozwala to przejść od identyfikowania ryzyka do ilościowej oceny jego wpływu na zdolności operacyjne.

Po czwarte, rozwój utrzymania predykcyjnego może zwiększyć jednocześnie gotowość sprzętu i efektywność wykorzystania zasobów. Analiza danych eksploatacyjnych umożliwia wcześniejsze wykrywanie symptomów zużycia i lepsze planowanie dostaw części zamiennych. Nie powinno to jednak prowadzić do bezrefleksyjnego przenoszenia cywilnego modelu just-in-time do sektora obronnego. W warunkach kryzysu i wojny odporność wymaga utrzymywania odpowiednich zapasów oraz redundancji. AI powinna zatem służyć

do optymalizacji poziomu rezerw, a nie do ich eliminowania.

Po piąte, cyberbezpieczeństwo staje się integralnym elementem bezpieczeństwa dostaw. Cyfryzacja zwiększa powierzchnię ataku, a wykorzystanie podmiotów trzecich, zewnętrznego oprogramowania, aktualizacji i usług utrzymaniowych tworzy dodatkowe punkty wejścia do systemów organizacji. Formalna zgodność wykonawcy końcowego z wymaganiami nie gwarantuje zatem bezpieczeństwa całego łańcucha. Konieczne jest zarządzanie ryzykiem obejmujące także podwykonawców i dalsze poziomy dostaw.

Po szóste, obecne otoczenie regulacyjne daje już podstawy do wdrożenia bardziej rygorystycznego podejścia. NIS2, znowelizowana ustawa o krajowym systemie cyberbezpieczeństwa, przepisy PZP, regulacje dotyczące ochrony informacji niejawnych oraz Akt o cyberodporności tworzą ramy, w których bezpieczeństwo łańcucha dostaw może być uwzględniane nie tylko jako wymóg techniczny, ale również jako element procesu zakupowego i zarządzania ryzykiem. Jednocześnie przepisy nie zastępują aktywnego zarządzania ryzykiem przez zamawiającego.

Po siódme, najważniejszym ograniczeniem nie jest obecnie brak technologii, lecz brak spójnego modelu zarządzania odpornością. AI może wykryć zależność, anomalię lub wąskie gardło, ale samo wykrycie problemu nie tworzy alternatywnego dostawcy, nie buduje zapasu strategicznego i nie zwiększa krajowych zdolności produkcyjnych. Odporność wymaga więc połączenia narzędzi cyfrowych z instrumentami polityki przemysłowej, dywersyfikacją dostaw, redundancją, zapasami strategicznymi oraz rozwojem krajowych zdolności produkcyjnych.

Po ósme, wykorzystanie AI w obszarze bezpieczeństwa wymaga zachowania kontroli człowieka nad decyzjami krytycznymi. Szczególne znaczenie mają ryzyko halucynacji modeli LLM, automation bias, brak wyjaśnialności części modeli oraz ryzyko uzależnienia od zagranicznych dostawców technologii. W konsekwencji AI powinna pełnić funkcję systemu wspierania decyzji, a nie autonomicznego decydenta.

Rekomendacje:

Zbudować centralny system mapowania krytycznych łańcuchów dostaw obronnych

Wszystkie podmioty uczestniczące w łańcuchu dostaw sprzętu wojskowego powinny opracować system umożliwiający mapowanie zależności co najmniej do poziomu P3, a dla komponentów krytycznych również P4. System powinien obejmować nie tylko producentów, lecz także dostawców komponentów elektronicznych, oprogramowania, firmware'u, usług ICT, surowców i usług serwisowych. Docelowym rezultatem powinien być dynamiczny rejestr zależności, wskazujący m.in. pojedyncze punkty awarii, koncentrację geograficzną, brak substytutów oraz zależności od państw wysokiego ryzyka.

Wykorzystać AI do widoczności łańcucha dostaw

Należy wdrożyć rozwiązania AI umożliwiające automatyczne łączenie danych pochodzących z systemów przedsiębiorstw, dokumentacji zakupowej, rejestrów gospodarczych i innych dostępnych źródeł. Celem nie powinno być stworzenie kolejnej statycznej bazy dostawców, lecz ciągłe wykrywanie zmian w strukturze zależności. System powinien automatycznie sygnalizować pojawienie się nowych dostawców, zmianę kraju pochodzenia komponentu, zmianę podwykonawcy, wzrost koncentracji dostaw lub pojawienie się nowego pojedynczego punktu awarii.

Zbudować pilotażowy cyfrowy bliźniak wybranego łańcucha dostaw

Nie należy rozpoczynać od próby stworzenia pełnego cyfrowego bliźniaka całego polskiego przemysłu obronnego. Bardziej racjonalne jest wybranie kilku krytycznych systemów uzbrojenia i przetestowanie rozwiązania na ograniczonej liczbie łańcuchów dostaw. Cyfrowy bliźniak powinien umożliwiać symulowanie m.in. utraty dostawcy, blokady transportu, ograniczenia dostępu do komponentu, cyberataku, awarii infrastruktury krytycznej oraz nagłego wzrostu zapotrzebowania na części zamienne. Wynikiem powinny być konkretne rekomendacje dotyczące

zapasów, alternatywnych dostawców, tras logistycznych i zdolności produkcyjnych.

Wprowadzić obowiązkową ocenę dostawców krytycznych

Należy ustanowić formalny program oceny dostawców krytycznych, obejmujący komponenty, oprogramowanie, firmware, usługi serwisowe oraz elementy, dla których brak jest realnego substytutu. Dla każdej takiej zależności powinny zostać określone: poziom ryzyka, dostępność alternatywnego dostawcy, minimalny poziom zapasu, możliwość szybkiego zastąpienia komponentu oraz możliwość odtworzenia produkcji w kraju lub państwie sojusznicy.

Wprowadzić obowiązkowe wymagania cyberbezpieczeństwa do dokumentacji zakupowej i umów

W dokumentacji zamówień oraz umowach z wykonawcami należy wprowadzić mierzalne wymagania dotyczące co najmniej: ochrony dokumentacji technicznej, zarządzania podatnościami, kontroli dostępu, bezpieczeństwa aktualizacji, obsługi incydentów, ciągłości dostaw oraz bezpieczeństwa podwykonawców.

Wprowadzić obowiązek ujawniania kluczowych podwykonawców i zmian w łańcuchu dostaw

Wykonawca powinien mieć obowiązek wskazywania kluczowych podwykonawców, dostawców komponentów cyfrowych, dostawców oprogramowania oraz istotnych zmian w strukturze łańcucha dostaw w całym okresie obowiązywania umowy. Pozwoli to odejść od modelu, w którym zamawiający zna wyłącznie wykonawcę głównego.

Wprowadzić obowiązek szybkiego raportowania incydentów i podatności

Każdy wykonawca oraz podwykonawca uczestniczący w realizacji dostaw krytycznych powinien być zobowiązany do niezwłocznego raportowania incydentów, podatności, kompromitacji systemów oraz

innych zdarzeń mogących wpłynąć na ciągłość dostaw dla Sił Zbrojnych RP.

Uzależnić poziom wymagań od krytyczności dostawy

Nie powinien obowiązywać jeden, identyczny poziom wymagań dla wszystkich dostawców. Wymagania należy różnicować w zależności od: znaczenia komponentu dla zdolności operacyjnych, poziomu informacji wrażliwych, stopnia zależności od technologii cyfrowych, możliwości zastąpienia dostawcy oraz konsekwencji przerwania dostaw. Takie podejście pozwoli skoncentrować zasoby ochronne na zależnościach o największym znaczeniu dla bezpieczeństwa państwa.

Wprowadzić audyty i testy odporności całego łańcucha dostaw

W przypadku dostawców krytycznych należy ustanowić prawo zamawiającego do przeprowadzania audytów, żądania wyników testów penetracyjnych oraz dokumentów potwierdzających spełnienie wymagań bezpieczeństwa. Dodatkowo powinny być prowadzone cykliczne ćwiczenia odporności obejmujące nie tylko wykonawcę głównego, ale również kluczowych podwykonawców.

Utworzyć wspólny mechanizm wymiany informacji między MON, przemysłem i operatorami infrastruktury krytycznej.

Należy stworzyć stały mechanizm wymiany informacji o zdarzeniach mogących wpływać na produkcję, transport, magazynowanie, serwis i dostawy dla Sił Zbrojnych RP. Powinien on opierać się na jasno określonych progach raportowania, krótkich alertach operacyjnych i wspólnych ćwiczeniach, bez tworzenia nadmiernego obciążenia administracyjnego.

Wdrożyć system mierników odporności łańcuchów dostaw

Ocena odporności nie powinna opierać się wyłącznie na jakościowej analizie ryzyka. Należy wprowadzić ograniczony zestaw mierników obejmujących m.in. pokrycie mapą zależności, liczbę pojedynczych punktów awarii, czas odtworzenia funkcji krytycznej,

zdolność do pracy w warunkach degradacji, pokrycie testami BCP/DRP oraz udział dostawców krytycznych objętych oceną ryzyka.

Wprowadzić minimalny standard ciągłości działania dla zakładów o znaczeniu obronnym

Powinno się ustanowić minimalny, audytowalny standard ciągłości działania dla zakładów, magazynów i innych podmiotów o znaczeniu dla zdolności obronnych państwa. Standard powinien obejmować co najmniej: zasilanie rezerwowe, niezależne kanały łączności, kopie zapasowe przechowywane poza środowiskiem produkcyjnym, możliwość pracy w trybie ograniczonym, ręczne procedury magazynowe i logistyczne, podstawową ewidencję poza systemami online, możliwość odtworzenia krytycznych instancji ERP/MES/WMS oraz okresowe testy odtworzeniowe. Spełnienie standardu powinno być weryfikowane w ramach audytów i ćwiczeń odporności, a jego wymagania różnicowane w zależności od krytyczności danego zakładu lub procesu dla Sił Zbrojnych RP.

Wprowadzić obowiązkowe ćwiczenia cyber-fizyczne obejmujące cały łańcuch dostaw

Ćwiczenia odporności powinny obejmować jednoczesne zakłócenia infrastruktury cyfrowej i fizycznej, w szczególności scenariusze łączące awarię zasilania lub telekomunikacji z incydem w środowisku IT/OT. Ćwiczenia powinny obejmować wykonawcę głównego, kluczowych podwykonawców oraz – w zakresie niezbędnym do oceny efektów kaskadowych – operatorów infrastruktury krytycznej. Należy weryfikować wpływ zakłócenia na produkcję, magazynowanie, transport, systemy ERP/MES/WMS, dostawy komponentów oraz serwis. Wyniki ćwiczeń powinny prowadzić do aktualizacji map zależności, planów BCP/DRP, procedur eskalacji oraz priorytetów inwestycyjnych.

Traktować AI jako narzędzie wspierające decyzje, a nie substytut zarządzania

Każde zastosowanie AI w procesach krytycznych powinno posiadać mechanizm walida-

cji eksperckiej, możliwość odtworzenia podstawy rekomendacji, kontrolę jakości danych oraz nadzór człowieka. Szczególnie wrażliwe decyzje – dotyczące dostawców, relokacji zasobów, zapasów czy zdolności operacyjnych – nie powinny być podejmowane automatycznie wyłącznie na podstawie rekomendacji modelu.

6. ANALIZA POTENCJAŁU POLONIZACJI ŁAŃCUCHÓW DOSTAW DLA KLUCZOWEGO SPRZĘTU WOJSKOWEGO I ŚRODKÓW BOJOWYCH

6.1. Określenie możliwości produkcji podstawowego sprzętu wojskowego przez polski potencjał przemysłowy

Pojęcie **polskiego przemysłu** można definiować na kilka sposobów. W badaniach ekonomicznych, statystycznych i dotyczących bezpieczeństwa państwa najczęściej stosuje się następujące kryteria:

- kryterium lokalizacji działalności produkcyjnej (za polski przemysł uznaje się przedsiębiorstwa prowadzące działalność produkcyjną na terytorium Polski, niezależnie od struktury własnościowej),
- kryterium własności kapitałowej (W węższym znaczeniu polski przemysł tworzą przedsiębiorstwa kontrolowane przez polski kapitał prywatny lub państwowy).
- kryterium wartości dodanej (czyli, jaka część produktu została zaprojektowana, opracowana i wytworzona w Polsce. W takim ujęciu liczy się nie tylko montaż, ale także: działalność badawczo-rozwojowa, projektowanie, własność intelektualna, krajowy łańcuch dostaw).
- kryterium bezpieczeństwa państwa

i przemysłu obronnego. W tym ujęciu w kontekście przemysłu obronnego za polski przemysł najczęściej uznaje się przedsiębiorstwa: posiadające zdolności produkcyjne na terytorium Polski, zdolne do utrzymania produkcji w czasie kryzysu lub wojny, kontrolowane przez polskie podmioty lub państwo, posiadające krajowe kompetencje projektowe i serwisowe. Oznacza to, iż zakład zagranicznej firmy produkujący wyłącznie na podstawie dokumentacji właściciela zagranicznego może być traktowany jako element przemysłu zlokalizowanego w Polsce, ale niekoniecznie jako część krajowych zdolności przemysłowo-obronnych²¹².

W niniejszym opracowaniu za polski przemysł obronny uznaje się zbiór przedsiębiorstw prowadzących działalność produkcyjną na terytorium Rzeczypospolitej Polskiej, posiadających zdolności wytwórcze, kompetencje techniczne oraz zasoby kadrowe umożliwiające tworzenie wartości dodanej w krajowej gospodarce. W przy-

212 Przemysł ten składa się w wąskim znaczeniu z przedsiębiorstw „koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym” zgodnie z ustawą z dnia 13 czerwca 2019 roku Dz. U. 2019 poz. 1214

padku przemysłu obronnego szczególne znaczenie mają krajowe zdolności projektowe, produkcyjne, serwisowe i rozwojowe pozostające pod kontrolą podmiotów działających na terytorium Polski.

Przyjęta definicja jest typowa dla analiz potencjału przemysłowo-obronnego prowadzonych przez NATO, European Defence Agency oraz instytucje zajmujące się odpornością łańcuchów dostaw i bazą przemysłowo-obronną. W takich analizach samo położenie fabryki nie jest wystarczające — liczy się również kontrola technologii, serwisu, dokumentacji i produkcji. Analiza możliwości produkcji podstawowego sprzętu wojskowego przez polski przemysł obronny dotyczy asortymentu ujętego w czterech kategoriach:

- amunicji artyleryjskiej kalibru 155 mm,
- bojowych wozów piechoty (BWP BORSUK),
- systemu amunicji krążącej (WARMATE),
- armatohaubic samobieżnej (AHS KRAB).

W analizie pominięto Armatohaubicę Samobieżną K9 jako reprezentującą model stricte importowy, a jej analiza wykraczałaby poza określoną objętość niniejszego rozdziału.

Analiza asortymentu w kontekście możliwości produkcji wykracza poza prostą odpowiedź o techniczne możliwości produkcji sprzętu. Produkcja jest efektem procesu zachodzącego między odbiorcami i producentami, który, jeśli jest dobrze zarządzany, powoduje długookresowe relacje przekładające się na stały proces unowocześniania dostarczonego sprzętu jak również obniżanie kosztów jego utrzymania w przyszłości. Produkcja podstawowego sprzętu wojskowego przez polski przemysł obronny ma kilka istotnych aspektów. Po pierwsze, efekt makroekonomiczny powoduje powstanie w gospodarce efektów mnożnika inwestycyjnego i konsumpcyjnego, czego efektem jest zwiększenie wielkości PKB i zwiększone generowanie podatków pośrednich i bezpośrednich wpływających do budżetu państwa. Po drugie, polonizacja produkcji asortymentu przez

przemysł obronny powoduje rozwój kompetencji produkcyjnych i efekt uczenia się oraz możliwości prowadzenia prac badawczo-rozwojowych udoskonalających sprzęt, czego efektem może być oferowanie asortymentu partnerom zagranicznym. Istotnym elementem w tym kontekście jest też wchodzenie w łańcuchy kooperacji i dostaw do światowych producentów uzbrojenia. Wchodzenie w taką współpracę powinno być poprzedzone analizą strategiczną, aby nie prowadziła do zaprzestania rozwijania własnych produktów, tak jak miało to miejsce w przypadku umowy na Rosomaka z Patrią. Podsumowując, wchodzenie w łańcuchy kooperacji nie powinno polegać na pozyskiwaniu usług nisko marżowych, kosztownych z punktu widzenia wymagań środowiskowych czy roboczogodzin pracowników, lecz badań rozwojowych i produkcji wysokomarżowych kluczowych komponentów. Niewątpliwie rozwój produkcji podstawowego sprzętu wojskowego przez rodzimy przemysł obronny w istotny sposób może wpłynąć na koszty i czas serwisowania sprzętu, ale tylko wtedy, gdy wolumeny produkcji są wysokie, a marże wysokie. Po trzecie, rodzima produkcja powoduje zwiększenie odporności na zakłócenia zewnętrzne wynikające z różnych warunkowań od wytwarzania poprzez transport jak również zmiany o charakterze geostrategicznym. Te ostatnie w obecnej sytuacji międzynarodowej odgrywają istotną rolę przekładającą się na potencjalną warunkowość dostaw części lub podzespołów lub kompletnych systemów uzbrojenia. Po czwarte, zwiększenie bazy produkcyjnej na wypadek wojny, czego efektem jest zwiększenie kontroli nad produkcją i dostawami sprzętu w tej sytuacji. Celem niniejszej części jest ocena zdolności polskiego przemysłu obronnego do projektowania, produkcji, utrzymania, modernizacji oraz zwiększania skali wytwarzania podstawowego sprzętu wojskowego w warunkach pokoju, co w oczywisty sposób przekłada się na produkcję czasu wojny lub dalszej intensyfikacji wojny hybrydowej. Metodologia niniejszej części została opracowana na podstawie koncepcji suwerenności technologicznej, autonomii strategicznej,

odporności łańcuchów dostaw oraz otwartej autonomii strategicznej²¹³.

Jednostką analizy są poszczególne kategorie uzbrojenia wymienione powyżej. Model badawczy opiera się na pięciu filarach. Pierwszy obejmuje zdolność technologiczną, rozumianą jako możliwość samodzielnego projektowania, rozwijania i modernizacji technologii wojskowych²¹⁴. Drugi dotyczy zdolności produkcyjnych, obejmujących moce wytwórcze, potencjał mobilizacyjny oraz zdolności remontowe. Trzeci filar analizuje suwerenność łańcucha dostaw poprzez identyfikację zależności od zagranicznych dostawców komponentów, materiałów i technologii.²¹⁵ Czwarty filar ocenia dostęp do komponentów krytycznych, takich jak półprzewodniki, optoelektronika, oprogramowanie oraz materiały strategiczne. Piąty filar mierzy odporność strategiczną, czyli zdolność utrzymania produkcji w warunkach embarga, sankcji lub zakłóceń geopolitycznych.²¹⁶

Obecnie przemysł obronny działający w Polsce tworzą zarówno przedsiębiorstwa państwowe, jak i prywatne – krajowe i zagraniczne. Działają one na potrzeby realizacji zamówień krajowych i zagranicznych. Tworzą one ekosystem, czyli strukturę od integratorów krajowych, przez dostawców poziomu 1, 2, 3 i 4. Grupa integratorów systemów (Prime Contractor – dalej: PC), czyli głównych wykonawców kontraktów odpowiedzialnych za cały produkt końcowy. Integrator odpowiada za: projekt końcowy, certyfikację, integrację podzespołów, kontakt z MON, eksport. Poziom 1 dostawców to główni dostawcy strategicznych podsystemów (modułów, podzespołów) np. wieże bezzałogowe, systemy kierowania ogniem, radary, silniki, skrzynie biegów itd. Poziom 2 to dostawcy krytycznych komponentów specjalistycznych - produkują elementy wykorzystywane przez dostawców poziomu 1 np. układy hydrauliczne,

wiązki elektryczne, optoelektronika, elementy radarów itd. Do tej grupy należą często średnie przedsiębiorstwa przemysłowe posiadające specjalistyczne technologie. Z kolei poziom dostawców 3 to dostawcy materiałów i komponentów podstawowych - części produkcyjnych, czyli dostawcy pojedynczych elementów mechanicznych: odlewów, odkuwek, elementów stalowych, elementów z tworzyw sztucznych. Jest to segment, w którym znajduje się duża część polskich firm rodzinnych i regionalnych zakładów przemysłowych. Na końcu poziom 4, czyli dostawcy materiałów w tym surowców krytycznych. Bez nich niemożliwa jest produkcja na wyższych poziomach.

