

JAK ZBUDOWAĆ ODPORNOSC PAŃSTWA WE WSPÓŁPRACY Z PRZEDSIĘBIORCAMI





Instytut
Sobieskiego
ul. Lipowa 1a lok. 20
00-316 Warszawa

sobieski@sobieski.org.pl
www.sobieski.org.pl



Instytut
Wschodniej Flanki

Institut du flanc
est de l'OTAN
/ Chau.d'Alsemberg 8971180 Uccle,
Belgia

kontakt@wschodniaflanka.pl
www.wschodniaflanka.pl



OLDMAN
SAGE

OLDMAN SAGE
- Draba, Ginel i Wspólnicy, sp.k.
ul. Jasna 7/37
00-007 Warszawa

sekretariat@oldmansage.org
www.oldmansage.org



RADA POLSKICH
PRZEDSIĘBIORCÓW

Rada Polskich
Przedsiębiorców

JAK ZBUDOWAĆ ODPORNOŚĆ PAŃSTWA WE WSPÓŁPRACY Z PRZEDSIĘBIORCAMI

Ines Biegaj
Rafał Brzoska
Maciej Dachowski
Robert Draba
Michał Dworczyk
Elżbieta Jakubiak
Bartosz Marczuk
Krzysztof Michalski
Piotr Woyke

Redakcja językowa, korekta
Agata Sawicka-Korgol

©Copyright by Instytut Sobieskiego 2025
ISBN 978-83-68374-14-8

Projekt i produkcja: Piotr Perzyna

nowe media 24.pl

RAPORT
2025

JAK ZBUDOWAĆ ODPORNOŚĆ PAŃSTWA

WE WSPÓŁPRACY Z PRZEDSIĘBIORCAMI

Ines Biegaj
Rafał Brzoska
Maciej Dachowski
Robert Draba
Michał Dworczyk
Elżbieta Jakubiak
Bartosz Marczuk
Krzysztof Michalski
Piotr Woyke

SPIS TREŚCI



SŁOWO WSTĘPNE	6
OD AUTORÓW	8
1. BADANIA GOTOWOŚCI FIRM I PRACOWNIKÓW DO BUDOWANIA ODPORNOŚCI PAŃSTWA	10
UDZIAŁ W SZKOLENIACH I KOMPETENCJE PRACOWNIKÓW	11
POSTAWY WOBEC OBRONNOŚCI W MIEJSCU PRACY	14
OBAWY ZWIĄZANE Z MOBILIZACJĄ	14
GOTOWOŚĆ DO TWORZENIA GRUP SAMOOBRONY	15
CO ZWIĘKSZA ZAANGAŻOWANIE	16
WNIOSKI I REKOMENDACJE	18
2. WYZWANIA ZWIĄZANE Z RYNKIEM PRACY	20
ILU POLAKÓW PRACUJE	21
NA JAKICH KONTRAKTACH	22
W JAKICH BRANŻACH	24
ROZDROBNIENIE FIRM	27
WNIOSKI I KONKLUZJE	28
3. JAK JEST W INNYCH KRAJACH	30
SZWECJA- MODEL OBRONY TOTALNEJ	31
FINLANDIA - BEZPIECZEŃSTWO POWSZECHNE	32
SZWAJCARIA - SUBSYDIARNOŚĆ JAKO MODEL	33
UKRAINA - SZYBKA ADAPTACJA, PARTNERSTWO Z BIZNESEM	34
WIELKA BRYTANIA - MOCNE WŁĄCZANIE FIRM W SFERĘ BEZPIECZEŃSTWA	35
KOREA POŁUDNIOWA - PEŁNA INTEGRACJA Z BIZNESEM	37
KONKLUZJE I WNIOSKI	38
4. KONCEPCJA WŁĄCZENIA SEKTORA PRYWATNEGO W TWORZENIE SYSTEMU BEZPIECZEŃSTWA PAŃSTWA	39
FIRMY WESPRĄ BEZPIECZEŃSTWO	41
GŁÓWNE ZAŁOŻENIA NOWEGO SYSTEMU	42
TRZY MECHANIZMY SPINAJĄCE SYSTEM	44
O AUTORACH	62
O WYDAWCACH	68