W Polsce stosunkowo dobrze rozwinięte są poziomy 2 i 3, natomiast słabsza pozostaje pozycja na poziomie integratorów (PC) oraz poziom 1, czyli w obszarze: projektowania całych systemów, własnych silników, zaawansowanej elektroniki wojskowej, mikroelektroniki. Najprostsza jest ścieżka przechodzenia poziomu 3 w górę, która polega na eliminowaniu wykonawców zewnętrznych. O skali wyzwania świadczy fakt, iż w przypadku analizowanego asortymentu Bojowych Wozów Piechoty (BWP) BORSUK występują tysiące kooperantów. Według najnowszych danych publikowanych przez Polską Grupę Zbrojeniową oraz media branżowe, PGZ współpracuje z 11 981 kooperantów w całym kraju. Są to zarówno duże przedsiębiorstwa przemysłowe, jak i małe firmy produkcyjne, zakłady usługowe, firmy IT, logistyczne oraz dostawcy materiałów. PGZ nie publikuje oficjalnego podziału wszystkich 11 981 kooperantów według standardu poziomu 1 do 4, jednak na podstawie raportów branżowych i struktury programów zbrojeniowych można oszacować ich rozmieszczenie.

213 Ambroziak Ł. i in., *Dekada bezpieczeństwa ekonomicznego. Od offshoringu do częściowego friendshoringu*, Polski Instytut Ekonomiczny, Warszawa 2022, https://pie.net.pl/wp-content/uploads/2022/09/PIE-Raport_Friendshoring_2022.pdf (dostęp 24 maja 2026).

214 J. Edler, 'Technology Sovereignty of the EU: Needs, Concepts, Pitfalls and Ways Forward', w: *Science, Research and Innovation Performance of the EU 2024*, European Commission, Brussels 2024, s. 428–435.

215 G. Perotto, 'The Legal Framework of the EU Defence Industry and the Pursuit of Strategic Autonomy', *European Papers*, Vol. 8, No. 1, 2023, s. 475–486.

216 OECD, *OECD Supply Chain Resilience Review: Navigating Risks*, OECD Publishing, Paris 2025, rozdz. 3–6., F. Stoelinga, K. van Loon, D. Ellison, R. Stoop, D. Zandee, *Catching Up: Europe's Path to Strategic Autonomy in the Defence Industry*, Clingendael Institute & HCSS, Haga 2026, s. 1–15.

Tab. 6.1. Szacunkowa liczba kooperantów w zależności od poziomu dostawcy w przypadku PGZ S.A.

Poziom	Rola	Szacowany udział
P1	główni dostawcy systemów i modułów	1-3%
P2	dostawcy specjalistycznych komponentów	10-15%
P3	producenci części i podzespołów	40-50%
P4	dostawcy materiałów, usług i półproduktów	35-45%

Oznacza to, że zdecydowana większość polskich kooperantów znajduje się na poziomach 3 i 4, czyli w obszarach: obróbki metali, spawalnictwa, odlewów i odkuwek, przewodów, części mechanicznych, logistyki, usług przemysłowych, materiałów produkcyjnych. W praktyce oznacza to, że spośród prawie 12 tys. kooperantów tylko niewielka część znajduje się na poziomach odpowiadających za technologie krytyczne, natomiast kilka tysięcy przedsiębiorstw uczestniczy w produkcji jako dostawcy komponentów, usług przemysłowych i materiałów.²¹⁷ Zatem polonizacja produkcji niezależnie od analizowanego asortymentu wymaga przechodzenia dostawców krajowych w łańcuchu z poziomów niższych na poziomy wyższe, co będzie powodowało wykonywanie bardziej złożonych produktów wymagających wyższych umiejętności technicznych, technologicznych i organizacyjnych. Jednocześnie dążenie do optymalizacji cenowej łańcucha oznacza zwiększenie konkurencyjności między podmiotami działającymi na różnych poziomach dostawców. Jest to możliwe do uzyskania po

spełnieniu dwóch warunków: zainteresowania przedsiębiorstw uczestnictwem w łańcuchach dostaw dla przemysłu obronnego – czyli wprowadzenie szybkich ścieżek certyfikacji i długoterminowych umów dotyczących współpracy na podstawie analogicznych umów podpisywanych na poziomie integratorów systemów oraz zachowania ogólnego poziomu konkurencyjności polskiego przemysłu. Podsumowując, potencjał produkcji jest możliwy do rozbudowy poprzez włączanie nowych przedsiębiorstw do tej pory nie zainteresowanych tym obszarem działalności w łańcuchy produkcji i dostaw lub/i poprzez rozbudowę zdolności już funkcjonujących przedsiębiorstw w tym obszarze. W obu przypadkach istotną rolę odgrywają procesy inwestycyjne i czas ich realizacji – od uzyskania pozwolenia na budowę, poprzez zapewnienie dostaw energii i ciepła, aż po lokalizację inwestycji. Kolejnym zagadnieniem są technologie. W tabeli poniżej przedstawiono kluczowe zależności technologiczne dla analizowanego asortymentu.

Tab. 6.2. Zestawienie największych zależności technologicznych i przemysłowych Polski w czterech analizowanych segmentach uzbrojenia

Obszar zależności	Amunicja 155 mm	BWP Borsuk	WARMATE	AHS Krab
Silniki	Brak	Wysoka zależność (MTU i pokrewne rozwiązania)	Niska (silniki elektryczne i małe spalinowe)	Wysoka (MTU)
Przekładnie	Brak	Wysoka	Brak	Wysoka
Półprzewodniki	Średnia	Wysoka	Bardzo wysoka	Wysoka
Elektronika specjalistyczna	Średnia	Wysoka	Bardzo wysoka	Wysoka

²¹⁷ <https://portalobronny.se.pl/przemysl-zbrojeniowy/z-pgz-wspolpracuje-11-981-kooperantow-bedzie-ich-znacznie-wiecej-aa-HWrP-Lqie-6ncq.html> (dostęp).

Obszar zależności	Amunicja 155 mm	BWP Borsuk	WARMATE	AHS Krab
Sensory i optoelektronika	Niska	Średnia	Bardzo wysoka	Średnia
Kamery termowizyjne wysokiej klasy	Brak	Średnia	Bardzo wysoka	Średnia
Systemy nawigacji GNSS	Brak	Niska	Wysoka	Niska
Baterie i magazyny energii	Brak	Niska	Wysoka	Niska
Materiały wybuchowe specjalne (RDX, HMX, TNT)	Wysoka	Brak	Średnia	Średnia (przez amunicję)
Nitroceluloza i prochy	Bardzo wysoka	Brak	Brak	Bardzo wysoka
Zapalniki elektroniczne	Wysoka	Brak	Niska	Wysoka
Modułowe ładunki miotające	Bardzo wysoka	Brak	Brak	Brak
Kompozyty zaawansowane	Niska	Średnia	Wysoka	Niska
Metale krytyczne	Niska	Średnia	Wysoka	Średnia
Oprogramowanie krytyczne	Niska	Niska	Niska	Niska (TOPAZ – rozwiązanie krajowe)
System kierowania ogniem	Niska	Niska	Niska	Niska
Integracja systemu	Niska	Niska	Niska	Niska

Na podstawie zestawienia największych zależności technologicznych i przemysłowych Polski w czterech analizowanych segmentach uzbrojenia zidentyfikowano najbardziej krytyczne zależności.

Tab. 6.3. Najbardziej krytyczne zależności według segmentów

Segment	Największe ryzyko
Amunicja 155 mm	Nitroceluloza, prochy wielobazowe, modułowe ładunki miotające, zaawansowane materiały energetyczne, zapalniki analogowe i/lub elektroniczne
BWP Borsuk	Silnik, przekładnia, wybrane komponenty elektroniki i sensory specjalistyczne
WARMATE	Mikroelektronika, półprzewodniki, sensory EO/IR, baterie, odbiorniki GNSS, silniki elektryczne lub/i odrzutowe ²¹⁸
AHS Krab	Napęd (silnik i przekładnia), część podwozia,

Najwyższy poziom suwerenności przemysłowo-technologicznej osiągnięto w przypadku systemu Warmate opracowanego przez Grupę WB. Przedsiębiorstwo odpowiada za architekturę systemu, integrację oprogramowania, transmisję danych oraz współpracę z krajowymi systemami rozpoznania i dowodzenia²¹⁹. Oznacza to, że Polska kontroluje kluczowe kompetencje na poziomie integratora systemu oraz znaczną część technologii pierwszego poziomu. Największe zależności występują w obszarze półprzewodników, kamer termowizyjnych, wybranych

²¹⁸ W przyszłości prawdopodobne jest zastosowanie silników odrzutowych w ewolucji tej konstrukcji.

²¹⁹ WB Group, System Amunicji Krążącej Warmate, <https://www.wbgroup.pl/produkt/system-amunicji-krazacej-warmate/> (dostęp 26.05.2026) WB Group, Warmate Loitering Munitions, <https://www.wbgroup.pl/en/produkt/warmate-loitering-munitions/> (dostęp 26.05.2026)

sensorów i źródeł zasilania. Pomimo tych ograniczeń Warmate należy uznać za jeden z najbardziej samodzielnych technologicznie systemów uzbrojenia produkowanych obecnie w Polsce.

Drugim analizowanym systemem była Armatohaubica Samobieźna Krab. Huta Stalowa Wola odpowiada za integrację systemu, produkcję wieży artyleryjskiej oraz montaż końcowy²²⁰. Atutem jest wykorzystanie krajowego systemu kierowania ogniem TOPAZ (produkcja Grupy WB). Dzięki temu Polska posiada zdolność do samodzielnego utrzymania i rozwijania systemu artyleryjskiego. Jednocześnie występują istotne zależności związane z układem napędowym, przekładniami oraz częścią komponentów podwozia.

Program Bojowego Wozu Piechoty Borsuk jest przykładem budowy krajowych kompetencji w zakresie integracji nowoczesnych platform bojowych. Polska odpowiada za rozwój wieży bezzałogowej, znaczną część elektroniki wojskowej oraz systemów kierowania ogniem²²¹.

Najważniejsze zależności technologiczne dotyczą jednak silników, przekładni oraz części zaawansowanej mikroelektroniki. Oznacza to wysoki poziom suwerenności produkcyjnej, lecz niepełną suwerenność technologiczną. Najniższy poziom samodzielności spośród analizowanych kategorii występuje w przypadku amunicji artyleryjskiej kalibru 155 milimetrów. Polski przemysł posiada zdolności do produkcji korpusów pocisków, części materiałów wybuchowych oraz montażu końcowego. Kluczowe ograniczenia dotyczą jednak nitrocelulozy, prochów wielobazowych, modułowych ładunków miotających oraz zaawansowanych zapalników elektronicznych.

Wnioski i rekomendacje

- najwyższy poziom suwerenności przemysłowo-technologicznej Polsce zbudowało przedsiębiorstwo prywatne Grupa WB w produkcji WARMATE. Armatohaubica Samobieźna Krab oraz Bojowy Wóz Piechoty Borsuk reprezentują wysoki poziom zdolności integracyjnych i produkcyjnych,

jednak nadal pozostają zależne od zagranicznych dostawców napędów oraz części mikroelektroniki. Największe luki występują natomiast w produkcji amunicji artyleryjskiej, gdzie szczególne znaczenie mają materiały energetyczne i chemia specjalistyczna.

- możliwość polonizacji produkcji zbrojeniowej powinna opierać się na szczegółowej analizie kosztów takich działań. Konieczne jest zwiększenie konkurencyjności polskich produktów na rynkach międzynarodowych, ponieważ rynek polski jest za mały, aby utrzymywać zdolności produkcji w czasie pokoju na odpowiednim wymaganym poziomie w przypadku ograniczeń finansowych budżetu oraz wzmocnienie bazy produkcyjnej w całym polskim przemyśle.
- istotnym ograniczeniem jest dostępność do technologii i podpisane w tym zakresie umowy, które mogą ograniczać wprowadzane zmiany w analizowanym asortymencie.
- kwestie mikroelektroniki i półprzewodników wymagają szczególnej uwagi nie tylko w kontekście analizowanego asortymentu, ale również innych istotnych zdolności dla bezpieczeństwa narodowego Polski w kontekście cyberbezpieczeństwa, łączności i sztucznej inteligencji (AI).
- istotnym elementem powinna być zmiana filozofii działania zamawiającego polegająca na zawieraniu umów długoterminowych na produkcję, serwis oraz rozwój systemów. Konieczność elastyczności i zawierania umów ramowych o współpracy wynika z konieczności utrzymania zdolności i dynamicznego rozwoju unowocześniania asortymentu. W tym kontekście obszar polityki zakupowej powinien być poddany analizie i przebudowie w kierunku poprawy efektywności i szybkości działania,

220 Huta Stalowa Wola, 155 mm Samobieźna Haubica Krab, <https://www.hsw.pl/produkty/155-mm-samobiezna-haubica-krab/> (dostęp 26.05.2026) Huta Stalowa Wola, 155 mm Self-Propelled Howitzer Krab, <https://www.hsw.pl/en/offer/155-mm-self-propelled-howitzer-krab/> (dostęp 26.05.2026)

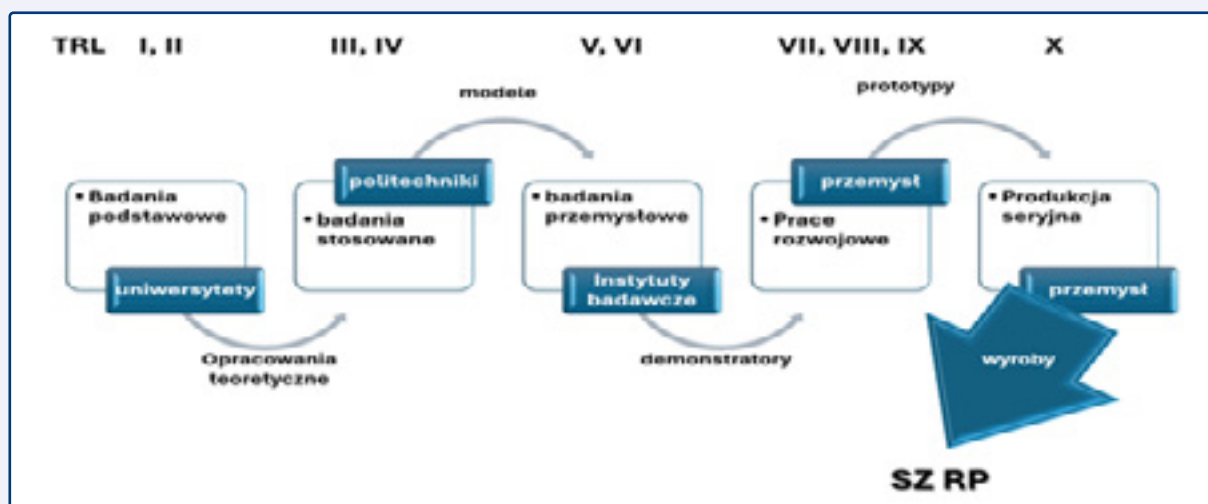
221 Huta Stalowa Wola, Bojowy Wóz Piechoty Borsuk, <https://www.hsw.pl/produkty/howy-bojowy-plywajacy-woz-piechoty-borsuk/> (dostęp 26.05.2026)

- Określenie luk technologicznych nie oznacza konieczności rozwoju własnych technologii. W niektórych przypadkach państwo może przejmować podmioty działające za granicą. Takie działania powinny być agresywne i szybkie, dające pełną kontrolę nad przedsiębiorstwami (co nie oznacza konieczności zakupu 51% akcji lub udziałów). Takie zadania mogą być realizowane lub wspierane przez już funkcjonujące instytucje,
- budowanie silnych więzi „współzależności” z przedsiębiorstwami międzynarodowymi poprzez tworzenie wspólnych projektów, programów rozwojowych, a w szczególności podmiotów JV dedykowanych do produkcji konkretnych produktów,
- zwiększenie penetracji ekonomiczno-technologicznej przedsiębiorstw działających poza granicami kraju w przemyśle obronnym,
- produkcja krajowa może obniżyć koszty serwisowania oraz drastycznie skrócić czas ich realizacji. Składnik serwisu będzie w nadchodzących latach przewyższał koszty ponoszonych obecnie zakupów,
- konieczne jest doprowadzenie do zmiany postrzegania przez przedsiębiorstwa i polityków z USA i Europy Polski nie jako rynku zbytu, lecz jako partnera i lidera technologicznego. Również Międzymorze powinno być naturalnym obszarem działań lobbujących wspartych agresywną dyplomacją publiczną mającą na celu budowę pożądanego wizerunku przemysłu obronnego.

6.2. Ocena potencjału i możliwości zaangażowania uczelni na rzecz rozwoju polskiego przemysłu obronnego

Wzrost nakładów na obronność jest dla Polski szansą na poprawę innowacyjności gospodarki oraz zapewnienie jej dalszego dynamicznego rozwoju. Badania naukowe oraz liczne

przykłady z ubiegłych dekad potwierdzają, że programy badawczo-rozwojowe prowadzone w obszarze obronności przekładają się na innowacje również w sektorze cywilnym²²².



Rys. 6.1. Uogólniony model przepływu technologii nauka-przemysł-wojsko

²²² Marcin Wroński, Karol Bąkowski, Jan Muchorowski, Wzrost nakładów na obronę narodową – szansa na poprawę innowacyjności polskiej gospodarki? Łukasiewicz – Instytut Technologii Eksploatacji Wydawnictwo Naukowe 2025 r.

Uogólniony model przepływu technologii pomiędzy podmiotami naukowymi, przemysłem i wojskiem przedstawiono na rysunku 30. Pewne uproszczenie, jakie przyjęto, to kwalifikacja poziomów gotowości technologicznej (ang. Technology Readiness Level – TRL) do poszczególnych rodzajów podmiotów, która w praktyce ma znacznie bardziej elastyczny charakter. Uczelnie mogą realizować badania w pełnym zakresie 1–6 TRL, podobnie jak instytuty badawcze. Często też instytuty badawcze posiadają zdolności produkcyjne na 9 TRL, np. Sieć Łukasiewicz PIAP czy ITWL, WITU.