SŁOWO WSTĘPNE



Żyjemy w czasie niestabilności i nieustannego napięcia, w świecie, który przyspieszył do granic możliwości. Globalna gospodarka, technologia, geopolityka i bezpieczeństwo spłótły się ze sobą tak ściśle, że żadne państwo ani żadna firma nie mogą już działać w izolacji. Dziś nie ma bezpieczeństwa państwa bez odporności i siły jego gospodarki, nie ma też odpornej gospodarki bez silnego, elastycznego biznesu, który potrafi działać w warunkach ryzyka, niepewności i zmiany.

Polska wchodzi w okres, w którym musi zdecydować, czy wykorzysta okno możliwości, by zbudować system nowoczesny, oparty na współpracy i zaufaniu, czy ugrzęźnie w biurokracji i doraźnych rozwiązaniach. To nie tylko wybór administracyjny – to decyzja cywilizacyjna. Od tego, jak połączymy siłę instytucji publicznych z dynamiką sektora prywatnego, zależy nasza przyszłość – bezpieczeństwo, rozwój, konkurencyjność i zdolność przetrwania w świecie coraz częstszych kryzysów.

Zawsze powtarzam, że potrzebujemy mniej kontroli, a więcej zaufania i współodpowiedzialności. Biurokracja nie stworzy innowacji, a nadmierna regulacja nigdy nie zbuduje odporności. Tylko wolność w działaniu, wspierana przez mądre państwo, pozwoli stworzyć system zdolny reagować szybciej niż zagrożenia, które go otaczają. Potrzebujemy nie kolejnych procedur, lecz więcej ludzi gotowych brać odpowiedzialność w biznesie, administracji i codziennym życiu.

Raport ten jest pierwszym w Polsce tak kompleksowym opracowaniem, które w sposób praktyczny i systemowy pokazuje, jak połączyć potencjał państwa i biznesu w budowie odporności kraju. To nie kolejna analiza ani zbiór postulatów, ale konkretna mapa drogowa – wskazująca, jak współdziałanie sektora publicznego i prywatnego może realnie wzmacniać bezpieczeństwo narodowe. Raport, który oddajemy w Państwa ręce, dowodzi, że w Polsce możliwe jest myślenie o bezpieczeństwie nie tylko w kategoriach instytucji i przepisów, lecz także relacji, zaufania i odpowiedzialności.

Nie mamy czasu na wahanie. Świat nie zwolni, żebyśmy mogli się dostosować. To my musimy nadążyć, działając odważnie, szybko i odpowiedzialnie. Jeśli dziś połączymy potencjał państwa, przedsiębiorców i obywateli, możemy stworzyć coś unikalnego: system, który nie tylko reaguje na kryzysy, ale potrafi z nich wychodzić silniejszy.

Odporność, przygotowanie i współodpowiedzialność – to trzy słowa, które powinny definiować nasze myślenie o przyszłości. Wierzę, że Polska może być krajem, który nie tylko przetrwa w czasach niepewności, ale stanie się wzorem, jak budować siłę na fundamencie wolności, innowacji i współpracy. Prawdziwe bezpieczeństwo nie rodzi się z przepisów, lecz z zaufania, determinacji i odwagi ludzi, którzy potrafią działać razem.



*Rafał
Brzoska*

OD AUTORÓW



Oddajemy w Państwa ręce kolejny raport poświęcony budowie systemu odporności państwa na wypadek kryzysów lub wojny. Tym razem przedstawiamy unikalne w Polsce opracowanie dotyczące budowania tego systemu we współpracy z sektorem prywatnym. Bezpieczeństwo państwa jest wartością fundamentalną, a reformy powinny zmierzać w kierunku zaangażowania zasobów wszystkich istotnych interesariuszy – Sił Zbrojnych RP, pozostałych służb mundurowych, administracji centralnej i samorządowej, organizacji społecznych, a także przedsiębiorstw.