Wiodącym przykładem współpracy uczelni z przemysłem obronnym jest Wojskowa Akademia Techniczna, która za opracowane i wdrożone technologie wojskowe i dual-use była wielokrotnie nagradzana. W szczególności należy podkreślić 38 różnych prestiżowych wyróżnień nagrodami Prezydenta RP, Ministerstwa Obrony Narodowej, aż 16-krotne w konkursie Lider Bezpieczeństwa Państwa oraz 21-krotne nagrodą DEFENDER na Międzynarodowym Salonie Przemysłu Obronnego między innymi: laserowy system wykrywania i śledzenia nisko latających obiektów „SkanDron”, autonomiczny pojazd kołowy „Perun”, mobilny wieloczynnikowy system obserwacji, rodzina karabinków MSBS „GROT”, platforma nawodno-powietrzna „DROZD” opracowana przy udziale ITWL i Politechniki Gdańskiej, czy radar RWKO „Sajna” opracowany przez PIT-RADWAR S.A. przy udziale WAT i Politechniki Warszawskiej.

Trwająca od dziesięcioleci współpraca WAT z przemysłem obronnym przyniosła wymierne rezultaty w postaci setek innowacyjnych rozwiązań zaimplementowanych w sprzęcie wojskowym oraz licznych patentów i praw ochronnych. Przykładem tej efektywnej współpracy są prace badawczo-rozwojowe realizowane wspólnie z CRW Telesystem-Mesko Sp. z o.o., w wyniku których powstała seria rozwiązań w obszarze zestawów rakiet przeciwlotniczych bardzo krótkiego zasięgu GROM/PIORUN, należących do sprawdzonych w warunkach bojowych najlepszych tego typu systemów na świecie. Znaczące są

dokonania w obszarze radiolokacji zakończone opracowaniem już wdrożonych lub będących w fazie wdrażania systemów: P18, WARTA, SAJNA opracowanych wspólnie z PIT RADWAR. Nie mniej istotne są także liczne systemy wspierające cyberbezpieczeństwo i kryptologię, wykorzystywane nie tylko w komponencie Wojsk Obrony Cyberprzestrzeni ale i systemach zabezpieczenia krajowej infrastruktury krytycznej. W systemie ciągłym powoływane są zespoły eksperckie WAT, które opracowują na potrzeby SZ RP i podmiotów gospodarczych współpracujących z wojskiem, opinie i ekspertyzy w zakresie zabezpieczenia eksploatacji sprzętu wojskowego, rozwiązań organizacyjnych systemu wsparcia i zabezpieczenia logistycznego, lokalizacji i zabezpieczenia infrastruktury specjalnej i krytycznej itp.

Także bardzo dobrym przykładem współpracy uczelni z przemysłem jest Politechnika Warszawska, która dostarczyła szereg kluczowych technologii dla polskiego przemysłu zbrojeniowego. Innym istotnym obszarem takiej współpracy jest np. radiolokacja, w której widoczna jest pozytywna rywalizacja z WAT.

Modelowym przykładem kooperacji nauka-przemysł jest działalność zespołu profesora Krzysztofa Kulpy z Instytutu Systemów Elektronicznych Wydziału Elektroniki i Technik Informacyjnych PW z PIT-Radwar (PGZ). W roku 2004 zespół ten rozpoczął prace nad przełomową technologią radiolokacji pasywnej PET/PCL. Zaowocowało to stworzeniem demonstratora, a następnie prototypu urządzenia we współpracy z PIT-Radwar. Unikalność tego przedsięwzięcia polegała na wdrożeniu przez krajowy przemysł (PIT-Radwar) dwóch technologii krytycznych, rozwiniętych od poziomu TRL 2 do TRL 6. Aktualnie urządzenie po badaniach kwalifikacyjnych znajduje się w fazie pozyskiwania przez Agencję Uzbrojenia na potrzeby Sił Zbrojnych RP²²³.

Politechnika Warszawska od dziesięcioleci uczestniczy w konsorcjach z PIT-Radwar, realizując projekty radiolokacyjne finansowane ze środków NCBR w tym m.in. Mobilna trój-

223 <https://www.pitradwar.com/oferta/515,projekty-wspolfinansowane-z-narodowego-centrum-badan-i-rozwoju#> dostęp: 17.03.2026 r.

współrzędna stacja radiolokacyjna dalekiego zasięgu (pasmo L, kryptonim „WARTA”, zakończona sukcesem). Bistatyczny radar bardzo dalekiego zasięgu do monitorowania obiektów w przestrzeni kosmicznej (akronim: BiRaKos, w trakcie realizacji inne podmioty SpaceForest Sp. z o.o., XY-Sensing Sp. z).

Na przykładzie tej wieloletniej współpracy można wysnuć wniosek o kluczowym znaczeniu ciągłości kooperacji zespołów projektowych. Przy finansowaniu projektów rozwojowych zasadne jest zapewnienie stałego dopływu zleceń i środków dla zespołów akademickich, co pozwala utrzymać kompetencje badawcze oraz kontynuować prace nad kolejnymi wersjami technologii.

W obszarze technologii obronnych intensywnie współpracuje z przemysłem obronnym (PGZ)²²⁴, z Instytutem Lotnictwa Sieci Badawczej Łukasiewicz oraz Wojskowym Instytutem Technicznym Uzbrojenia²²⁵ w obszarze technologii raketowych, kosmicznych oraz technologii amunicji przeciwpancernej.

Na uwagę zasługuje fakt, że Centrum Zaawansowanych Materiałów i Technologii CEZAMAT Politechniki Warszawskiej powstało z misją przywrócenia w Polsce zdolności do wytwarzania wysokich technologii materiałowych, w tym układów elektronicznych o wysokim stopniu integracji²²⁶. Likwidacja w 1994 roku Naukowo-Produkcyjnego Centrum Półprzewodników „Cemi” oraz Zakładów Wytwórczych Półprzewodników „Tewa” spowodowała, że przez trzy dekady kraj nie był w stanie samodzielnie produkować układów scalonych niezbędnych w obszarze technologii wrażliwych²²⁷. CEZAMAT wyrasta na lidera sektora nowoczesnych technologii elektronicznych i materiałowych. W roku 2026 Centrum podjęło aktywną współpracę z kluczowymi podmiotami sektora obronnego, w tym z firmą PCO S.A. (Grupa PGZ) oraz

Wojskowym Instytutem Techniki Pancernej i Samochodowej przy projekcie systemu gogli noktowizyjnych o powiększonym kącie obserwacji (SOWA) oraz ze spółką AZA-Tech oraz Wojskowym Instytutem Techniki Inżynierskiej przy opracowaniu gogli noktowizyjnych ze zwiększoną głębią pola widzenia (NOKTOR).

W zakresie technologii wytwarzania środków bojowych kluczowym podmiotem PW jest Zakład Mechaniki i Technik Uzbrojenia na Wydziale Mechanicznym Technologicznym. Kompetencje w projektowaniu amunicji przeciwpancernej oraz programowaniu różnych typów. Zakład współpracuje ze spółkami Grupy PGZ, m.in. z Zakładami Mechanicznymi Tarnów, MESKO S.A. oraz Hutą Stalowa Wola. Kooperacja ta może być szczególnie istotna w kontekście produkcji amunicji artyleryjskiej i moździerzowej, na którą, ze względu na obecną sytuację geopolityczną, zapotrzebowanie jest krytycznie wysokie²²⁸. Niemniej, analizując efekty w postaci wyrobów gotowych, należy uznać, że współpraca Politechniki Warszawskiej z PIT RADWAR w obszarze techniki radiolokacyjnej jest modelowa.

Poza Politechniką Warszawską istotną współpracę z przemysłem obronnym prowadzi inne wiodące politechniki. Syntetyczne zestawienie tej działalności przedstawiono w tabeli 6.4.

224 <https://milmag.pl/polska-grupa-zbrojeniowa-zaciesnia-wspolprace-z-politechnika-warszawska/> dostęp 20.03.2026 r.

225 <https://www.biuletyn.pw.edu.pl/Wydarzenia/Wspolpraca-naukowo-badawcza-Wydzialu-MEiL-PW-z-Wojskowym-Instytutem-Technicznym-Uzbrojenia> dostęp 21.03.2026 r.

226 <https://cezamat.pw.edu.pl/o-nas/cezamat/> dostęp 18.03.2026 r.

227 Zob. Szymon Piotrowski, Stan i perspektywy dla sektora półprzewodników w Polsce rozdział w monografii Kierunki usprawnień gospodarki oraz organizacji w aspekcie zarządczym i prawnym red. Michał Flieger Dominik Mączyński, Uniwersytet im. Adama Mickiewicza w Poznaniu Seria Nauki Ekonomiczne Nr 13, Poznań 2024.

228 <https://www.mt.pw.edu.pl/zmitu/Osiagniecia> dostęp 16.03.2026

Tab. 6.4. Zestawienie kluczowych obszarów współpracy przemysł – nauka dla wybranych uczelni wyższych technicznych w kraju

Uczelnie	Kluczowi partnerzy przemysłowi	Główne obszary technologii (specjalizacje)
Wojskowa Akademia Techniczna	PGZ; PIT RADWAR, MESKO, HSW, ZW TARNÓW, FB RADOM, DEZAMET, MASKPOL, BELMA, CTM, BUMAR ŁABĘDY, WZL 2 WZL 1, WZL 4, ROSOMAK NITROCHEM, GRUPA WB Electronics, CREOTECH S.A., LUBAWA S.A., TELDAT, VIGO Photonics S.A., WITU, CRW Telesystem-Mesko Sp. z o.o. i inne	Technologie raketowe, broń skierowanej energii, systemy radiolokacyjne i optoelektroniczne, technologie kosmiczne i telekomunikacyjne, w tym łączność laserowa, technologie kwantowe i sensory, systemy rozpoznania i dowodzenia, systemy walki radio-elektronicznej, cyberbezpieczeństwo, kryptologia, broń lufowa różnych kalibrów, technologie bezzałogowe lądowe i powietrzne, technologie lotnicze, amunicja precyzyjna, materiały energetyczne, pojazdy wojskowe, inżynieria lądowa i budownictwo ochronne, ochrona i przetrwanie na polu walki, technologie wytwarzania przyrostowego.
Politechnika Warszawska	PGZ; PIT RADWAR, MESKO, ZM TARNÓW, HSW inne. WITU, Ł-ILoT, Ł-PIAP	Radiolokacja, technologie raketowe i satelitarne, amunicja klasyczna i uzbrojenie, energia skierowana, optoelektronika.
Politechnika Gdańska	PGZ - CTM S.A. Stocznia Wojenna, Remontowa Shipbuilding, PGZ PIT RADWAR	Technologie morskie: systemy hydrolokacyjne (sonary), niszczyciele min, ochrona portów, robotyka podwodna, radiolokacja.[8]
Politechnika Wrocławska	PGZ, Wojskowe Zakłady Łączności nr 2, PGZ PIT RADWAR, JELCZ S.A., Łukasiewicz PIMOT	Łączność i sensory: radiolokacja, kryptografia, systemy laserowe, mikrosatelity, elektronika wysokich częstotliwości, pojazdy wojskowe.
Politechnika Poznańska	Wojskowe Zakłady Uzbrojenia (WZU), PGZ, WZMot, H. Cegielski-Poznań	Lotnictwo i drony: bezzałogowe statki powietrzne (BSP)[9], inżynieria materiałowa (kompozyty), mechanika pojazdowa.
Politechnika Śląska	BUMAR-ŁABĘDY, Huta Stalowa Wola, Rosomak S.A.	Ciężka mechanika i robotyka: modernizacja wozów bojowych i czołgów, systemy autonomiczne, automatyzacja linii produkcyjnych amunicji.[10]
AGH w Krakowie	PGZ, MESKO S.A., Zakłady Mechaniczne „Tarnów”	Inżynieria materiałowa: nowoczesne pancerze, materiały wybuchowe, inteligentna sensoryka, systemy sterowania.

Technologie podwójnego zastosowania: perspektywa Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie

Kamieniem milowym dla technologii podwójnego zastosowania w AGH było dołączenie (wspólnie z Krakowskim Parkiem Technologicznym, KPT) do NATO DIANA (ang. Defence Innovation Accelerator for the North Atlantic), w którym WAT wykonuje zadania centrum testowego. W ramach tej współpracy AGH wspólnie z KPT utworzyli akcelerator FORT Kraków, który jest jednym z szesnastu centrów inkubacyjnych należących do sieci akceleracyjnej DIANA, jedynym zlokalizowanym na wschodniej flance NATO.

Akceleratorzy te dedykowane są rozwojowi technologii istotnych z punktu widzenia bezpieczeństwa i obronności przez łączenie innowatorów technologicznych z przedstawicielami instytucji wojskowych, zapleczem testowym, oraz mentorami z sektora obronnego, przemysłu, i uczelni wyższych. Do tej pory FORT wsparł siedem międzynarodowych

startupów (AegisX, Alpha Autonomy, Arcani Systems, Mara Solutions, Robotto, Picogrid, Wave Sciences), a do polskich uczestników DIANA należą między innymi IS-Wireless, Blue Armada Robotics, czy Revobeam.

AGH posiada potencjał w następujących obszarach badawczych: cyberbezpieczeństwo, systemy IT, technologie kosmiczne i satelitarne, systemy autonomiczne i robotyczne, materiałoznawstwo. Z perspektywy typowych jednostek pomocniczych uczelni wyższych typu centra transferu technologii (z jaką autor jest związany) należy mieć na uwadze, iż technologie, które posiadają potencjał podwójnego zastosowania i trafiają w obszar zainteresowań wspomnianych wyżej akceleratorów, stają się często utajnione, co wynika z wymogów instytucji uczestniczących w procesie podnoszenia gotowości technologicznej oraz odbiorców. W związku z tym, wiedza oraz możliwość szerszej promocji tych rozwiązań jest ograniczona.

6.3. Analiza ryzyka polonizacji łańcucha dostaw

Analizę ryzyka polonizacji łańcucha dostaw przeprowadzono w oparciu o metodologię PHA (Preliminary Hazard Analysis). Metoda ta należy do grupy systemowych metod identyfikacji i oceny ryzyka stosowanych na wczesnych etapach projektowania, rozwoju oraz eksploatacji systemów technicznych i organizacyjnych. Jej podstawowym celem jest rozpoznanie potencjalnych zagrożeń, określenie możliwych przyczyn ich wystąpienia, oszacowanie skutków oraz wskazanie działań ograniczających ryzyko do poziomu akceptowalnego. Metoda ma charakter przede wszystkim jakościowy, choć może być również wspierana ocenami ilościowymi opartymi na skalach prawdopodobieństwa i skutków²²⁹.

Istotą metody jest systematyczne przejście od identyfikacji zagrożeń do oceny ich znaczenia dla funkcjonowania analizowanego systemu. Analiza rozpoczyna się od określenia granic systemu oraz jego podstawowych funkcji. Następnie identyfikowane są potencjalne źródła zagrożeń wynikające między innymi z awarii technicznych, błędów ludzkich, niewłaściwej organizacji pracy, oddziaływania środowiska zewnętrznego lub zakłóceń logistycznych. Dla każdego zagrożenia określa się możliwe przyczyny wystąpienia oraz potencjalne skutki dla bezpieczeństwa, ciągłości działania lub realizacji założonych celów.²³⁰ W niniejszym opracowaniu poddano analizie zagrożenia technologiczne, kadrowe, finansowe, logistyczne, regulacyjne oraz związane z dostępnością komponentów i surowców strategicznych. Pozwala to na systematyczne określenie ryzyk wpływających na zdolność przemysłu do realizacji zamówień obronnych zarówno w czasie pokoju, jak i w warunkach kryzysu lub konfliktu zbrojnego²³¹.

W zakresie analizowanego asortymentu, jakim jest amunicja artyleryjska kalibru 155 mm, największe ryzyka dotyczą materiałów energetycznych, nitrocelulozy, prochów wielobazowych, modułowych ładunków miota-

jących, zapalników elektronicznych oraz gazogeneratorów (importowanych obecnie ze Słowacji, a produkowanych w Serbii). Produkcja tych komponentów wymaga zaawansowanej infrastruktury chemicznej, wysokich standardów bezpieczeństwa oraz dostępu do specjalistycznych surowców. W przypadku pełnej polonizacji konieczne byłoby stworzenie krajowego ekosystemu dostaw obejmującego zarówno produkcję materiałów energetycznych, jak i rozwój zaplecza badawczo-rozwojowego. Na terenie Polski nie ma poligonu, na którym można testować amunicję o zasięgu co najmniej 38 km. Najdłuższy pas poligonu przeznaczony do celów artyleryjskich znajduje się w Nowej Dębie i ma 23 km długości. Na podstawie doświadczeń ukraińskich konieczne jest zapewnienie obiektu umożliwiającego testy do 60 km. Ryzyko technologiczne jest bardzo wysokie, ponieważ odtworzenie takich zdolności wymaga wielu lat inwestycji. Dodatkowym problemem jest koncentracja światowych dostaw surowców chemicznych. Oznacza to podatność na zakłócenia geopolityczne, ograniczenia eksportowe oraz wzrost cen. Z perspektywy suwerenności przemysłowo-technologicznej jest to obszar o najwyższym poziomie ryzyka spośród wszystkich analizowanych kategorii uzbrojenia. Program Bojowego Wozu Piechoty Borsuk jest przykładem budowy krajowych kompetencji w zakresie nowoczesnych platform bojowych. Polska posiada znaczące zdolności w zakresie integracji systemowej, elektroniki wojskowej oraz konstrukcji pojazdów opancerzonych. Największe wyzwania dotyczą jednak silników, przekładni oraz zaawansowanej mikroelektroniki. Silniki i przekładnie należą do najbardziej wymagających technologicznie komponentów pojazdu. Ich rozwój wymaga wieloletnich doświadczeń przemysłowych, szerokiego zaplecza badawczego oraz dużej skali produkcji. Ryzyko ekonomiczne wynika z wysokich kosztów stworzenia krajowych zdolności przy relatywnie ograniczonej licz-

229 International Electrotechnical Commission, Risk Management – Risk Assessment Techniques, Geneva 2019, s. 71–74.

230 Sam Mannan (red.), Lees' Loss Prevention in the Process Industries, Oxford 2012, s. 1021–1028.

231 United States Department of Defense, System Safety Standard Practice, Washington D.C. 2012, s. 41–44.

bie produkowanych pojazdów. Pomimo tych ograniczeń program Borsuk charakteryzuje się wysokim poziomem krajowej integracji. Obecnie Polska zachowuje zdolność do rozwoju, modernizacji i utrzymania systemu. Dalsza polonizacja powinna koncentrować się na komponentach o najwyższej wartości technologicznej.

Inteligentny System Kierowania do Rażenia Celów Warmate reprezentuje kategorię nowoczesnych systemów bezzałogowych. Wartość systemu wynika przede wszystkim z oprogramowania, integracji, transmisji danych oraz zdolności do działania w środowisku sieciocentrycznym. Największe ryzyko związane jest z półprzewodnikami, sensorami elektrooptycznymi, kamerami termowizyjnymi i źródłami zasilania. Produkcja tych komponentów jest skoncentrowana w niewielkiej liczbie państw. Obecnie Polska posiada kontrolę nad architekturą systemu, oprogramowaniem i integracją. Warmate jest przykładem systemu o najwyższym poziomie suwerenności technologicznej spo-

śród analizowanych kategorii. Dalsze ograniczanie ryzyka wymaga rozwoju kompetencji w zakresie mikroelektroniki, optoelektroniki oraz technologii podwójnego zastosowania.

Armatohaubica Samobieżna Krab stanowi jeden z najbardziej zaawansowanych systemów artyleryjskich produkowanych przez polski przemysł. Krajowe przedsiębiorstwa odpowiadają za integrację systemu, produkcję wieży artyleryjskiej oraz znaczną część wyposażenia. Największe ryzyka dotyczą układu napędowego, przekładni, lufy, podwozia oraz wybranych komponentów elektronicznych. Szczególne znaczenie ma również zależność od dostępności amunicji artyleryjskiej kalibru 155 milimetrów. Oznacza to, że część ryzyk identyfikowanych w sektorze amunicji wpływa bezpośrednio na zdolności bojowe systemu.

Ryzyka polonizacji łańcucha dostaw z perspektywy systemowej przedstawiono w macierzy oceny ryzyka w poniższej tabeli:

Tab. 6.5. Ryzyka polonizacji łańcucha dostaw – podejście systemowe

Zagrożenie	Przyczyna	Potencjalne skutki	P	S	Ryzyko	Działania ograniczające
Niewystarczające kompetencje krajowych dostawców	Brak doświadczenia w produkcji wojskowej	Opóźnienia wdrożeń i spadek jakości komponentów	3	3	9	Programy certyfikacji i transfer technologii
Brak krajowych odpowiedników komponentów krytycznych	Uzależnienie od zagranicznych technologii	Utrzymanie zależności importowej	3	3	9	Rozwój technologii krajowych i wspólne projekty badawcze
Wzrost kosztów produkcji	Mniejsza skala produkcji krajowej	Spadek konkurencyjności cenowej	3	2	6	Długoterminowe kontrakty i wsparcie inwestycyjne
Niedobór specjalistów technicznych	Luka pokoleniowa i konkurencja sektora cywilnego	Ograniczenie zdolności produkcyjnych	3	3	9	Programy stypendialne i współpraca z uczelniami
Niedostateczne moce produkcyjne dostawców	Wieloletnie zaniedbania inwestycyjne	Brak możliwości zwiększenia produkcji podczas kryzysu	3	3	9	Rozbudowa infrastruktury produkcyjnej
Niepowodzenie transferu technologii	Ograniczenia licencyjne i własność intelektualna	Brak pełnej polonizacji produktu	2	3	6	Negocjowanie pełnych praw technologicznych
Ryzyko finansowe nowych inwestycji	Wysokie koszty uruchomienia produkcji	Utrata płynności przedsiębiorstw	2	3	6	Finansowanie państwowe i fundusze unijne

Zagrożenie	Przyczyna	Potencjalne skutki	P	S	Ryzyko	Działania ograniczające
Niewystarczająca liczba zamówień	Niepewność zakupów obronnych	Nieopłacalność inwestycji produkcyjnych	3	3	9	Wieloletnie programy zakupowe
Zakłócenia dostaw surowców strategicznych	Import metali ziem rzadkich i materiałów specjalnych	Ograniczenie produkcji krajowej	2	3	6	Rezerwy strategiczne i dywersyfikacja dostaw
Niska zdolność do współpracy w ekosystemie przemysłowym	Słaba integracja przedsiębiorstw	Wzrost kosztów i wydłużenie procesów	2	2	4	Rozwój klastrów przemysłowych
Zagrożenia cybernetyczne	Cyfryzacja produkcji i logistyki	Zakłócenie procesów produkcyjnych	3	3	9	Rozbudowa systemów cyberbezpieczeństwa
Długie procesy inwestycyjne	Brak planów zagospodarowania przestrzennego, długie procedury	Przedłużanie procesów inwestycyjnych i wysokie CAPEX	3	3	9	Deregulacja procesów inwestycyjnych
Wysokie koszty energii, szczególnie dla przedsiębiorstw energochłonnych	Dysfunkcje rynku energii w Polsce	Niska konkurencyjność produktów	3	3	9	Obniżenie cen energii elektrycznej i gazu; zastosowanie nowych nośników energii, np. wodoru.
Słabość zarządcza sektora publicznego oraz przedsiębiorstw kontrolowanych przez Skarb Państwa	Kultura organizacyjna	Brak wymaganej elastyczności i szybkości działania	3	3	9	Wzmocnienie możliwości analitycznych sektora publicznego, wprowadzenie kodeksu menedżerskiego w przedsiębiorstwach kontrolowanych przez Skarb Państwa oraz Korpusu Menedżerów
Ograniczenia regulacyjne UE	Wymogi konkurencyjności i zamówień publicznych	Utrudnienia w preferowaniu dostawców krajowych	2	2	4	Dostosowanie instrumentów wsparcia do regulacji UE

Źródło: opracowanie własne²³²

Analiza wskazuje, że najwyższy poziom ryzyka związany z polonizacją łańcucha dostaw dotyczy ośmiu obszarów:

- Niedoboru kompetencji technicznych i inżynierskich oraz trudności w szybkim uzyskaniu zdolności operacyjnych nowych zespołów inżynierskich.
- Braku krajowych technologii i komponentów krytycznych.
- Niewystarczających mocy produkcyjnych przedsiębiorstw krajowych.
- Niepewności długookresowego finanso-

wania i zamówień obronnych.

- Zagrożeń cybernetycznych związanych z cyfryzacją procesów produkcyjnych.
- Słabości zarządczej i niewystarczającej elastyczności i szybkości działania zarówno przemysłu jak również różnych instytucji państwowych, w tym certyfikujących, czego efektem jest niewystarczająca szybkość działania w zakresie zmian założeń sprzętu w obliczu nowych technologii i doświadczeń pola walki.
- Zbyt duży poziom skomplikowania procedur koncesyjnych, certyfikacyjnych,

²³² Macierz oceny ryzyka. Przyjęto następującą skalę: Prawdopodobieństwo wystąpienia:

1), Średnie (2), Wysokie (3) Skutki: Niskie (1), Średnie (2), Wysokie (3)

Poziom ryzyka = Prawdopodobieństwo × Skutki

Wynik Ocena: 1–2 Niskie, 3–4 Średnie, 6 Wysokie, 9 Krytyczne

środowiskowych i inwestycyjnych (plany zagospodarowania przestrzennego, podłączenia energii elektrycznej i ewentualnie ciepła).

- Duże prawdopodobieństwo braku właściwej integracji służb specjalnych w procesy polonizacji produkcji uzbrojenia zarówno w zakresie ochrony przed np. dezinformacją, dyskredytacją kadry zarządzającej i aktywnym pozyskiwaniem technologii i rozwiązań.

Wyniki te są zgodne z ustaleniami raportu, który podkreśla znaczenie rozwoju kompetencji technologicznych, zwiększania nakładów na działalność badawczo-rozwojową, rozbudowy infrastruktury produkcyjnej, budowania partnerstw przemysłowych, ograniczania zależności od importowanych technologii i komponentów oraz sposobu zarządzania.

Dalsza szczegółowa analiza polonizacji łańcucha dostaw w zakresie analizowanego asortymentu z podziałem na poziomy dostawców od poziomu dostawców 1 do poziomu dostawców 4 zgodnie z metodologią PHA prowadzi do następujących wniosków.

W zakresie amunicji 155 mm na poziomie dostawców P1 zidentyfikowano krytyczne produkty takie jak prochy, zapalniki, gazogeneratory, komponenty chemiczne. Przyczynami tego stanu są: ograniczenia technologiczne, brak mocy produkcyjnej, dostawcy spoza UE, koncentracja produkcji i brak inwestycji. Konieczne jest również podkreślenie opóźnień i wysokich kosztów realizacji inwestycji, co wynika z quasi-monopolistycznego rynku wytworzonego przez system formalnych i nieformalnych powiązań instytucji, przedsiębiorstw i osób. W zakresie armatohaubicy Krab na poziomie dostawców P1 zidentyfikowano krytyczne produkty takie jak: napęd, optoelektronika, elektronika specjalna, produkcja luf. Przyczynami tego stanu są: import technologii, wysokie bariery technologiczne, brak krajowych zdolności produkcji, uzależnienie od importu z Azji, ograniczenia licencyjne, pojedynczy dostawcy. W zakresie bojowych wozów piechoty Borsuk na poziomie dostawców P1 zidentyfikowano krytyczne produkty takie jak: napęd, elektronika, sensory optoelektroniczne. Przyczynami tego stanu są wysokie bariery wejścia na ry-

nek, ograniczone kompetencje oraz koncentracja dostaw u pojedynczych dostawców. W zakresie Warmate na poziomie dostawców P1 zidentyfikowano krytyczne produkty takie jak: mikroelektronika, sensory EO/IR, układy nawigacyjne, procesory i komponenty półprzewodnikowe, silniki odrzutowe. Przyczynami tego stanu są: bariery technologiczne i ograniczone kompetencje. Z perspektywy polityki przemysłowej państwa i rozwoju polonizacji łańcuchów dostaw analiza PHA wskazuje, że największą redukcję ryzyka dla wszystkich czterech asortymentów przyniosłaby budowa krajowych zdolności w zakresie: elektroniki wojskowej, optoelektroniki, materiałów energetycznych (prochy i materiały wybuchowe) oraz napędów wojskowych, ponieważ są to wspólne krytyczne obszary P1 występujące w większości analizowanych systemów.

Przejście do analizy niższych poziomów dostawców P2, P3 i P4 jest kluczowe. Poziom dostawców P3 i P4 jest uznawany za poziom krytyczny, ponieważ obejmuje surowce, materiały podstawowe, technologie bazowe i infrastrukturę przemysłową, bez których nie można funkcjonować ani poziom 2, ani poziom 1. Właśnie na poziomach dostawców 2 i 3 występuje większość rzeczywistych zależności strategicznych, których często nie widać na poziomie integratora.

W zakresie amunicji 155 mm na poziomie dostawców zidentyfikowano krytyczne produkty takie jak: nitroceluloza, nitrogliceryna, bawełna strzelnicza, prekursorzy chemiczne, stal stopowa do korpusów, elementy precyzyjne zapalników, materiały polimerowe, na niższych bawełna przemysłowa, kwas azotowy, kwas siarkowy, celuloza specjalna, miedź, cynk, nikiel, energia elektryczna, gaz ziemny. W zakresie armatohaubicy Krab na poziomie dostawców P2 zidentyfikowano krytyczne produkty takie jak: stal wysokowytrzymała, elementy chromowania luf, matryce termowizyjne, procesory, moduły elektroniczne, serwomechanizmy. Na niższych poziomach krzem metalurgiczny, gazy techniczne, metale krytyczne w tym metale ziem rzadkich, aktynowce, wolfram, molibden, chrom oraz energię elektryczną. W zakresie bojowych wozów piechoty BWP Borsuk na poziomie dostawców P2 zidentyfikowano krytyczne

produkty takie jak: wtryskiwacze, turbosprężarki, łożyska, układy sterowania silnikiem, sensory optoelektroniczne, procesory, pancerz ceramiczny. Na niższych poziomach dostawców: tlenek glinu, węgiel krzemu, tytan, metale krytyczne w tym metale ziem rzadkich, aktynowce, miedź elektrotechniczna, krzem. W zakresie Warmate na poziomie

dostawców P2 i P3 zidentyfikowano krytyczne produkty takie jak: mikroprocesory, układy FPGA, matryce podczerwieni, żyroskopy MEMS, akcelerometry, moduły kryptograficzne, ogniwa litowo-jonowe, a P4 wafle krzemowe, gal, german, ind, arsenek galu, neodym, dysproz, lit, kobalt.

Tab. 6.6. Zbiorcza ocena ryzyka polonizacji

Asortyment	Dominujące ryzyko P1	Dominujące ryzyko P2	Dominujące ryzyko P3/4
Amunicja 155 mm	Prochy i zapalniki	Nitroceluloza i chemia specjalna	Bawełna strzelnicza, energia, chemikalia
Krab	Napęd, elektronika	Matryce termowizyjne, procesory	Wolfram, molibden, metale ziem rzadkich
Borsuk	Napęd i sensory	Elektronika i pancerz	Krzem, ceramika specjalna, metale ziem rzadkich
Warmate	Komputer pokładowy i EO/IR	FPGA, MEMS, sensory	Gal, german, ind, lit, krzem

Źródło: opracowanie własne²³³

Wnioski i rekomendacje

Podsumowując poziom dostawców P1 determinuje zdolność montażu i integracji systemów uzbrojenia, poziom P2 determinuje zdolność wytwarzania kluczowych komponentów, natomiast poziom P3 i 4 determinuje rzeczywistą autonomię strategiczną państwa (upraszczając pomijając zagadnienia infrastruktury, finansowania, cyberbezpieczeństwa, kadr, prawa, zapasów i dywersyfikacji). O ile Polska posiada realne możliwości osiągnięcia wysokiego poziomu polonizacji na poziomie P1, a częściowo również P2, to pełna polonizacja P3 i P4 jest wyzwaniem ze względu na zależność od globalnych rynków surowców krytycznych, materiałów specjalnych oraz półprzewodników. Pełna polonizacja dostawców P1 jest możliwa w perspektywie średnioterminowej, natomiast pełna polonizacja P2 wymagałaby odbudowy lub stworzenia w Polsce kompetencji w sektorach chemii specjalnej, mikroelektroniki, optoelektroniki oraz zaawansowanych materiałów, co oznacza konieczność prowadzenia długookresowej polityki przemysłowej wykraczającej poza sektor obronny. Tym samym

obecne wyzwania strategiczne uzasadniają konieczność szerszego uwzględnienia w strategii rozwoju Polski potrzeb i korzyści, jakie może przynieść rozwój sektora obronnego w rozwoju gospodarczym Polski w średnio- i długoterminowej strategii rozwoju. Na poziomie P3 Krab jest przede wszystkim zależny od globalnych rynków metali krytycznych (patrz szerzej R 2.3). Warmate na poziomie P3 i P4 jest najbardziej zależny od globalnych łańcuchów dostaw surowców krytycznych i półprzewodników. Warto podkreślić, iż analiza pokazuje jedynie obszary możliwego działania, potrzeb w dążeniu do zwiększenia odporności jednak pomija kwestie kosztów takich działań. Jednocześnie zwiększenie odporności może polegać również na innych działaniach zarządczych, poszukiwaniu rozwiązań zgodnie z metodologią VRIO lub też budowy współzależności co może okazać się bardziej efektywnym rozwiązaniem. Polonizacja łańcucha dostaw jest środkiem, a nie celem do osiągnięcia efektów makroekonomicznych oraz zwiększenia odporności i w tym kontekście powinna być postrzegana. Brak rygorystycznej i ciągłej analizy kosztów, dynamiki i elastyczności stanowi jedno

233 Macierz oceny ryzyka. Przyjęto następującą skalę: Prawdopodobieństwo wystąpienia: Niskie (1), Średnie (2), Wysokie (3) Skutki: Niskie (1), Średnie (2), Wysokie (3)
Poziom ryzyka = Prawdopodobieństwo × Skutki
Wynik Ocena: 1–2 Niskie, 3–4 Średnie, 6 Wysokie, 9 Krytyczne

z trzech kluczowych ryzyk obok ryzyka braku stabilnego (długoterminowego) portfela zamówień państwowych oraz ryzyka braku skutecznego transferu technologii umożliwiającego przejście od montażu licencyjne-

go do samodzielnego projektowania i produkcji kluczowych systemów uzbrojenia oraz ryzyka utraty konkurencyjności całego przemysłu szczególnie w zakresie zaopatrzenia w energię.

6.4. Wnioski i rekomendacje

Przeprowadzona analiza wskazuje, że Polska posiada istotny, lecz niepełny potencjał do budowy suwerennych zdolności przemysłowo-technologicznych w zakresie produkcji, utrzymania i rozwoju podstawowego sprzętu wojskowego. Największym atutem krajowego przemysłu jest zdolność do integracji systemów, produkcji wielu komponentów oraz rozwinięta baza przedsiębiorstw działających na poziomach P2–4. Jednocześnie zasadnicza luka występuje na poziomie PC i P1, w szczególności w zakresie własnych napędów, zaawansowanej elektroniki, mikroelektroniki oraz części technologii materiałowych. Oznacza to, że samo zwiększanie liczby krajowych dostawców nie będzie wystarczające do osiągnięcia rzeczywistej autonomii strategicznej.

- zachowanie kontroli nad kluczową dokumentacją, własnością intelektualną i architekturą systemu;
- możliwość zwiększenia produkcji w sytuacji gwałtownego wzrostu zapotrzebowania.

W konsekwencji decyzja o polonizacji każdego komponentu powinna być poprzedzona analizą koszt-ryzyko-korzyść. W przypadku części technologii bardziej efektywnym rozwiązaniem może być utrzymywanie strategicznej współzależności z wiarygodnym partnerem zagranicznym, dywersyfikacja dostawców lub uzyskanie kontroli kapitałowej i technologicznej nad zagranicznym przedsiębiorstwem.

1. Polonizacja powinna być traktowana jako instrument odporności, a nie cel sam w sobie.

Najważniejszym wnioskiem z analizy jest konieczność odejścia od utożsamiania polonizacji z maksymalizacją krajowego udziału w każdym elemencie łańcucha dostaw. Pełna krajowa produkcja wszystkich komponentów nie jest ani technicznie, ani ekonomicznie możliwa i nie zawsze jest racjonalna z punktu widzenia bezpieczeństwa państwa. Celem polityki przemysłowo-obronnej powinno być zapewnienie takiego poziomu krajowej kontroli nad łańcuchem dostaw, który umożliwi:

- utrzymanie produkcji w warunkach kryzysu i wojny;
- zapewnienie dostępu do części zamiennych i usług serwisowych;
- modernizację i rozwój posiadanych systemów;
- ograniczenie ryzyka przerwania dostaw przez decyzje państw trzecich;

2. Priorytetem powinno być przechodzenie z poziomów P2–P4 do P1 oraz budowanie kompetencji PC

Polski przemysł posiada szeroką bazę przedsiębiorstw funkcjonujących na niższych poziomach łańcucha dostaw. Szacunki przedstawione w analizie wskazują, że zdecydowana większość kooperantów PGZ funkcjonuje na poziomach P3 i P4, podczas gdy udział przedsiębiorstw dostarczających kompletne moduły i systemy jest znacznie mniejszy. Dlatego polityka polonizacji powinna zostać ukierunkowana nie tylko na zwiększanie liczby krajowych dostawców, lecz przede wszystkim na podnoszenie ich pozycji technologicznej w łańcuchu wartości. Oznacza to konieczność:

- wspierania inwestycji umożliwiających przechodzenie przedsiębiorstw z P3 do P2;
- tworzenia krajowych dostawców kluczowych modułów P1;
- rozwijania zdolności projektowania całych systemów na poziomie PC;

- wspierania krajowej własności intelektualnej;
- rozwijania kompetencji konstrukcyjnych, integracyjnych i systemowych;
- tworzenia warunków do eksportu produktów opracowanych w Polsce.

To właśnie przesunięcie przedsiębiorstw w górę łańcucha wartości powinno być jednym z podstawowych mierników skuteczności polityki polonizacyjnej.