Istotny kontekst dla tych działań stanowi publikacja z czerwca 2025 r. – raport Instytutu Sobieskiego i Instytutu Wschodniej Flanki, w którym przedstawiono propozycję całościowej reformy tworzenia rezerw osobowych na potrzeby bezpieczeństwa państwa. Postulowane utworzenie Powszechnej Służby Państwowej, której architektura byłaby oparta na wspólnej bazie danych obywateli świadczących różne formy służby na rzecz Ojczyzny, otwiera nowe możliwości również z perspektywy pracodawców i pracowników.

Pogłębiając tę koncepcję, eksperci Instytutu Sobieskiego, Instytutu Wschodniej Flanki, kancelarii Oldman Sage i Rady Polskich Przedsiębiorców zainicjowali projekt, który miał dać odpowiedź na pytanie: w jaki sposób biznes może wspomóc system bezpieczeństwa narodowego RP?

Podstawą analiz stały się dane zebrane podczas badań rodzimego rynku pracy oraz opinie przedstawicieli sektora prywatnego dotyczące kwestii związanych z bezpieczeństwem państwa. Autorzy wzięli pod uwagę również doświadczenia państw demokratycznych i wolnorynkowych uznawanych za wyróżniające się przykłady, a także wnioski płynące z sytuacji znajdującej się w stanie wojny Ukrainy.

W rezultacie opracowano zestaw rekomendacji dla instytucji państwowych oraz propozycji ich praktycznej realizacji poprzez odpowiednie zmiany prawne, organizacyjne i funkcjonalne. Wszystkie rozwiązania łączy dążenie do jak najlepszego wykorzystania zasobów już obecnie dostępnych z perspektywy administracji rządowej, bez tworzenia dodatkowych obciążeń budżetowych. Wypracowana koncepcja ma charakter przekrojowy i pozwoli:

- efektywnie zaangażować przedsiębiorców w funkcjonowanie państwa i społeczeństwa w ramach procesu zarządzania kryzysowego;
- stworzyć możliwie przewidywalne otoczenie regulacyjne w wymiarze zarządzania kryzysowego, zarówno dla państwa, jak i dla pracodawców i pracowników;
- uporządkować przepisy i usprawnić rozwiązania służące efektywnej współpracy między państwem a przedsiębiorcami.

Mamy nadzieję, że zaprezentowana przez nas koncepcja stanie się impulsem do debaty na temat racjonalnego włączenia przedsiębiorstw w system budowy odporności państwa. Liczymy również, że stanie się inspiracją dla decydentów przy tworzeniu skutecznych mechanizmów realizacji tego celu.

1. BADANIA GOTOWOŚCI FIRM I PRACOWNIKÓW DO BUDOWANIA ODPORNOŚCI PAŃSTWA

Ines Biegaj
Maciej Dachowski



Na wstępie naszego raportu chcielibyśmy przedstawić unikatowe badania dotyczące gotowości – zarówno firm, jak i pracowników – do budowania wewnątrz przedsiębiorstw modułu odporności państwa na wypadek kryzysów, tj. gotowości sektora prywatnego do udziału w systemie bezpieczeństwa i obrony cywilnej.

UDZIAŁ W SZKOLENIACH I KOMPETENCJE PRACOWNIKÓW

Zebrane w badaniu dane wskazują, że znacząca część pracowników sektora prywatnego ma już pewne doświadczenia związane ze szkoleniami proobronnymi lub jest nimi zainteresowana. Ponad połowa ankietowanych pracowników (52,3%) deklaruje, iż brali udział w zajęciach na strzelnicy i mieli kontakt z bronią palną. Aktualne przeszkolenie z pierwszej pomocy ma 36,3% pracowników, a kolejne 34,7% nie ma takiego certyfikatu, lecz wyraża chęć jego zdobycia w przyszłości. Oznacza to, że łącznie ponad 70% zatrudnionych posiada lub chce zdobyć umiejętności ratownicze. Warto zauważyć, że tylko 29% badanych nie ma ani przeszkolenia medycznego, ani takiego zainteresowania. Samoocena kompetencji w zakresie udzielania pierwszej pomocy jest jednak umiarkowana – niemal połowa pracowników (44,9%) ocenia swoje umiejętności jako przeciętne, natomiast 19,3% określa je jako słabe, a 5,7% jako bardzo słabe; tylko 30% badanych ocenia swoje kompetencje pierwszopomocowe dobrze lub bardzo dobrze. Wyniki te sugerują, że większość pracowników dostrzega u siebie braki, co współgra z dużym zainteresowaniem szkoleniami w tym zakresie.