3. Najwyższy priorytet należy nadać kilku krytycznym lutom technologicznym

Analiza wskazuje, że poszczególne systemy uzbrojenia charakteryzują się odmienną strukturą zależności. W przypadku amunicji 155 mm największe ryzyko związane jest z nitrocelulozą, prochami wielobazowymi, modułowymi ładunkami miotającymi i specjalistycznymi zapalnikami. W przypadku Borsuka kluczowe pozostają napędy, przekładnie oraz wybrane komponenty elektroniki. W przypadku Warmate szczególne znaczenie mają półprzewodniki, sensory EO/IR, baterie i odbiorniki GNSS, natomiast w przypadku Kraba – przede wszystkim napęd, przekładnia oraz wybrane komponenty podwozia i technologie materiałowe. Rekomendowane jest zatem odejście od rozproszonego wspierania wszystkich technologii na rzecz tzw. krajowej mapy technologii krytycznych, obejmującej co najmniej:

- materiały energetyczne i chemię specjalną;
- napędy i przekładnie;
- półprzewodniki i mikroelektronikę;
- optoelektronikę i sensory;
- zaawansowane materiały;
- technologie magazynowania energii;
- wybrane materiały i surowce krytyczne.

Dla każdego z tych obszarów należy określić cel technologiczny, horyzont czasowy, budżet oraz wskazanego właściciela programu.

4. Mikroelektronika powinna być traktowana jako technologia horyzontalna

Szczególne znaczenie należy przypisać mikroelektronice, ponieważ zależność od półprzewodników nie dotyczy jednego systemu uzbrojenia, lecz praktycznie całej współczesnej architektury bezpieczeństwa państwa. Problem ten obejmuje jednocześnie obronność, cyberbezpieczeństwo, łączność, sztuczną inteligencję, systemy rozpoznania oraz technologie bezzałogowe. Dlatego rozwój krajowych zdolności mikroelektronicznych nie powinien być traktowany wyłącznie jako element polityki obronnej. Powinien stać się elementem szerszej polityki przemysłowej i technologicznej państwa. W krótkim okresie priorytetem powinno być zapewnienie dostępu do komponentów, dywersyfikacja dostaw i budowanie zapasów strategicznych. W średnim okresie – rozwój krajowych zdolności projektowych, testowych i integracyjnych. W długim okresie – budowa wybranych zdolności produkcyjnych tam, gdzie ich znaczenie strategiczne uzasadnia poniesienie wysokich nakładów.

5. W przypadku surowców krytycznych należy stosować model odporności, a nie dążyć do pełnej samowystarczalności

Analiza P3 pokazuje, że pełna polonizacja jest szczególnie trudna w przypadku surowców krytycznych, półprzewodników i materiałów specjalnych. Krab pozostaje zależny m.in. od globalnych rynków metali strategicznych, natomiast Warmate od globalnych łańcuchów dostaw półprzewodników i surowców krytycznych. W tych obszarach Polska nie powinna dążyć do autarkii. Należy natomiast budować „wielowarstwową odporność”, obejmującą:

- dywersyfikację geograficzną dostaw;
- strategiczne zapasy wybranych materiałów;
- dostęp do alternatywnych dostawców;
- rozwój recyklingu i odzysku materiałów;
- udział w europejskich i sojuszniczych łańcuchach dostaw;
- zawieranie długoterminowych umów dostaw;
- inwestycje kapitałowe w zagraniczne

aktywa surowcowe i technologiczne.

6. Polityka zakupowa MON powinna zostać powiązana z polityką budowy zdolności przemysłowych.

Jednym z podstawowych warunków utrzymania krajowych zdolności produkcyjnych jest stabilny i przewidywalny portfel zamówień. W przypadku przemysłu obronnego nie można ograniczać się do logiki jednorazowego zakupu sprzętu. Rekomendowane jest przechodzenie w kierunku wieloletnich umów obejmujących cały cykl życia produktu tj.:

projektowanie → produkcja → modernizacja
→ serwis → części zamienne → rozwój kolejnej generacji systemu

Umowy powinny jednocześnie umożliwiać zwiększenie wolumenu produkcji w sytuacji kryzysowej. Pozwoli to utrzymywać kompetencje przemysłowe także w okresie pokoju i ograniczyć ryzyko utraty kadr oraz zdolności produkcyjnych. Potrzeba długoterminowych i elastycznych form współpracy jest już wskazana w analizowanym materiale.

7. Transfer technologii powinien być oceniany przez pryzmat przejścia od montażu do samodzielnego projektowania

Samo uruchomienie produkcji w Polsce nie może być utożsamiane z transferem technologii. Kluczowym kryterium powinno być to, czy po zakończeniu programu Polska uzyska:

- dokumentację techniczną;
- kompetencje konstrukcyjne;

- prawa do modernizacji;
- zdolność samodzielnego serwisowania;
- możliwość produkcji części zamiennych;
- zdolność do integracji nowych komponentów;
- możliwość opracowania kolejnej generacji systemu.

W przeciwnym przypadku krajowa fabryka może pozostawać jedynie miejscem produkcji zlokalizowanym w Polsce, bez uzyskania rzeczywistej suwerenności technologicznej. Przyjęta w opracowaniu definicja polskiego przemysłu obronnego słusznie wskazuje, że sama lokalizacja produkcji jest niewystarczająca.

8. Należy aktywnie wykorzystywać przejęcia, joint ventures i inwestycje zagraniczne

W przypadku technologii, których stworzenie w Polsce wymagałoby kilkunastu lub kilkudziesięciu lat, zasadne jest wykorzystanie instrumentów przejęć, inwestycji kapitałowych oraz joint ventures. Polityka państwa powinna identyfikować zagraniczne przedsiębiorstwa posiadające technologie odpowiadające krajowym lukom i umożliwiać polskim podmiotom uzyskiwanie wpływu na ich działalność. Nie zawsze musi to oznaczać pełne przejęcie przedsiębiorstwa. Kluczowa jest kontrola nad technologią, prawami do rozwoju produktu, dostępem do dokumentacji oraz możliwością wykorzystania kompetencji w Polsce.

9. Cywilne uczelnie techniczne powinny zostać włączone do systemu budowy suwerenności technologicznej

Polskie uczelnie cywilne dysponują kompetencjami, które mogą uzupełniać istniejące zdolności przemysłu obronnego. Szczególnie istotne są kompetencje w zakresie radiolokacji, elektroniki, materiałów, optoelektroniki, technologii raketowych, amunicji, robotyki i systemów bezzałogowych. Konieczne jest zatem przejście od okazjonalnych projektów do stałych programów nauka–przemysł–wojsko, których celem będzie rozwiązywanie konkretnych luk technologicznych wskazanych przez przemysł i Siły Zbrojne RP.

10. Finansowanie badań powinno zostać przesunięte z modelu projektowego na programowy

Największym problemem współpracy nauki z przemysłem nie jest wyłącznie poziom finansowania, lecz jego niestabilność. Przerwy pomiędzy kolejnymi projektami prowadzą do utraty zespołów, kompetencji i ciągłości technologicznej. Dlatego rekomendowane jest:

- finansowanie kluczowych zespołów badawczych w perspektywie wieloletniej;
- odejście od finansowania wyłącznie pojedynczych projektów;
- utrzymywanie zespołów pracujących nad technologiami krytycznymi;
- tworzenie programów obejmujących kolejne poziomy TRL;
- powiązanie finansowania badań z rzeczywistym zapotrzebowaniem przemysłu i wojska.

Analiza wskazuje, że ciągłość finansowania jest warunkiem utrzymania kompetencji zespołów i skutecznego przechodzenia technologii od badań do wdrożenia.

11. Polityka własności intelektualnej wymaga zmiany

W przypadku technologii dual-use nadmierne restrykcyjne podejście do własności intelektualnej może ograniczać możliwość ich

dalszego rozwoju i komercjalizacji. Należy zatem stworzyć model, w którym państwo zachowuje kontrolę nad technologiami krytycznymi dla bezpieczeństwa, ale jednocześnie umożliwia uczelniom i przedsiębiorstwom rozwijanie cywilnych zastosowań technologii. Pozwoli to zwiększać skalę wykorzystania technologii, obniżać koszty ich rozwoju i zwiększać potencjał eksportowy.

12. Konieczne jest wprowadzenie systemu pomiaru skuteczności polonizacji

Rekomenduje się stworzenie Krajowego Indeks Suwerenności Technologicznej Systemów Uzbrojenia, który pozwalałby oceniać nie tylko procentowy udział krajowej produkcji, ale również:

- udział wartości dodanej w Polsce;
- poziom kontroli nad dokumentacją;
- kontrolę własności intelektualnej;
- krajową zdolność serwisową;
- możliwość samodzielnej modernizacji;
- zależność od pojedynczych dostawców;
- możliwość zwiększenia produkcji;
- czas odtworzenia zdolności produkcyjnych;
- zależność od surowców i komponentów krytycznych;
- koszt uzyskania dodatkowego poziomu odporności.

Pozwoliłoby to odejść od prostego mierzenia „procentu polonizacji” na rzecz oceny rzeczywistej odporności systemu.

13. Należy stworzyć mechanizm oceny kosztu dodatkowej odporności

Każda decyzja o zwiększeniu krajowej produkcji powinna być poprzedzona analizą ekonomiczną. Zwiększenie odporności może być bowiem osiągnięte poprzez różne instrumenty: polonizację, dywersyfikację, zapasy strategiczne, współpracę międzynarodową, inwestycje kapitałowe lub zmianę technologii. Dlatego dla każdego komponentu kry-

tycznego należy porównywać co najmniej cztery warianty:

- produkcja krajowa;
- dywersyfikacja dostaw zagranicznych;
- strategiczne zapasy i umowy gwarantujące dostawy;
- przejęcie lub współkontrola zagranicznego dostawcy.

Dopiero porównanie kosztów tych wariantów z wartością uzyskanej odporności powinno przesądzać o wyborze instrumentu. Jest to szczególnie istotne w odniesieniu do P 3, gdzie pełna polonizacja może być ekonomicznie nieuzasadniona.

14. Rozwój przemysłu obronnego powinien zostać włączony do szerszej strategii gospodarczej Polski

Analiza pokazuje, że rozwój przemysłu obronnego może generować efekty wykraczające poza bezpieczeństwo militarne: zwiększa kompetencje technologiczne, pobudza inwestycje, rozwijać sektor B+R, tworzyć produkty dual-use oraz zwiększać udział polskich przedsiębiorstw w międzynarodowych łańcuchach wartości. Warunkiem jest jednak odejście od modelu, w którym Polska jest przede wszystkim odbiorcą zagranicznego uzbrojenia, na rzecz modelu, w którym staje się producentem, integratorem i eksporterem wybranych technologii. W tym kontekście szczególne znaczenie powinno mieć budowanie pozycji polskiego przemysłu na rynkach Europy Środkowej i Wschodniej oraz wykorzystanie rosnącego zapotrzebowania państw wschodniej flanki NATO.

Analiza wskazuje, że przemysł zbrojeniowy współpracuje obecnie z uczelniami cywilnymi. Jednocześnie cywilne uczelnie techniczne dysponują unikalnymi kompetencjami, które mogą istotnie wzmacniać ofertę przemysłu zbrojeniowego. Aby jednak w pełni wykorzystać ten potencjał i uczynić z przemysłu obronnego krajowego lidera technologicznego, niezbędne jest:

1. Uruchamianie większej liczby badań naukowych i prac rozwojowych na wzór roz-

wiązań stosowanych w latach 2012–2015 w NCBR, co powinno być działaniem kierunkowym w celu aktywizacji takiej współpracy. Jednocześnie odwrócenie negatywnego trendu poprzez zwiększenie finansowania innowacji względem wydatków zakupowych w obszarze BiO;

2. Uelastycznienie polityki praw własności intelektualnej poprzez pozostawianie (pod kontrolą MON) tych praw podmiotom naukowym, które pozwolą uczelniom na dalszy rozwój technologii w obszarach cywilnych (dual-use) bez ich blokowania przez MON po zakończeniu fazy badań i rozwoju;
3. Ciągłość finansowania poprzez przejście z modelu „projektowego” (konkursowego) na model „programowy”, zapewniający stałe finansowanie kluczowych zespołów badawczych.
4. Na obecnym etapie rozwoju przemysłu obronnego celem badań naukowych na uczelniach powinno być pilne spolonizowanie istniejących rozwiązań technicznych w przemyśle obronnym. Chodzi zatem o skierowanie badań bardziej na suwerenność niż wyłącznie na innowacyjność.
5. Celem współpracy nauki z przemysłem obronnym powinno być zatem uzyskanie pełnej suwerenności łańcucha dostaw poprzez stosowanie polskich rozwiązań technicznych i wykorzystywanie polskich materiałów.
6. Z tego powodu wydaje się, iż transfer rozwiązań technologicznych z nauki do przemysłu obronnego powinien odbywać się przede wszystkim drogą komercjalizacji bezpośredniej (licencje, sprzedaż patentów).
7. Nie wyklucza to komercjalizacji pośredniej, tj. tworzenia start-upów uczelnianych ukierunkowanych na współpracę z przemysłem obronnym, w szczególności, jeśli dotyczy to technologii deep tech o przełomowym charakterze (disruptive deep tech) i rozwiązań powstających początkowo w małej skali (niski TRL).

Z punktu widzenia bezpieczeństwa państwa najważniejszym wyzwaniem nie jest

osiągnięcie maksymalnego poziomu krajowego udziału w produkcji uzbrojenia, lecz uzyskanie kontroli nad tymi elementami łańcucha wartości, których utrata uniemożliwiłaby produkcję, modernizację lub utrzymanie sprzętu w warunkach kryzysu. Polska posiada już znaczące kompetencje w zakresie integracji systemów i produkcji sprzętu wojskowego. Największa luka występuje natomiast w technologiach znajdujących się wyżej w łańcuchu wartości – szczególnie w P 1 i wybranych obszarach P 2. Pełna niezależność P 3, zwłaszcza w odniesieniu do półprzewodników i surowców krytycznych, nie powinna być traktowana jako realistyczny cel strategiczny. Dlatego polska polityka przemysłowo-obronna powinna opierać się na selektywnej suwerenności technologicznej: krajowej kontroli nad kluczowymi technologiami i zdolnościami, przy jednoczesnym wykorzystywaniu dywersyfikacji, współzależności, inwestycji zagranicznych i współpracy sojuszniczej tam, gdzie pełna polonizacja byłaby nadmiernie kosztowna lub technologicznie nieefektywna. W praktyce oznacza to konieczność przejścia od polityki „kupowania sprzętu w Polsce” do polityki „budowania zdolności do projektowania, produkcji, utrzymania i eksportu sprzętu w Polsce”. Taka zmiana powinna obejmować równocześnie politykę zakupową MON, politykę przemysłową, politykę naukowo-technologiczną, politykę surowcową oraz politykę zagraniczną.

WNIOSKI KOŃCOWE I KLUCZOWE REKOMENDACJE

Każdy rozdział kończy się szczegółowymi wnioskami i rekomendacjami. Niniejsza część stanowi syntezę najważniejszych wniosków i rekomendacji zawartych w raporcie.

Polska kupuje broń, ale nie zawsze kupuje bezpieczeństwo jej dostaw. Przeprowadzona analiza prowadzi do zasadniczego i niepokojącego wniosku: Polska szybko zwiększa wydatki na obronność i skalę zakupów uzbrojenia, ale system zarządzania bezpieczeństwem łańcuchów dostaw nie rozwija się w tym samym tempie. Problemem nie jest wyłącznie to, że część komponentów pochodzi z zagranicy. Problemem jest to, że państwo nie posiada jeszcze wystarczająco sprawnego, zintegrowanego mechanizmu, który pozwalałby określić, które z tych zależności są krytyczne, jak szybko mogą doprowadzić do zatrzymania produkcji oraz jakie działania należy podjąć, aby temu zapobiec. W praktyce oznacza to, że możemy posiadać coraz więcej nowoczesnego sprzętu, a jednocześnie pozostawać zależni od pojedynczego dostawcy silnika, jednego typu elektroniki, jednego materiału energetycznego, jednego producenta półprzewodników czy jednego źródła surowca. Jeżeli taki element zostanie objęty embargiem, sankcjami lub ograniczeniem eksportowym albo stanie się niedostępny z powodu awarii produkcji lub przyczyn geopolitycznych, problem nie będzie dotyczył pojedynczego komponentu, a może zatrzymać cały system.

Analiza dowodzi, że rzeczywiste słabości polskiego przemysłu obronnego znajdują się często nie na poziomie końcowego producenta, lecz niżej, tj. u jego dostawców podzespołów czy materiałów do produkcji, takich

jak półprzewodniki, elektronika, chemia specjalna, surowce krytyczne oraz technologie, bez których nie można utrzymać ciągłości produkcji. Oznacza to, że samo kupienie lub zmontowanie systemu uzbrojenia w Polsce nie gwarantuje suwerenności technologicznej. Polska może produkować platformę, ale jeżeli nie kontroluje kluczowych komponentów, dokumentacji, praw serwisowych, oprogramowania lub technologii modernizacji, pozostaje zależna od zagranicznego dostawcy, który posiada te prawa. Raport wskazuje wprost, że ograniczona kontrola nad tymi zasobami może prowadzić do trwałego uzależnienia nawet wtedy, gdy część sprzętu jest produkowana w kraju.

Dlatego konieczne jest odejście od modelu „kupowania sprzętu” na rzecz modelu „budowania i utrzymywania zdolności”. Kluczowym wyzwaniem dla Ministerstwa Obrony Narodowej i Agencji Uzbrojenia powinno być kształtowanie procesów pozyskiwania i finansowania w taki sposób, aby rosnące nakłady na obronność przekładały się nie tylko na zakup sprzętu, lecz przede wszystkim na trwałe zdolności jego utrzymania, modernizacji i odnowienia. Kontrakty powinny obejmować nie tylko dostawę, ale także serwis, części zamienne, modernizację, rozwój, transfer technologii i możliwość zwiększenia produkcji. Dotyczy to w szczególności systemów, które mają pozostawać w służbie przez kilkadziesiąt lat. Warto zauważyć, iż słabością jest nie brak pieniędzy, lecz brak adekwatnego nimi zarządzania, czego efektem jest ograniczona dostępność i struktura finansowania całego łańcucha. Sytuacja finansowa liderów przedsiębiorstw zarówno sektora państwowego, jak i prywatnego, jest dobra, a wpływy do budżetu z sektora pochodzą nie tylko z podat-

ków, ale również wypłacanych dywidend.²³⁴ W ostatnich latach Polska przeznacza na modernizację Sił Zbrojnych środki o skali wcześniej niespotykanej. Jednak wzrost wydatków nie może być utożsamiany ze wzrostem odporności państwa.

Agencja Uzbrojenia nie może być wyłącznie administratorem wielkich kontraktów zakupowych. Powinna stać się instytucją zarządzającą bezpieczeństwem zdolności w całym cyklu życia uzbrojenia. Dzisiaj problem polega na tym, że system jest rozproszony. MON, Agencja Uzbrojenia, przemysł państwowy, przemysł prywatny, operatorzy infrastruktury, RARS, AMW, BGK i inne instytucje posiadają fragmenty informacji i kompetencji, ale raport wskazuje na konieczność eliminacji silosowości i udrożnienia przepływu informacji, a z drugiej strony sprawnego zarządzania ekosystemem. **Państwo nie może zarządzać bezpieczeństwem łańcucha dostaw, jeżeli nie widzi całego łańcucha.**

Najważniejszym zadaniem MON powinno być zatem stworzenie rzeczywistej „mapy zależności” polskiej obronności. Nie wystarczy wiedzieć, kto jest producentem Kraba, Borsuka, K9 czy Warmate. Trzeba wiedzieć, kto dostarcza komponenty do poszczególnych elementów tego systemu, skąd pochodzi materiał, kto produkuje elektronikę, kto dostarcza półprzewodniki, kto ma prawa do dokumentacji, kto może wykonać serwis, kto posiada technologię oraz co się stanie, jeżeli dany dostawca przestanie dostarczać produkt jutro rano. Właśnie na tym poziomie pojawia się największa luka instytucjonalna.