Po stronie pracodawców widać rosnącą świadomość znaczenia takich szkoleń, choć formalna polityka ich wspierania nie jest jeszcze powszechna. Tylko 40% firm zadeklarowało, że prowadzi lub planuje wdrożyć oficjalną politykę wspierającą uczestnictwo pracowników w szkoleniach obronnych (pierwsza pomoc, samoobrona, posługiwanie się bronią), podczas gdy 60% firm nie wypracowało w tej kwestii żadnych rozwiązań. Niemniej wiele przedsiębiorstw już organizuje wybrane kursy. Szkolenia z pierwszej pomocy przeprowadzono w 59,2% badanych firm. Znacznie rzadziej dotąd odbywały się firmowe treningi z samoobrony (10,8% firm) czy posługiwania się bronią (10% firm). Ponad jedna trzecia pracodawców (37,5%) przyznała, że żadne z tego typu szkoleń nie odbyło się dotąd w ich firmie. Dane te wskazują na istotną przestrzeń do zwiększenia zaangażowania przedsiębiorstw w podnoszenie kompetencji obronnych załóg.

Co istotne, obie badane grupy dostrzegają wymierne korzyści płynące z podnoszenia takich kwalifikacji. Pracodawcy wprost wskazywali, w jakich obszarach widzą największą wartość organizowania szkoleń

obronnych dla pracowników – dla 70,8% firm główną zaletą jest posiadanie przeszkolonej kadry (co przekłada się na wyższe bezpieczeństwo i przygotowanie na sytuacje kryzysowe), 38,3% postrzega takie szkolenia jako dodatkowy benefit dla pracowników, zwiększający atrakcyjność miejsca pracy, a 21,7% uważa, że oferowanie szkoleń obronnych podnosi prestiż i atrakcyjność firmy wśród potencjalnych kandydatów do pracy. Tylko 11,7% wskazało inne, indywidualne korzyści.

Z punktu widzenia pracowników możliwość udziału w tego typu zajęciach organizowanych przez pracodawcę spotyka się z ogromnym odzewem – **aż 83,5% pracowników deklaruje chęć uczestnictwa w szkoleniach obronnych organizowanych przez własny zakład pracy.** Jedynie co szósty pracownik (16,5%) nie byłby takim szkoleniem zainteresowany. Te wyniki jednoznacznie pokazują, że wśród załóg istnieje wysoki popyt na rozwój kompetencji obronnych, który pracodawcy mogą wykorzystać, wpisując się jednocześnie w szerszy system podnoszenia odporności kraju.

KOGO I JAK ZBADANO

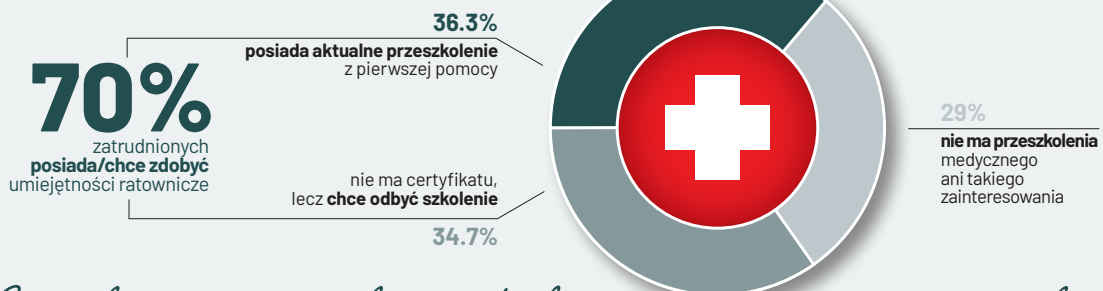
Badanie zostało zrealizowane w ostatnim kwartale 2024 r. za pomocą dwóch równoległych kwestionariuszy online skierowanych osobno do pracodawców (N=120) oraz pracowników (N=841) sektora prywatnego. Dobór próby miał charakter celowy, ankiety wypełnili przedstawiciele firm prywatnych zrzeszonych w Radzie Polskich Przedsiębiorców przy Pracodawcach RP oraz pracownicy firm członkowskich tej organizacji. Celem badania było zebranie opinii na temat gotowości sektora prywatnego do aktywnego udziału w systemie obrony cywilnej, w tym ocena postaw wobec szkoleń obronnych oraz identyfikacja barier i warunków wpływających na zaangażowanie firm i pracowników.