Jednym z kierunków rozwijania kompetencji MON powinno być zbudowanie wspólnego obrazu zależności między zakładami, dostawcami oraz operatorami infrastruktury krytycznej. Dopiero taki obraz umożliwia racjonalne określenie, gdzie potrzebne są zapasy, redundancja, alternatywni dostawcy, inwestycje i działania ochronne. To powinno znaleźć odzwierciedlenie w zadaniach Agencji Uzbrojenia lub innej nowo powołanej instytucji. Każdy strategiczny program modernizacyjny powinien posiadać nie tylko

harmonogram dostaw i cenę kontraktu, ale również mapę zależności przemysłowych i technologicznych oraz plan odporności łańcucha dostaw. **Raport wskazuje, iż Polska ma problem z filozofią zakupów.** Drugim zasadniczym problemem jest polityka kontraktowania. Raport pokazuje, że w przypadku amunicji 155 mm polityka kontraktowania jest jednym z ryzyk o znaczeniu krytycznym. **Bez długoterminowych zamówień, przewidywalnego finansowania i stabilnego popytu nie można utrzymać zdolności do produkcji wielkoseryjnej. Jednocześnie zamawiający i dostawca muszą być otwarci na wprowadzanie modyfikacji i zmian.**

To prowadzi do fundamentalnego pytania: czy państwo kupuje zdolność produkcyjną, czy tylko kolejne partie produktów?

Jeżeli państwo zamawia sprzęt wyłącznie w logice pojedynczych kontraktów, może uzyskać produkt, ale niekoniecznie zdolność przemysłową. Tymczasem w warunkach kryzysu liczy się nie to, ile sprzętu wyprodukowano w ubiegłym roku, lecz jak szybko można zwiększyć jego produkcję, naprawić uszkodzone systemy i uzupełnić zużyte zasoby. **Dlatego polityka zakupowa powinna zostać zmieniona z polityki „kupowania sprzętu” na politykę „budowania i utrzymywania zdolności”.** Kontrakt powinien obejmować nie tylko dostawę, ale także serwis, części zamienne, modernizację, rozwój, transfer technologii i możliwość zwiększenia produkcji. Dotyczy to w szczególności systemów, które mają pozostawać w służbie przez kilkadziesiąt lat.

Najbardziej jaskrawym przykładem problemu jest amunicja artyleryjska 155 mm. Polska posiada kompetencje w zakresie produkcji niektórych elementów amunicji i montażu końcowego, ale nadal zależy od zagranicznych dostawców kluczowych komponentów. Ograniczenia dotyczą m.in. nitrocelulozy, prochów wielobazowych, modułowych ładunków miotających oraz zaawansowanych zapalników. Nie jest to wyłącznie problem przemysłu. Jeżeli państwo chce posiadać zdolność do prowadzenia

²³⁴ Dla przykładu Grupa WB zapłaciła w 2024 roku 511 mln podatków i wypłaciła 15,8 mln złotych dywidendy do PFR.

długotrwałego konfliktu, musi posiadać zdolność do produkcji amunicji w skali odpowiadającej temu konfliktowi. Dlatego rozwój amunicji 155 mm powinien zostać potraktowany jako jeden z najważniejszych programów przemysłowo-obronnych państwa. Powinien obejmować nie tylko fabrykę końcowego produktu, lecz cały łańcuch: surowce, chemię specjalną, materiały energetyczne, komponenty, zapalniki, ładunki miotające, elaborację, kontrolę jakości, magazynowanie i transport. Budowa fabryki bez zabezpieczenia jej P2 i P3 nie rozwiązuje problemu. Nie zapewnia rzeczywistej suwerenności technologicznej.

Polska nie może być suwerenna tylko na poziomie montażu. Analiza Kraba, Borsuka, Warmate i amunicji 155 mm pokazuje różne modele krajowych zdolności. Szczególnie wysoki poziom suwerenności technologicznej osiągnięto w przypadku Warmate, podczas gdy Krab i Borsuk posiadają wysokie zdolności integracyjne i produkcyjne, ale pozostają zależne m.in. od zagranicznych napędów i części mikroelektroniki. Największe luki występują w przypadku amunicji, szczególnie w obszarze materiałów energetycznych i chemii specjalistycznej. Wniosek jest jednoznaczny: polonizacja nie może ograniczać się wyłącznie do przeniesienia montażu do Polski.

Warunkiem wzmocnienia bezpieczeństwa Polski w analizowanym obszarze jest **zapewnienie ciągłości kompetencji zarządczych w przedsiębiorstwach o strategicznym znaczeniu dla bezpieczeństwa państwa**. Stabilność i rozwój zdolności przemysłowych wymagają nie tylko finansowania, lecz także długofalowego zarządzania, zachowania wiedzy organizacyjnej i ciągłości odpowiedzialności za realizację strategicznych programów. Częste zmiany kierownictwa mogą utrudniać realizację wieloletnich inwestycji, rozwój kompetencji i budowanie relacji w łańcuchach dostaw. Dlatego zarządzanie strategicznymi spółkami powinno zapewniać większą ciągłość kompetencji i odpowiedzialności, adekwatną do wieloletniego charakteru programów obronnych.

Mikroelektronika jest dziś tak samo ważna jak stal i materiały energetyczne

Nowoczesny system uzbrojenia bez elektroniki, sensorów, procesorów, FPGA, MEMS i półprzewodników nie istnieje. Zależność od tych komponentów przenosi się jednocześnie na obronność, cyberbezpieczeństwo, łączność, AI i systemy bezzałogowe. Dlatego państwo powinno traktować mikroelektronikę **jako technologię bezpieczeństwa narodowego, a w ujęciu węższym – bezpieczeństwa ekonomicznego**, a nie jeden z wielu sektorów przemysłu. W krótkim okresie oznacza to zabezpieczenie dostaw i zapasy. W średnim – budowę kompetencji projektowych, testowych i integracyjnych. W długim – rozwój wybranych zdolności produkcyjnych.

Nie wszystko trzeba produkować w Polsce – ale wszystko, co krytyczne, musi być zabezpieczone

Raport nie daje podstaw do postulowania pełnej autarkii. Przeciwnie, analiza P3 pokazuje, że w przypadku surowców krytycznych, półprzewodników i materiałów specjalnych pełna polonizacja byłaby bardzo trudna z powodów technicznych i kosztów. Polska powinna zatem przyjąć zasadę „odporności zamiast autarkii”. Jeżeli czegoś nie możemy produkować w kraju lub nie opłaca się tego robić w kraju, musimy posiadać alternatywnego dostawcę, strategiczny zapas, długoterminową umowę, dostęp do rynku sojuszniczego albo – w przypadku najważniejszych aktywów – udział kapitałowy zapewniający wpływ na dostawy. Największym błędem byłoby zastąpienie jednej zależności inną zależnością. Infrastruktura może zatrzymać produkcję równie skutecznie jak brak komponentu. Raport pokazuje, że zagrożenie dla przemysłu obronnego nie znajduje się wyłącznie w fabryce. Utrata zasilania, łączności, centrum danych, systemów ERP/MES/WMS, infrastruktury transportowej lub dostawcy krytycznego może wywołać efekt kaskadowy prowadzący do zatrzymania produkcji i opóźnienia dostaw dla Sił Zbrojnych. Oznacza to, że **Polska musi zacząć traktować energię, transport, telekomunikację i infrastrukturę cyfrową jako część łańcucha dostaw uzbrojenia**. Fabryka, która nie ma odpornego zasilania, alternatywnej łączności i procedur

pracy awaryjnej, nie jest w pełni zabezpieczonym zakładem produkcyjnym. Potrzebujemy instytucji, która naprawdę zarządza odpornością. Najważniejsza rekomendacja ma więc charakter instytucjonalny. MON powinno przestać zarządzać wyłącznie zakupami. Powinno zarządzać zdolnościami. Dla każdego strategicznego programu należy wskazać podmiot odpowiedzialny za cały przepływ, przygotować warianty zastępcze w obszarze transportu, logistyki, zasilania i wymiany informacji oraz regularnie sprawdzać ich wykonalność. Odporność nie powinna być oceniana na podstawie deklarowanej dostępności zasobów, lecz na podstawie zdolności utrzymania dostaw po zakłóceniu oraz czasu potrzebnego do przełączenia i odtworzenia funkcji. **Z tego powodu konieczna jest pilna interwencja systemowa.**

System pozyskiwania sprzętu wojskowego powinien uwzględniać bezpieczeństwo całego cyklu życia strategicznych systemów uzbrojenia. Oznacza to odpowiedzialność za identyfikację krytycznych zależności, ocenę P1-P3, wymagania dotyczące transferu technologii, prawa do serwisu i modernizacji, dostęp do części zamiennych, zdolność zwiększenia produkcji oraz odporność infrastruktury i dostawców. Bez takiej zmiany organizacyjnej państwo będzie nadal wydawać coraz większe pieniądze, ale nie będzie miało pewności, jak długo i w jakich warunkach będzie mogło korzystać z zakupionego sprzętu. Również możliwości szybkiego skalowania produkcji będą ograniczone.

Potrzebna jest jedna mapa bezpieczeństwa polskiej obronności

Najpilniejszym zadaniem powinno być stworzenie centralnego systemu mapowania krytycznych łańcuchów dostaw. Powinien on obejmować wszystkich kluczowych dostawców, poziomy P1-P3, surowce, technologie, infrastrukturę oraz zależności serwisowe i cyfrowe. System powinien odpowiadać na pięć prostych pytań: Od czego zależy dana zdolność? Kto jest jedynym dostawcą? Jak długo możemy działać bez jego dostaw? Czy istnieje zamiennik? Jak szybko państwo może odtworzyć utraconą zdolność? Dopiero odpowiedzi na te pytania pozwolą racjonalnie kierować miliardowe środki przeznaczone na modernizację.

Konieczna jest odpowiedzialność za wynik, a nie za procedurę

Największym zagrożeniem jest sytuacja, w której każda instytucja formalnie realizuje swoje zadania, ale żadna nie odpowiada za odporność całego systemu. Jeżeli MON odpowiada za potrzeby wojska, Agencja Uzbrojenia za zakupy, przemysł za produkcję, operator infrastruktury za energię lub transport, a dostawca zagraniczny za komponent, może powstać sytuacja, w której wszyscy wykonują swoje zadania, ale państwo nadal nie posiada gwarancji ciągłości dostaw. To właśnie jest problem systemowy, który wynika z analizy. Dlatego potrzebna jest jasna odpowiedzialność za cały łańcuch – od decyzji o zakupie do zdolności do produkcji, serwisowania, modernizacji i odtworzenia systemu.

Jednym z najbardziej niedocenianych ryzyk dla bezpieczeństwa łańcuchów dostaw są kadry. Polska może kupić licencję, wybudować fabrykę i sprowadzić najnowocześniejszą technologię, ale nie kupi w krótkim czasie ludzi posiadających wiedzę konieczną do jej rozwijania, produkcji, serwisowania i modernizacji. Raport identyfikuje niedobór wykwalfikowanych kadr jako jedno z istotnych ryzyk wewnętrznych. Dotyczy to szczególnie niedoboru specjalistów posiadających unikalne kompetencje w technologiach obronnych oraz ryzyka utraty wiedzy krytycznej. W przypadku analizowanych systemów ryzyko kadrowe jest oceniane jako wysokie, a w odniesieniu do niektórych zdolności nawet jako krytyczne. Warto podkreślić, iż tworzenie zespołów badawczo-rozwojowych wymaga czasu, aby zaczęły optymalnie funkcjonować. Problem jest szerszy niż brak pracowników. Państwo ryzykuje utratę kompetencji, których odbudowa może trwać wiele lat. Odejście kilku kluczowych ekspertów może oznaczać utratę wiedzy dotyczącej technologii, procesu produkcyjnego, materiałów lub serwisu konkretnego systemu. W sektorze obronnym nie jest to zwykła rotacja pracowników – może to być utrata zdolności strategicznej. Dlatego polityka kadrowa powinna zostać uznana za element polityki bezpieczeństwa. Potrzebny jest system identyfikacji kompetencji krytycznych, programy sukcesji, kształcenie specjalistów, współpraca przemysłu z uczelniami i szkołami zawodowymi oraz mechanizmy zatrzy-

mywania ekspertów na wzór wdrażanego wojskowego kwestionariusza kompetencji opracowanego przez Sztab Generalny WP, Wojskową Akademię Techniczną i inne podmioty. Raport wskazuje wprost na potrzebę rozwoju kapitału ludzkiego poprzez reskilling i upskilling, pozyskiwanie specjalistów z innych branż oraz współpracę z uczelniami i szkołami zawodowymi. Niezwykle istotnym zagadnieniem w przypadku przedsiębiorstw kontrolowanych przez Skarb Państwa jest zachowanie ciągłości i dynamiki realizacji projektów, co wymaga wzmocnienia pozycji kadry zarządzającej poprzez **powołanie Korpusu Menedżerów** zarządzających kluczowymi projektami, a *zatem* wyłączenie kadry zarządzającej z bieżącego sporu politycznego oraz wprowadzenie jasnych, obiektywnych kryteriów oceny menedżerów, a także stabilnego sposobu ich zatrudniania i wynagradzania. Powołanie Korpusu powinno zostać wzmocnione przygotowaniem dobrych praktyk menedżerskich w spółkach Skarbu Państwa oraz wzmocnieniem Rady do spraw spółek z udziałem Skarbu Państwa i państwowych osób prawnych.

Monopol państwowy nie jest synonimem bezpieczeństwa. Bezpieczeństwo państwa wymaga silnego przemysłu krajowego, ale silny przemysł krajowy nie oznacza automatycznie silnego sektora państwowego. Nadmierna koncentracja zamówień w ograniczonej liczbie podmiotów może prowadzić do wzrostu kosztów, ograniczenia presji technologicznej, spadku innowacyjności i uzależnienia państwa od pojedynczych wykonawców. Raport pokazuje, że polski przemysł obronny tworzą zarówno przedsiębiorstwa państwowe, jak i prywatne, a analiza została celowo przeprowadzona z uwzględnieniem obu segmentów, aby zidentyfikować bariery współpracy oraz różnice potencjałów. **Państwo powinno zatem chronić zdolności strategiczne, ale jednocześnie zwiększać konkurencję wszędzie tam, gdzie jest to możliwe bez naruszania bezpieczeństwa informacji i dostaw.** Nie chodzi o to, aby każdą część uzbrojenia produkowało kilka przedsiębiorstw. Chodzi o to, aby państwo nie znalazło się w sytuacji, w której jeden podmiot jest jednocześnie jedynym producentem, jedynym integratorem, jedynym serwisantem i jedynym dysponentem wiedzy. **Konkurencja powinna być również**

narzędziem polityki technologicznej. Przedsiębiorstwa powinny konkurować nie tylko ceną, ale również czasem dostawy, innowacyjnością, poziomem polonizacji, zdolnością do zwiększenia produkcji, bezpieczeństwem dostaw oraz jakością serwisu. Raport wskazuje, że istnieją zarówno krajowe, jak i europejskie instrumenty pozwalające łączyć ochronę strategicznych zdolności z zasadami konkurencji. Prawo unijne dopuszcza szczególne rozwiązania w dziedzinie obronności, ale jednocześnie ogranicza możliwość wykorzystywania wyjątków w sposób prowadzący do nieuzasadnionego zakłócania konkurencji. **Dlatego konkurencyjność powinna być traktowana jako element bezpieczeństwa, a nie jako przeszkoda dla polityki przemysłowej.** Im więcej kompetentnych podmiotów może konkurować o zamówienia, tym większa presja na innowacyjność, efektywność i skracanie czasu realizacji. Jednocześnie państwo powinno świadomie utrzymywać wybrane zdolności strategiczne, nawet jeśli ich utrzymywanie nie jest optymalne z punktu widzenia krótkookresowej efektywności ekonomicznej. W tym kontekście kluczowe jest przygotowywanie zdolności do skalowania produkcji zbrojeniowej, co wymaga szczególnych analiz i zarządzania tym procesem. Przygotowania te muszą być prowadzone już dzisiaj i obejmować przyszłe łańcuchy dostaw.

Kolejnym obszarem, który wymaga znacznie większej uwagi, jest wywiad gospodarczy, kontrwywiad i bezpieczeństwo informacyjne. Współczesny łańcuch dostaw jest jednocześnie mapą zależności technologicznych, finansowych, kapitałowych i politycznych. Jeżeli państwo nie zna rzeczywistej struktury właścicielskiej dostawcy, jego powiązań kapitałowych, źródeł finansowania, zależności technologicznych oraz powiązań z innymi przedsiębiorstwami, nie jest w stanie prawidłowo ocenić ryzyka. **Raport wskazuje na możliwość wykorzystania zaawansowanych narzędzi analitycznych i danych OSINT do identyfikowania ukrytych powiązań, w tym podmiotów fasadowych oraz zależności znajdujących się na niższych poziomach łańcucha.** Jednocześnie raport podkreśla znaczenie analiz zagrożeń ekonomicznych i wywiadowczych przy ocenie dostawców wysokiego ryzyka.

Oznacza to konieczność stworzenia stałego systemu aktywności służb specjalnych na rzecz bezpieczeństwa łańcuchów dostaw obronnych, a zatem wzmocnienia ich struktur osobowych, finansowych i technologicznych. W przypadku strategicznych łańcuchów dostaw wywiad gospodarczy powinien być pierwszą linią ostrzegania państwa – systemem wczesnego ostrzegania. Pozyskiwanie informacji, a następnie przekształcanie ich w wiedzę użyteczną w procesach zarządczych i decyzyjnych, jest niezwykle istotne. Jednocześnie zwiększenie penetracji technologicznej w tym przejmowanie kontroli nad przedsiębiorstwami za granicą wymaga intensyfikacji działań. Wzmocnieniu tego obszaru powinien towarzyszyć transparentny, jasny system przepływu informacji między całym ekosystemem przedsiębiorstw państwowych i prywatnych gwarantujący z jednej strony ich odrębność i konkurencyjność na rynku, a jednocześnie wsparcie.

Przewlekłość postępowań zakupowych i certyfikacyjnych oraz brak elastyczności są zagrożeniem bezpieczeństwa. Sytuacja ta jest szczególnie szkodliwa w sektorze produkcji obronnej, w którym technologia zmienia się szybciej niż cykl administracyjny, a ekosystem musi elastycznie reagować na doświadczenia z wojny na Ukrainie. **W raporcie zwrócono uwagę, iż postępowania certyfikacyjne powinny być szybsze i bardziej transparentne.** Poważne wątpliwości budzi potencjalne ryzyko konfliktu interesów, które obecnie nie jest we właściwy sposób zarządzane.