Kwestionariusze obu ankiet miały zbliżoną konstrukcję merytoryczną, pytania pogrupowano tematycznie w pięć bloków obejmujących kolejno: (1) dotychczasowy udział w szkoleniach z zakresu obronności (np. pierwsza pomoc, samoobrona, posługiwanie się bronią), (2) postawy wobec udziału w systemie bezpieczeństwa i ocena roli przeszkolonych pracowników, (3) obawy i potencjalne ryzyka (m.in. w kontekście mobilizacji), (4) motywatory i preferowane formy wsparcia uczestnictwa (np. ulgi, dofinansowania, przywileje) oraz (5) metryczkę respondentów (np. wielkość przedsiębiorstwa, stanowisko pracy). Pytania sformułowano w sposób neutralny, dając możliwość udzielania wielokrotnych odpowiedzi tam, gdzie było to zasadne, oraz uwzględniając opcję „nie mam zdania” przy pytaniach dotyczących opinii, aby uchwycić ewentualne wahania respondentów.

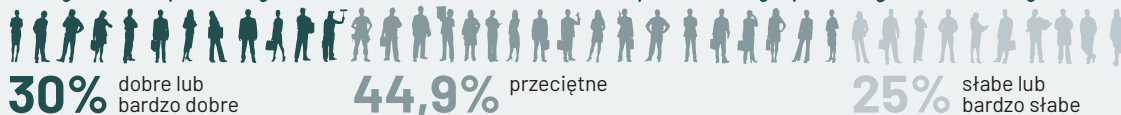
W badaniu pracodawców udział wzięli reprezentanci firm zróżnicowanych pod względem wielkości i branży. Najliczniej reprezentowane były średnie przedsiębiorstwa (51–300 pracowników – 29% próby) oraz mikro- i małe firmy (zatrudniające do 50 osób – łącznie ok. 33%). Pozostałe ~38% stanowili przedstawiciele dużych organizacji, w tym 13% – firm bardzo dużych (powyżej 1500 pracowników). Ankietowani pracodawcy reprezentowali m.in. sektor przemysłowy i produkcyjny (30%), usługi finansowe/ubezpieczeniowe (15,8%), handel detaliczny i hurtowy (15%), branżę IT/ICT (10,8%), ochronę zdrowia (4,2%), a 24,2% wskazało inne branże. Z kolei wśród 841 ankietowanych pracowników dominowali specjaliści (58,8%) oraz kadra menedżerska (30%); pozostałe 11% stanowili młodszy specjaliści/asystenci i pracownicy fizyczni. Taki dobór próby pozwolił uchwycić perspektywę zarówno decydentów firm, jak i szerokiego grona zatrudnionych, zainteresowanych tematyką obronności.

GOTOWOŚĆ DO BUDOWANIA ODPORNOŚCI PAŃSTWA

PRACOWNICY I PRACODAWCY

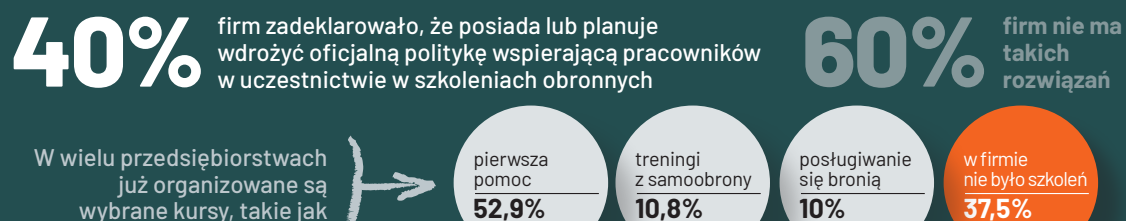


Swoje kompetencje w zakresie udzielania pierwszej pomocy oceniam jako:



Wśród **pracowników** istnieje **wysoki popyt na rozwój kompetencji obronnych**, który pracodawcy mogą wykorzystać, wpisując się jednocześnie w system podnoszenia odporności kraju.

Po stronie **pracodawców** widać rosnącą świadomość znaczenia takich szkoleń, choć formalna polityka ich wspierania nie jest jeszcze powszechna.



Istnieje więc przestrzeń do zwiększenia zaangażowania firm w podnoszenie kompetencji obronnych załóg.



Wyniki sugerują **potrzebę edukacji i komunikacji**, aby zarówno pracownicy, jak i kadra lepiej rozumieli ramy prawne przygotowań obronnych.

Warto zauważyć, że sami pracodawcy mają dość optymistyczne oczekiwania co do frekwencji, np. aż 41,7% badanych ocenia, że zainteresowanie udziałem w takich szkoleniach w ich firmie byłoby duże, kolejne 33,3% nie ma już takiej pewności (zakłada możliwość umiarkowanego zainteresowania); tylko 25% respondentów spodziewałoby się niskiej frekwencji ze strony załogi. Te przewidywania korespondują z deklaracjami pracowników. Realnie chętnych do udziału jest ponad trzy razy więcej niż sceptycznych. **Można zatem stwierdzić, że klimat dla szkoleń obronnych w miejscu pracy jest bardzo sprzyjający zarówno po stronie pracowników, jak i pracodawców.**

POSTAWY WOBEC OBRONNOŚCI W MIEJSCU PRACY

Tak pracownicy, jak i pracodawcy wyrażają silne poparcie dla zaangażowania sektora prywatnego w działania na rzecz bezpieczeństwa. Obie grupy są zgodne co do tego, że podnoszenie umiejętności obronnych przekłada się na realne korzyści. Aż 79,2% pracodawców uważa, że umiejętność posługiwania się bronią palną przez przeszkolonych pracowników może przyczynić się do zwiększenia bezpieczeństwa, tylko co piąty jest odmiennego zdania. Po stronie pracowników odsetek osób podzielających tę opinię jest również bardzo wysoki (71,9% zgadza się, że przeszkolony w zakresie broni pracownik wzmacnia obronność państwa), przy czym 15,6% badanych nie ma zdania, a jedynie 12,5% tę tezę neguje. Widać zatem, że przeważająca większość respondentów dostrzega pozytywną rolę wyszkolonych obywateli (zarówno w firmach, jak i ogółem) dla zwiększenia bezpieczeństwa i odporności kraju.

Jednocześnie ujawnia się istotna luka informacyjna w obszarze znajomości aktualnych regulacji prawnych dotyczących obronności wśród pracowników. Trzy czwarte z nich (75%) przyznaje, że nie zna obecnych przepisów dotyczących posiadania broni i samoobrony – tylko 25% deklaruje zaznajomienie z tymi regulacjami. Świadomość prawna w tym zakresie po stronie pracodawców jest nieco wyższa, ale nadal daleka od pełnej – 40% pracodawców zna obowiązujące przepisy dotyczące broni i obrony cywilnej, natomiast 60% nie ma takiej wiedzy. Braki informacyjne mogą przekładać się na niepewność co do ról i obowiązków firm oraz obywateli w systemie obronnym państwa. Wyniki sugerują potrzebę edukacji i komunikacji, np. kampanii informacyjnych lub szkoleń uświadamiających, aby zarówno pracownicy, jak i kadra zarządzająca lepiej rozumieli ramy prawne przygotowań obronnych.