Nowy model polityki publicznej w zakresie rozwoju możliwości obronnych Polski powinien opierać się na pięciu zasadach. Pierwszą zasadą powinno być *security by procurement* – bezpieczeństwo łańcucha dostaw musi być jednym z podstawowych kryteriów każdej decyzji zakupowej produktów i usług. Drugą zasadą powinna być *competition by design* – tam, gdzie nie ma uzasadnienia dla monopolu, państwo powinno projektować zamówienia tak, aby tworzyć rzeczywistą konkurencję technologiczną i przemysłową. Trzecią zasadą powinno być *intelligence by default* – każda krytyczna decyzja zakupowa powinna być poprzedzona analizą nie tylko wykonawcy, lecz całego łańcucha zależ-

ności i powiązań. Czwartą zasadą powinno być *time is security* – czas realizacji postępowania powinien być traktowany jako parametr bezpieczeństwa, a nie wyłącznie parametr administracyjny. Piątą zasadą powinno być *people are capability* – kompetencje i kadry muszą być traktowane jako element zdolności obronnej państwa, a nie jako zwykły koszt przedsiębiorstwa. Wprowadzenie tych zasad wymaga zmiany systemu pozyskiwania sprzętu wojskowego.

Konkluzja

Polska stoi obecnie przed wyborem pomiędzy dwoma modelami modernizacji obronnej. Pierwszy polega na dalszym szybkim kupowaniu sprzętu, zwiększaniu liczby kontraktów i liczeniu na to, że globalne łańcuchy dostaw pozostaną dostępne. Drugi zakłada budowę rzeczywistej odporności przemysłowej państwa – poprzez kontrolę nad technologiami krytycznymi, zabezpieczenie P2 i P3, strategiczne zapasy, krajowe zdolności produkcyjne, dywersyfikację dostaw, odporność infrastruktury i sprawne zarządzanie całym cyklem życia uzbrojenia. **Analiza przeprowadzona w raporcie wskazuje jednoznacznie, że drugi model jest konieczny.** Polska nie może pozwolić sobie na sytuację, w której posiada jedną z największych armii w Europie, ale jej zdolność do prowadzenia długotrwałych działań zależy od kilku zagranicznych dostawców komponentów, których państwo nie kontroluje. Również sytuacja budżetowa wskazuje na konieczność polonizacji łańcuchów w sposób przedstawiony w raporcie, aby zwiększyć wartość mnożnika i wpływy podatkowe do budżetu.

Nie wystarczy więc pytać, ile uzbrojenia kupimy. Trzeba odpowiedzieć na znacznie ważniejsze pytanie: czy będziemy w stanie produkować, naprawiać i uzupełniać to uzbrojenie wtedy, kiedy naprawdę będzie potrzebne? Jeżeli odpowiedź na to pytanie nie jest pozytywna, część obecnego programu modernizacji pozostaje inwestycją w potencjał wojskowy, ale nie jest jeszcze inwestycją w pełne bezpieczeństwo państwa.

Raport wskazuje, że dla MON kluczowe powinno być zbudowanie wspólnego obrazu

zależności między zakładami, dostawcami oraz operatorami sprzętu wojskowego (SpW) i infrastruktury krytycznej. Dopiero taki obraz umożliwia racjonalne określenie, gdzie potrzebne są zapasy, redundancja, alternatywni dostawcy, inwestycje i działania ochronne. **To powinno być podstawowym zadaniem istniejących struktur RON albo innej nowo powołanej instytucji.** Każdy strategiczny program modernizacyjny powinien posiadać nie tylko harmonogram dostaw i cenę kontraktu, ale również mapę zależności przemysłowych i technologicznych oraz plan odporności łańcucha dostaw. **Raport wskazuje, iż Polska ma problem z filozofią zakupów.** Drugim zasadniczym problemem jest polityka kontraktowania. Raport pokazuje, że w przypadku amunicji 155 mm polityka kontraktowania jest jednym z ryzyk o znaczeniu krytycznym. **Bez długoterminowych zamówień, przewidywalnego finansowania i stabilnego popytu nie można utrzymać zdolności do produkcji wielkoseryjnej. Jednocześnie zamawiający i dostawca muszą być otwarci na wprowadzanie modyfikacji i zmian.**

BIBLIOGRAFIA

Monografie, artykuły i publikacje naukowe

Ambroziak, Ł., Arak, P., Baszczak, Ł., Juszczak, A., Kopiński, D., Leszczyński, P., Maj, M. i Wąsiński, M. (2022). Dekada bezpieczeństwa ekonomicznego. Od offshoringu do częściowego friendshoringu. Warszawa: Polski Instytut Ekonomiczny.

Antai, I. i Hellberg, R. (2024). Identifying total defense logistics concepts: A comparative study of the Swedish pandemic response. *Journal of Humanitarian Logistics and Supply Chain Management*, 14(2), 208–222. <https://doi.org/10.1108/JHLSCM-07-2022-0084>

Antai, I. i Hellberg, R. (2025). Surge complexities in defense industry supply chains: evidence from multiple case studies. *The International Journal of Logistics Management*, 36(7), 242–261. <https://doi.org/10.1108/IJLM-07-2024-0458>

Apte, A., Rendon, R. i Salmeron, J. (2011). An optimization approach to strategic sourcing: A case study of the United States Air Force. *Journal of Purchasing and Supply Management*, 17(4), 222–230. <https://doi.org/10.1016/j.pur-sup.2011.03.002>

Center for Strategic and International Studies (2022). Building Supply Chain Resilience. Washington, DC: CSIS.

Dolgui, A., Ivanov, D. i Sokolov, B. (2018). Ripple effect in the supply chain: An analysis and recent literature. *International Journal of Production Research*, 56(1–2), 414–430. <https://doi.org/10.1080/00207543.2017.1387680>

Edler, J. (2024). Technology Sovereignty of the EU: Needs, Concepts, Pitfalls and Ways Forward. W: Science, Research and Innovation Performance of the EU 2024, 428–435. Brussels: European Commission.

Ekström, T. (2025). Supply Chain Resilience – An Empirical Exploration of Barriers and Enablers in Military Settings. *Scandinavian Journal of Military Studies*, 8(1), 119–136. <https://doi.org/10.31374/sjms.350>

Elvemo, L. (2025). Supply Chain Resilience in Military Operations: A Case Study Exploring Command and Control. *Scandinavian Journal of Military Studies*, 8(1), 178–199. <https://doi.org/10.31374/sjms.356>

Gauthier, D. J., Biederman, N., Gyovai, B. i Wilhelm, J. P. (2024). Digital twin of a DC brushless electric motor-propeller system with application to drone dynamics. *AIAA SCITECH 2024 Forum*, art. 2359. <https://doi.org/10.2514/6.2024-2359>

Hellberg, R. (2023). Swedish Public Procurement and the Defence Industry: Obstacles and Opportunities. *Journal of Defense Analytics and Logistics*. <https://doi.org/10.1108/JDAL-12-2022-0015>

Hu, K., Levi, R., Yahalom, R. i Zerhouni, E. G. (2023). Supply Chain Characteristics as Predictors of Cyber Risk: A Machine-Learning Assessment. *arXiv preprint arXiv:2210.15785*.

International Electrotechnical Commission (2019). IEC 31010:2019 Risk management — Risk assessment techniques. Geneva: IEC.

Ivanov, D. i Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning & Control*, 32(9), 775–788. <https://doi.org/10.1080/09537287.2020.1768450>

Johansen, A. i Kruck, A. (2025). The competence–control trade-off in military AI innovation: Autonomous weapons systems and shifting modes of state control over private experts. *European Journal of International Security*. <https://doi.org/10.1017/eis.2025.10020>

Jüttner, U. i Maklan, S. (2011). Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Management: An International Journal*, 16(4), 246–259. <https://doi.org/10.1108/13598541111139062>

Korkmaz, G. (2024). Supply Chain Risks and Management Strategies in the Defence Industry. *Journal of Defense Resources Management*, 15(1), 35–60.

Kos, B. (2013). Znaczenie łańcuchów dostaw we współczesnej gospodarce. *Zeszyty Naukowe Uniwersytetu Szczecińskiego, Problemy Zarządzania, Finansów i Marketingu*, 29(751), 73–88.

Kovács, G. i Tatham, P. (2009). Responding to Disruptions in the Supply Network – from Dormant to Action. *Journal of Business Logistics*, 30(2), 215–229. <https://doi.org/10.1002/j.2158-1592.2009.tb00121.x>

Li, Y., Kim, K., Leyffer, S., Menickelly, M., Lewis, L. P. i Bergerson, J. (2024). Modeling and solving cascading failures across interdependent infrastructure systems. *arXiv preprint arXiv:2407.16796*.

Liu, C., Wang, Y., Purvis, L. i Potter, A. (2026). Can digital twin technology enhance supply-chain resilience? A systematic literature review. *Sustainability*, 18(5), 2361. <https://doi.org/10.3390/su18052361>

Lopes, P. V., Chen, S., González Sánchez, J. P., Bekar, E. T., Bokrantz, J. i Skoogh, A. (2023). Data-driven smart maintenance decision analysis: A drone factory demonstrator combining digital twins and adapted AHP. W: *Proceedings of*

the 2023 Winter Simulation Conference, 1996–2007. <https://doi.org/10.1109/WSC60868.2023.10408351>

Loska, D., Hazen, B., Rich, N., Genchev, S. i Malik, T. (2025). Military Supply Chain Logistics and Dynamic Capabilities: A Literature Review and Synthesis. *Transportation Journal*, 64, e70002. <https://doi.org/10.1002/tjo3.70002>

Lucas, R., Ekström, T., Fusaro, P., Hastings Roer, E. i Retter, L. (2024). Toward Defense Supply Chain Disruption Management: A Research Agenda for Defense Supply Chain Resilience. Santa Monica, CA: RAND Corporation. <https://doi.org/10.7249/RR2504-1>

Mannan, S. (red.) (2012). *Lees' Loss Prevention in the Process Industries*. Oxford: Butterworth-Heinemann.

Mączyński, D. (2024). *Seria Nauki Ekonomiczne Nr 13*. Poznań: Uniwersytet im. Adama Mickiewicza w Poznaniu.

NIST (2022). *Praktyki zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw dla systemów i organizacji* (NIST SP 800-161 Rev. 1, wer. 1.0 PL). Gaithersburg: National Institute of Standards and Technology.

OECD (2025). *OECD Supply Chain Resilience Review: Navigating Risks*. Paris: OECD Publishing. <https://doi.org/10.1787/94e3a8ea-en>

Perotto, G. (2023). The Legal Framework of the EU Defence Industry and the Pursuit of Strategic Autonomy. *European Papers*, 8(1), 475–486.

Piotrowski, S. (2025). Stan i perspektywy dla sektora półprzewodników w Polsce. W: M. Flieger (red.), *Kierunki usprawnień gospodarki oraz organizacji w aspekcie zarządczym i prawnym*. Poznań.

RAND Corporation (2024). *Toward Defense Supply Chain Disruption Management*. Santa Monica, CA: RAND Corporation.

Rasmussen, A., Sabic, H., Saha, S. i Nielsen, I. E. (2023). Supplier selection for aerospace & defense industry through MCDM methods. *Cleaner Engineering and Technology*, 12, 100590. <https://doi.org/10.1016/j.clet.2022.100590>

Roberts, A. (2025). Utilization of Artificial Intelligence (AI) to Illuminate Supply Chain Risk. Fort Belvoir, VA: Defense Logistics Agency.

Shao, G., Kibira, D. i Frechette, S. (2024). *Digital Twins for Advanced Manufacturing: The Standardized Approach*. W: *Digital Twins, Simulation, and Metaverse*. Washington, DC: Springer Nature.

Stoelinga, F., van Loon, K., Ellison, D., Stoop, R. i Zandee, D. (2026). *Catching Up: Europe's Path to Strategic Autonomy in the Defence Industry*. Haga: Clingendael Institute & HCSS.

Stouffer, K., Pease, M., Tang, C. Y., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A. i Thompson, M. (2023). *Guide to Operational Technology (OT) Security* (NIST Special Publication 800-82 Rev. 3). Gaithersburg: National Institute of Standards and Technology.

Taylor, C. O. (2026). *Reshoring, Nearshoring, and North American Supply Chains*. Working Paper. Houston, TX: Rice University's Baker Institute for Public Policy.

Tudosia, M. (2026). Predictive maintenance and life cycle management for armoured vehicles. *European Security & Defence*. <https://euro-sd.com/2026/01/articles/exclusive/48523/predictive-maintenance-and-life-cycle-management-for-armoured-vehicles/>

UK Ministry of Defence (2022). *Defence Supply Chain Strategy*. London: Ministry of Defence.

United States Department of Defense (2012). *System Safety Standard Practice (MIL-STD-882E)*. Washington, D.C.: DoD.

U.S. Defense Business Board (2025). *Supply Chain Illumination in the Department of Defense*. Washington, D.C.: DBB.

Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X. i Hamin, M. (2025). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations (NIST AI 100-2 E2025). Washington, D.C.: U.S. Department of Commerce. <https://csrc.nist.gov/pubs/ai/100/2/e2025/final>

Wroński, M., Bąkowski, K. i Muchorowski, J. (2025). Wzrost nakładów na obronę narodową – szansa na poprawę innowacyjności polskiej gospodarki? Radom: Łukasiewicz – Instytut Technologii Eksploatacji Wydawnictwo Naukowe.

Raporty instytucjonalne, standaryzacja i dokumenty strategiczne

Centrum Unijnych Projektów Transportowych (b.r.). *Zintegrowany Model Ruchu*. Warszawa: CUPT.

European Defence Agency (b.r.). *Security of Supply*. <https://www.eda.europa.eu>

European Commission (2025a). *White Paper for European Defence Readiness 2030*. European Union. https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en

European Commission (2025b). *European Defence Readiness Roadmap 2030*. European Union. https://defence-industry-space.ec.europa.eu/eu-defence-industry/readiness-roadmap-2030_en

European Parliamentary Research Service (2026). *European defence readiness roadmap 2030* (EPRS Briefing

PE 782.589). European Parliament. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782589/EPRS_BRI\(2026\)782589_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782589/EPRS_BRI(2026)782589_EN.pdf)

Generalna Dyrekcja Dróg Krajowych i Autostrad (b.r.). Generalny Pomiar Ruchu 2020/2021–2025. Warszawa: GDDKiA.

International Air Transport Association (2026). Dangerous Goods Regulations. 67. wydanie. Montreal: IATA.

International Civil Aviation Organization (2022). Annex 14 to the Convention on International Civil Aviation: Aerodromes. Volume I: Aerodrome Design and Operations. 9. wydanie. Montreal: ICAO.

Komisja Europejska (2025). EU Stockpiling Strategy: Boosting the EU's Material Preparedness for Crises. COM(2025) 528 final. Bruksela: Komisja Europejska.

Komisja Europejska i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (2022). Action Plan on Military Mobility 2.0. JOIN(2022) 48 final. Bruksela: Komisja Europejska.

Ministerstwo Infrastruktury (2019). Strategia Zrównoważonego Rozwoju Transportu do 2030 roku. Warszawa: Ministerstwo Infrastruktury.

Ministerstwo Infrastruktury (b.r.). Krajowy Program Kolejowy do 2030 roku z perspektywą do roku 2032. Warszawa: Ministerstwo Infrastruktury.

NATO (2024a). Defence-Critical Supply Chain Security Roadmap. Brussels: NATO Headquarters.

NATO (2024b). Resilience, civil preparedness and Article 3. Brussels: NATO Headquarters.

NATO (2025). NATO's role in logistics. Brussels: NATO Headquarters.

NATO Standardization Office (2003). STANAG 2021: Military load classification of bridges, ferries, rafts and vehicles. Edition 6. Brussels: NATO.

OTIF (2025). Regulations concerning the International Carriage of Dangerous Goods by Rail (RID). 2025 Edition, Appendix C to COTIF. Bern: Intergovernmental Organisation for International Carriage by Rail.

PKP Polskie Linie Kolejowe S.A. (b.r.). Raport Roczny 2024. Warszawa: PKP PLK S.A.

Port Polska (2026). Start wspólnych projektów Port Polska i CUPT. Pasażerowie zyskają więcej połączeń i tańsze bilety. Komunikat prasowy z dnia 6 lutego 2026 r.

Port Polska (b.r.a). Kolejowy Model Mikrosymulacyjny (KMM). <https://portpolska.pl>

Port Polska (b.r.b). Pasażerski Model Transportowy. <https://portpolska.pl>

Rządowa Agencja Rezerw Strategicznych (b.r.). Nasze zadania. <https://www.rars.gov.pl>

Rządowe Centrum Bezpieczeństwa (2024). Systemy infrastruktury krytycznej. Gov.pl. <https://www.gov.pl/web/rcb>

Rządowe Centrum Bezpieczeństwa (b.r.a). Infrastruktura krytyczna. Warszawa: RCB.

Rządowe Centrum Bezpieczeństwa (b.r.b). Narodowy Program Ochrony Infrastruktury Krytycznej. Warszawa: RCB.

Strategic Airlift Capability (b.r.). Member Nations – Poland. <https://sacprogram.org/about-us/member-nations>

UNECE (2025). Agreement concerning the International Carriage of Dangerous Goods by Road (ADR). Geneva: United Nations Economic Commission for Europe.

Urząd Transportu Kolejowego (b.r.). Sprawozdanie z funkcjonowania rynku transportu kolejowego w 2024 r. Warszawa: UTK.

Akty prawne i oficjalne dokumenty rządowe

Decyzja Nr 26/MON Ministra Obrony Narodowej z dnia 11 marca 2025 r. w sprawie wprowadzenia do użytku w resorcie obrony narodowej „Wytycznych w sprawie poprawy bezpieczeństwa energetycznego, efektywności energetycznej kompleksów wojskowych i obiektów budowlanych w resorcie obrony narodowej”. Dz. U. MON z 2025 r., poz. 33.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS2). Dz.Urz. UE L 333 z 27.12.2022, s. 80.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (CER). Dz.Urz. UE L 333 z 27.12.2022, s. 164.

Ministerstwo Energii (2026). Krajowy Plan w dziedzinie Energii i Klimatu do 2030 r. z perspektywą do 2040 r. Warszawa: Ministerstwo Energii.

Obwieszczenie Ministra Rozwoju i Technologii z dnia 15 kwietnia 2022 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Infrastruktury w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie. Dz.U. 2022 poz. 1225.

Rada Ministrów (2015). Uchwała nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej (ze zm.).

Rada Ministrów (2019). Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Warszawa: Rada

Ministrów.

Rada Ministrów (2023). Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1: Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje. Warszawa: RCB.

Rozporządzenie Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznające niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu. Dz.Urz. UE L 187 z 26.06.2014, s. 1.

Rozporządzenie Komisji (UE) 2016/631 z dnia 14 kwietnia 2016 r. ustanawiające kodeks sieci dotyczący wymogów w zakresie przyłączenia jednostek wytwórczych do sieci (NC RfG). Dz.Urz. UE L 112 z 27.04.2016, s. 1.

Rozporządzenie Ministra Energii z dnia 23 listopada 2016 r. w sprawie szczegółowych wymagań dotyczących prowadzenia ruchu podziemnych zakładów górniczych. Dz.U. 2017 poz. 1118.

Rozporządzenie Ministra Klimatu i Środowiska z dnia 22 marca 2023 r. w sprawie szczegółowych warunków funkcjonowania systemu elektroenergetycznego. Dz.U. 2023 poz. 819.