OBAWY ZWIĄZANE Z MOBILIZACJĄ

Mimo ogólnego poparcia dla inicjatyw obronnych w obu grupach wyraźnie rysuje się obawa przed konsekwencjami ewentualnej mobilizacji. Dotyczy ona zwłaszcza możliwości powołania przeszkolonych osób do czynnej służby wojskowej w razie kryzysu lub konfliktu, co potencjalnie oznacza ubytek kadry dla pracodawcy lub osobiste ryzyko dla pracownika. Prawie połowa ankietowanych pracowników (49,6%) obawia się, że jeśli zdobędą umiejętności z zakresu użycia broni, pierwszej pomocy czy samoobrony, to właśnie oni mogą być pierwsi w kolejności do powołania do Sił Zbrojnych RP w razie mobilizacji. Tylko 28,1% pracowników deklaruje brak takich obaw, a 22,4% nie zastanawiało się dotąd nad tym zagadnieniem. Innymi słowy, co drugi pracownik wiąże swój udział w szkoleniach obronnych z ryzykiem szybszego wcielenia do wojska.

Po stronie pracodawców analogiczny niepokój również występuje: 44,2% firm obawia się, że przeszkoleni pracownicy mogą zostać powołani do armii w przypadku mobilizacji, co oznaczałoby uszczuplenie zasobów kadrowych przedsiębiorstwa. Niespełna jedna czwarta pracodawców (23,3%) nie ma takich obaw,

OBAWY ZWIĄZANE ZE SZKOLENIEM I POWOŁANIEM

PRACOWNICY 49,6%

obawia się, że jeśli zdobędą umiejętności z zakresu użycia broni, pierwszej pomocy czy samoobrony, w razie mobilizacji **mogą być powołani do wojska jako pierwsi**

28,1%

nie ma takich obaw

22,4%

nie zastanawiało się nad tym

44,2% PRACODAWCY

obawia się, że przeszkoleni pracownicy mogą zostać powołani do armii w przypadku mobilizacji, co oznaczałoby **uszczerpienie zasobów kadrowych** przedsiębiorstwa

23,3%

nie ma takich obaw

32,5%

nie potrafi ocenić tego ryzyka

CO DRUGI PRACOWNIK WIAŻE UDZIAŁ W SZKOLENIACH Z RYZYKIEM WCIĘCIA DO WOJSKA

Zagrożenie **odpływem przeszkolonych pracowników do służby wojskowej** jest jednym z **kluczowych czynników hamujących entuzjazm** dla powszechnych szkoleń.



INSTYTUT
SOBIESKIEGO



Instytut
Wschodniej Flanki



OLDMAN
SAGE



RADA POLSKICH
PRZEDSIĘBIORCÓW

INFOGRAFIKA: PIOTR PERZYNA

natomiast 32,5% nie potrafi jednoznacznie ocenić tego ryzyka. Wyniki te wskazują, że zagrożenie odpływem przeszkolonych pracowników do służby wojskowej jest jednym z kluczowych czynników hamujących entuzjazm dla powszechnych szkoleń. Jest to ważne zarówno z perspektywy firm, jak i samych pracowników. Tak jedni, jak i drudzy dostrzegają potrzebę wzmocnienia obronności, lecz obawiają się, że aktywne przygotowanie może skutkować osobistymi lub biznesowymi stratami w razie wojny.

GOTOWOŚĆ DO TWORZENIA GRUP SAMOOBRONY

Istotnym elementem badania było ustalenie, w jakim stopniu obie grupy popierają koncepcję organizowania cywilnych struktur samoobrony we współpracy z instytucjami państwowymi. Chodzi tu o formalne grupy obywateli (w tym pracowników firm), szkolone pod nadzorem służb państwowych, zwłaszcza policji, z zadaniem obrony lokalnych społeczności w sytuacjach zagrożenia (np. ataku terrorystycznego lub agresji hybrydowej). Idea ta spotkała się z bardzo dużym zrozumieniem, szczególnie wśród pracowników. Blisko 80% z nich uważa, że lokalne społeczności powinny mieć możliwość organizowania formalnych cywilnych grup samoobrony pod nadzorem państwa, a tylko 20,7% jest temu przeciwnych. Można zatem mówić o wyraźnej aprobacie społecznej dla włączenia obywateli we współtworzenie oddolnych struktur bezpieczeństwa w swoim otoczeniu.