Rozporządzenie Ministra Klimatu i Środowiska z dnia 29 listopada 2022 r. w sprawie sposobu kształtowania i kalkulacji taryf oraz sposobu rozliczeń w obrocie energią elektryczną. Dz.U. 2022 poz. 2505.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/821 z dnia 20 maja 2021 r. ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania. Dz.Urz. UE L 206 z 11.06.2021, s. 1.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1679 z dnia 13 czerwca 2024 r. w sprawie unijnych wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej. Dz.Urz. UE L 2024/1679 z 28.06.2024.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi (Cyber Resilience Act). Dz.Urz. UE L 2024/2847 z 20.11.2024.

Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne. Dz.U. z 2024 r., poz. 266 ze zm.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Dz.U. z 2007 r., Nr 89, poz. 590 ze zm.

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. t.j. Dz.U. z 2025 r., poz. 1209 ze zm.

Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych. t.j. Dz.U. z 2026 r., poz. 793 ze zm.

Ustawa z dnia 17 grudnia 2020 r. o rezerwach strategicznych. Dz.U. z 2021 r., poz. 255 ze zm.

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny. Dz.U. z 2022 r., poz. 655 ze zm.

Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. Dz.U. z 2026 r., poz. 252.

Źródła internetowe i portale branżowe

AGH (2024). Sprawozdanie z działalności uczelni 2024. https://www.agh.edu.pl/home/ckim/dokumenty/Sprawozdania_wladz/Sprawozdanie_z_dzialalnosci_uczelni_2024.pdf

AGH (b.r.). Rusza jedyny w Polsce ośrodek innowacji obronnych NATO DIANA. <https://www.agh.edu.pl/aktualnosci/detail/rusza-jedyny-w-polsce-osrodek-innowacji-obronnych-nato-diana>

CEZAMAT (b.r.). O nas – CEZAMAT Politechnika Warszawska. <https://cezamat.pw.edu.pl/o-nas/cezamat/>

ENISA (b.r.). SMEs Cybersecurity. <https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity>

EU-NATO Task Force on the Resilience of Critical Infrastructure (2023). Final Assessment Report. <https://www.nato.int/en/news-and-events/articles/news/2023/06/29/nato-and-european-union-release-final-assessment-report-on-resilience-of-critical-infrastructure>

European Defence Agency (b.r.). Guidelines facilitating SMEs' access to the defence market. <https://eda.europa.eu/docs/default-source/brochures/guidelines-smes-access-defence-market.pdf>

FinancialCraft Analytics (2025). Rynek zbrojeniowy w Polsce w 2024 roku. <https://financialcraft.pl/rynek-zbrojeniowy-w-polsce-2024-raport/>

Fort Kraków (b.r.). Ośrodek Innowacji NATO DIANA. <https://diana.krakow.pl/pl/>; <https://fortkrakow.pl/>

Główny Urząd Statystyczny (2025). Informacja Głównego Urzędu Statystycznego w sprawie skorygowanego szacunku produktu krajowego brutto za 2024 r. <https://stat.gov.pl/obszary-tematyczne/rachunki-narodowe/roczne-rachunki-narodowe/informacja-glownego-urzedu-statystycznego-w-sprawie-skorygowanego-szacunku-produktu-krajowego-brutto-za-2024-r-9,11.html>

Huta Stalowa Wola (b.r.a). 155 mm Samobieżna Haubica Krab. <https://www.hsw.pl/produkty/155-mm-samobieznahaubica-krab/>

- Huta Stalowa Wola (b.r.b). Bojowy Wóz Piechoty Borsuk. <https://www.hsw.pl/produkty/nowy-bojowy-plywajacy-woz-piechoty-borsuk/>
- MILMAG (b.r.). Polska Grupa Zbrojeniowa zacieśnia współpracę z Politechniką Warszawską. <https://milmag.pl/polska-grupa-zbrojeniowa-zaciesnia-wspolprace-z-politechnika-warszawska/>
- Ministerstwo Cyfryzacji (b.r.). Dostawcy wysokiego ryzyka – sprawdź najważniejsze informacje. <https://www.gov.pl/web/cyfryzacja/dostawcy-wysokiego-ryzyka---sprawdz-najwazniejsze-informacje>
- Ministerstwo Spraw Zagranicznych (2025). Eksport uzbrojenia i sprzętu wojskowego z Polski. Raport za rok 2024. <https://www.gov.pl/web/dyplomacja/eksport-uzbrojenia-i-sprzetu-wojskowego-z-polski-raport-za-rok-2024>
- NATO (2026). The Secretary General's Annual Report 2025 (Annex III: Defence Expenditure of NATO Countries). <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/annual-reports/sgar25-en.pdf>
- NATO DIANA (b.r.a). Accelerator Programme. <https://www.diana.nato.int/accelerator-programme.html>
- NATO DIANA (b.r.b). NATO Defence Innovation Accelerator for the North Atlantic. <https://www.diana.nato.int/index.html>
- PIT-RADWAR (b.r.). Projekty współfinansowane z Narodowego Centrum Badań i Rozwoju. <https://www.pitradwar.com/oferta/515,projekty-wspolfinansowane-z-narodowego-centrum-badan-i-rozwoju>
- Politechnika Gdańska (2023). Kolejna misja Głuptaka z PG trafi na nowe niszczyciele min typu Kormoran II. <https://pg.edu.pl/aktualnosci/2023-07/kolejna-misja-gluptaka-z-pg-trafi-na-nowe-niszczyciele-min-typu-kormoran-ii>
- Politechnika Poznańska (b.r.). Centrum Kształcenia i Technologii Bezzałogowych Statków Powietrznych (CKiT-BSP). <https://put.poznan.pl/ckit-bsp>
- Politechnika Warszawska (b.r.a). Współpraca naukowo-badawcza Wydziału MEiL PW z Wojskowym Instytutem Technicznym Uzbrojenia. Biuletyn PW. <https://www.biuletyn.pw.edu.pl>
- Politechnika Warszawska (b.r.b). Osiągnięcia Zakładu Mechaniki i Technik Uzbrojenia. <https://www.mt.pw.edu.pl/zmi-tu/Osiagniecia>
- Portal Obronny (b.r.). Z PGZ współpracuje 11 981 kooperantów – będzie ich znacznie więcej. <https://portalobronny.se.pl/przemysl-zbrojeniowy/z-pgz-wspolpracuje-11-981-kooperantow-bedzie-ich-znacznie-wiecej-aa-HWwP-Lqie-6ncq.html>
- SIMBA Chain (2026). Digital Thread. <https://simbachain.com/digital-thread/>
- SIPRI (2025). The SIPRI Top 100 Arms-producing and Military Services Companies, 2024. <https://www.sipri.org/publications/2025/sipri-fact-sheets/sipri-top-100-arms-producing-and-military-services-companies-2024>
- WB Group (b.r.). System Amunicji Krążącej WARMATE. <https://www.wbgroup.pl/produkt/system-amunicji-krazacej-warmate/>
- WNP.pl (b.r.). Gliwice: Politechnika Śląska nawiązała współpracę z Zakładami Bumar-Łabędy. <https://www.wnp.pl/rynki/gliwice-politechnika-slaska-nawiazala-wspolprace-z-zakladami-bumar-labedy,929825.html>

WYKAZ SKRÓTÓW I OZNACZEŃ

ADR – umowa dotycząca międzynarodowego przewozu drogowego towarów niebezpiecznych

AIDC – automatyczna identyfikacja i gromadzenie danych (Automatic Identification and Data Capture)

AIP – Zbiór Informacji Lotniczych (Aeronautical Information Publication)

AI – sztuczna inteligencja (Artificial Intelligence)

AHS – armatohaubica samobieżna

AMW – Agencja Mienia Wojskowego

API – interfejs programowania aplikacji (Application Programming Interface)

BCP – plan ciągłości działania (Business Continuity Plan)

BDOT10k – Baza Danych Obiektów Topograficznych

BGK – Bank Gospodarstwa Krajowego

BOM – wykaz materiałowy wyrobu (Bill of Materials)

BWP – bojowy wóz piechoty

CUPT – Centrum Unijnych Projektów Transportowych

CSIRT – zespół reagowania na incydenty bezpieczeństwa komputerowego (Computer Security Incident Response Team)

EDI – elektroniczna wymiana danych (Electronic Data Interchange)

EPC – Elektroniczny Kod Produktu (Electronic Product Code)

EPCIS – standard wymiany danych o zdarzeniach związanych z przepływem produktów (Electronic Product Code Information Services)

ERP – system planowania zasobów przedsiębiorstwa (Enterprise Resource Planning)

ERTMS – Europejski System Zarządzania Ruchem Kolejowym (European Rail Traffic Management System)

ETCS – Europejski System Sterowania Pociągami (European Train Control System)

GDDKiA – Generalna Dyrekcja Dróg Krajowych i Autostrad

GLN – Globalny Numer Lokalizacyjny (Global Location Number)

GNSS – globalny system nawigacji satelitarnej (Global Navigation Satellite System)

GPR – Generalny Pomiar Ruchu

GPS – Globalny System Pozycjonowania (Global Positioning System)

GSI – globalny system standardów identyfikacji, gromadzenia i wymiany danych

GSM-R – kolejowy system cyfrowej łączności radiowej (Global System for Mobile Communications – Railway)

GTIN – Globalny Numer Jednostki Handlowej (Global Trade Item Number)

HSW – Huta Stalowa Wola S.A.

ICT – technologie informacyjno-komunikacyjne (Information and Communication Technologies)

IKMR – Intermodalny Krajowy Model Ruchu

IoT – Internet rzeczy (Internet of Things)

ITS – inteligentne systemy transportowe (Intelligent Transport Systems)

JIM – Jednolity Indeks Materiałowy

JWCD – jednostki wytwórcze centralnie dysponowane

KET – Karta Efektywnej Transformacji Sieci Dystrybucyjnych Polskiej Elektroenergetyki

KSE – Krajowy System Elektroenergetyczny

LNG – skroplony gaz ziemny (Liquefied Natural Gas)

MAP – Ministerstwo Aktywów Państwowych

MEMS – mikrosystemy elektromechaniczne (Micro-Electro-Mechanical Systems)

MLC – wojskowa klasyfikacja obciążenia (Military Load Classification)

MON – Ministerstwo Obrony Narodowej

MRO – obsługa techniczna, naprawy i remonty (Maintenance, Repair and Overhaul)

NATO – Organizacja Traktatu Północnoatlantyckiego (North Atlantic Treaty Organization)

NEW/NSE – Narodowy Element Wsparcia (National Support Element)

NIS2 – dyrektywa Unii Europejskiej w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa

NRAA – Krajowa Ocena Wystarczalności Zasobów Wytwórczych (National Resource Adequacy Assessment)

OG – oddział gospodarczy

OSD – operator systemu dystrybucyjnego

OZE – odnawialne źródła energii

P1 – główni dostawcy strategicznych podsystemów

P2 – dostawcy krytycznych komponentów specjalistycznych

P3 – dostawcy podstawowych materiałów i komponentów

P4 – dostawcy materiałów, w tym surowców krytycznych

PC – główny wykonawca i integrator systemu (Prime

Contractor), odpowiedzialny za realizację kontraktu i dostarczenie produktu końcowego	WOM – wskaźnik odtworzenia majątku
PEP2040 – Polityka energetyczna Polski do 2040 r.	ZMR – Zintegrowany Model Ruchu
PGZ – Polska Grupa Zbrojeniowa S.A.	ZWSI RON – Zintegrowany Wieloszczeblowy System Informatyczny Resortu Obrony Narodowej
PHA – wstępna analiza zagrożeń (Preliminary Hazard Analysis)	u.k.s.c. – ustawa o krajowym systemie cyberbezpieczeństwa
PIAST – Polish ImAging SaTellites – projekt nanosateli-tarnej konstelacji rozpoznania obrazowego	u.o.O. – ustawa o obronie Ojczyzny
PKB – produkt krajowy brutto	u.o.l. – ustawa o ochronie ludności i obronie cywilnej
PKP PLK – PKP Polskie Linie Kolejowe S.A.	u.r.s. – ustawa o rezerwach strategicznych
PKW – Polski Kontyngent Wojskowy	u.z.k. – ustawa o zarządzaniu kryzysowym
PLN – polski złoty	u.z.r.p.n.g. – ustawa o zapasach ropy naftowej, produk-tów naftowych i gazu ziemnego oraz zasadach po-stępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym
PMT – Pasażerski Model Transportowy	
PRSP – Plan Rozwoju Systemu Przesyłowego	
PSE – Polskie Sieci Elektroenergetyczne S.A.	
RARS – Rządowa Agencja Rezerw Strategicznych	
RFID – identyfikacja radiowa (Radio-Frequency Identi-fication)	
RID – regulamin międzynarodowego przewozu koleja-mi towarów niebezpiecznych	
RTGMS – System Monitorowania Sygnałów GNSS w Pol-sce w Czasie Rzeczywistym (Real-time GNSS Monito-ring System for Poland)	
SBOM – wykaz komponentów oprogramowania (So-ftware Bill of Materials)	
SHM – monitorowanie stanu technicznego konstrukcji (Structural Health Monitoring)	
SIPRI – Sztokholmski Międzynarodowy Instytut Badań nad Pokojem (Stockholm International Peace Research Institute)	
SMR – mały reaktor modułowy (Small Modular Reactor)	
SSCC – Seryjny Numer Jednostki Logistycznej (Serial Shipping Container Code)	
STANAG – porozumienie standaryzacyjne NATO (NATO Standardization Agreement)	
SpW – sprzęt wojskowy	
ŚB – środki bojowe	
ŚM – środki materiałowe	
SZ RP – Siły Zbrojne Rzeczypospolitej Polskiej	
TEN-T – transeuropejska sieć transportowa (Trans-Eu-ropean Transport Network)	
TMS – system zarządzania transportem (Transportation Management System)	
TMT – Towarowy Model Transportowy	
TRL – poziom gotowości technologicznej (Technology Readiness Level)	
UE – Unia Europejska	
UPRP – Urząd Patentowy Rzeczypospolitej Polskiej	
UTK – Urząd Transportu Kolejowego	
WMS – system zarządzania magazynem (Warehouse Management System)	

SPIS RYSUNKÓW

Rys. 2.1. Struktura branżowa narodowego przemysłu obronnego	33
Rys. 2.2. Komponenty produkcyjne pocisku 155 mm	34
Rys. 2.3. Bojowy wóz piechoty BORSUK	35
Rys. 2.4. Amunicja krążąca Warmate	36
Rys. 2.5. Armatohaubica AHS Krab (155 mm)	37
Rys. 2.6. Armatohaubica K9 Thunder	38
Rys. 2.7. Model domen zależności dostaw BMS/C4I	44
Rys. 2.8. Schemat łańcucha dostaw w polskim przemyśle obronnym	47
Rys. 2.9. Macierz zapotrzebowania na surowce wykorzystywane w produkcji wybranych systemów uzbrojenia	61
Rys. 2.10. Ocena ryzyka dostaw surowców	62
Rys. 2.11. Uporządkowany poziom istotności kluczowych surowców	63
Rys. 4.1. Rozkład ruchu na autostradach, drogach ekspresowych, krajowych i wojewódzkich – modele PMT oraz IKMR.	83
Rys. 4.2. Gęstość dróg krajowych i wojewódzkich w powiatach [km/100 km ²]	84
Rys. 4.3. Dostępność infrastruktury magazynowej na tle jednostek wojskowych w Polsce	87
Rys. 4.4. Zainstalowana moc obecnie eksploatowanych konwencjonalnych źródeł wytwórczych	92
Rys. 4.5. Prognoza luki mocy sterowalnych w KSE.	93
Rys. 4.6. Struktura wiekowa wybranych elementów sieci dystrybucyjnej; stan na koniec 2025 r.	95
Rys. 4.7. Nakłady prognozowane do realizacji przez OSD w kategorii inwestycje konieczne w ujęciu łącznym (a) oraz w podziale na główne kategorie inwestycyjne (b); perspektywa realizacji to 2030 r.	95
Rysunek 4.8. Łańcuchy dostaw do jednostek i instytucji wojskowych	100
Rys. 5.1. Cyberzagrożenia stanowiące największe ryzyko dla firm w Polsce	116
Rys. 5.2. Uproszczony model współzależności infrastruktury fizycznej i cyfrowej w obronnym łańcuchu dostaw	125
Rys. 5.3. Przykładowa propagacja zakłócenia cyber-fizycznego od infrastruktury wspierającej do dostaw dla Sił Zbrojnych RP	126
Rys. 6.1. Uogólniony model przepływu technologii nauka-przemysł-wojsko	137

SPIS TABEL

Tab. 2.1. Możliwości lokowania produkcji i budowania łańcuchów dostaw w polskim przemyśle obronnym (2026-2030)	39
Tab. 2.2. Ocena potencjału finansowego PGZ i Grupy WB względem wskaźników UE	57
Tab. 3.1. Dominujące ryzyka w zależności od modelu łańcucha dostaw	67
Tab. 3.2. Kluczowe obszary ryzyka wewnętrznego i zewnętrznego w łańcuchach dostaw sprzętu wojskowego	70
Tab. 3.3. Przykłady materializacji ryzyka w różnych obszarach oraz ich potencjalne skutki w łańcuchach dostaw polskiego przemysłu obronnego	71
Tab. 3.4. Macierz ryzyka dla polskiego przemysłu obronnego	73
Tab. 3.5. Znaczenie poszczególnych rodzajów ryzyka dla wybranych kategorii sprzętu wojskowego	74
Tab. 3.6. Strategie i metody zarządzania ryzykiem w polskim przemyśle obronnym według obszarów	76
Tab. 4.1. Najważniejsze grupy ryzyka i możliwe kierunki jego ograniczania	80
Tab. 4.2. Syntetyczna macierz oceny infrastruktury podwójnego zastosowania	82
Tab. 4.3. Warstwowy model infrastruktury logistycznej dla łańcuchów dostaw obronności	88
Tab. 4.4. Rejestr ryzyk w zakresie zapewnienia mobilności strategicznej i dostaw sprzętu wojskowego oraz kierunki optymalizacji	89
Tab. 5.1. Typowe zagrożenia cyberbezpieczeństwa w łańcuchach dostaw	115
Tab. 5.2. Kluczowe węzły i zależności infrastrukturalne wymagające oceny odporności.	125
Tab. 5.3. Minimalny zestaw wskaźników odporności infrastrukturalnej.	127
Tab. 6.1. Szacunkowa liczba kooperantów w zależności od poziomu dostawcy w przypadku PGZ S.A.	134
Tab. 6.2. Zestawienie największych zależności technologicznych i przemysłowych Polski w czterech analizowanych segmentach uzbrojenia	134
Tab. 6.3. Najbardziej krytyczne zależności według segmentów	135
Tab. 6.4. Zestawienie kluczowych obszarów współpracy przemysł – nauka dla wybranych uczelni wyższych technicznych w kraju	140
Tab. 6.5. Ryzyka polonizacji łańcucha dostaw – podejście systemowe	142
Tab. 6.6. Zbiorcza ocena ryzyka polonizacji	145



WYDAWCA

Fundacja Instytut Studiów Wschodnich
ul. Solec 85, 00-382 Warszawa
tel.: +48 22 583 11 00, fax: +48 22 583 11 50
e-mail: forum@isw.org.pl
www.forum-ekonomiczne.pl

OPRACOWANIE GRAFICZNE I SKŁAD

Szymon Tomaszewski

WARSZAWA 2026

Fundacja Instytut Studiów Wschodnich

ul. Solec 85, 00-382 Warszawa
tel. (+48 22) 583 11 00
e-mail: forum@isw.org.pl
www.forum-ekonomiczne.pl

Warszawa 2026