W przypadku pracodawców również przeważa przekonanie, że firmy mogłyby odegrać ważną rolę w tworzeniu takich formacji. Około dwóch trzecich badanych przedsiębiorców (65–66%) deklaruje zainteresowanie lub gotowość współpracy z lokalnymi władzami i policją przy tworzeniu grup samoobrony na swoim terenie. Pozostała jedna trzecia (ok. 34%) nie widzi siebie w takiej roli lub ma wątpliwości co do angażowania się

firmy w tego typu inicjatywę. Mimo wszystko przewaga głosów za współpracą jest wyraźna, co sygnalizuje otwartość sektora prywatnego na partnerstwo z administracją w obszarze bezpieczeństwa lokalnego.

Deklaracje poparcia idei samoobrony terytorialnej nie zawsze przekładają się jednak na osobistą gotowość do udziału w takich grupach. Gdy zapytano pracowników, czy byliby osobiście zainteresowani dołączeniem do zorganizowanej lokalnej grupy samoobrony (współpracującej z policją i władzami, pod nadzorem państwa), twierdząco odpowiedziało 40% badanych. Pozostali nie byliby skłonni wstąpić do takiej formacji (26,3% odpowiedzi „nie”) bądź też wahają się i nie mają zdania na ten temat (33,8%). Warto zauważyć, że odsetek chętnych (40%) jest istotnie niższy niż odsetek popierających samą ideę tworzenia grup (79%). Można to interpretować w ten sposób, że wielu osobom koncept „obywatelskiej obrony” odpowiada co do zasady, jednak włączenie się osobiście wymagałoby dodatkowych zachęt lub sprzyjających okoliczności.

Analogicznie, po stronie pracodawców można zakładać, że sama deklaracja gotowości współpracy z władzami nie oznacza automatycznego tworzenia firmowych oddziałów samoobrony, potrzebne są jasne ramy prawne i organizacyjne. Ogólny wniosek jest taki, że społeczny mandat dla tworzenia struktur samoobrony jest silny, ale ich powodzenie zależeć będzie od czynników praktycznych i bodźców skłaniających do aktywnego udziału.

CO ZWIĘKSZA ZAANGAŻOWANIE

Aby lepiej zrozumieć, co mogłoby skłonić do aktywnego włączenia się w inicjatywy obrony cywilnej, respondentom przedstawiono listę potencjalnych udogodnień, przywilejów i form wsparcia z prośbą o zaznaczenie tych, które zwiększyłyby ich skłonność (pracownicy) lub gotowość do wsparcia pracowników (pracodawcy) w dołączaniu do lokalnych grup samoobrony. Wyniki obu ankiet są tu spójne i bardzo wymowne. Zarówno dla pracowników, jak i dla pracodawców najsilniejszym motywatorem okazało się zagwarantowanie osobom zaangażowanym w obronę cywilną ochrony przed przymusowym wcieleniem do wojska w razie mobilizacji.

- Istotną rolę odgrywa ewentualne wsparcie finansowe. Zwrot kosztów poniesionych na szkolenia lub zakup wyposażenia obronnego zachęciłby 47,7% pracowników i 37,5% pracodawców, a dofinansowanie (np. częściowe pokrycie kosztów przez państwo) byłoby bodźcem dla 31,6% pracowników i 40,8% pracodawców. Innymi słowy, dzielenie kosztów z państwem, czy to *ex post*, w formie refundacji, czy *ex ante*, w formie subsydiów, znacząco zwiększa akceptację udziału w szkoleniach i grupach obrony cywilnej.
- Wśród pracowników niemal połowa (48,8%) wskazała, że skłoniłby ich do udziału przywilej w postaci **braku powołania do Sił Zbrojnych RP w razie mobilizacji** pod warunkiem służby jako cywil w lokalnej grupie samoobrony. Podobny warunek jako kluczowy czynnik motywujący wymieniło 57,5% pracodawców, którzy byliby skłonni wspierać pracowników wstępujących do takich grup, gdyby ci pracownicy uzyskali gwarancję niekierowania na front w sytuacji kryzysowej (pozostaliby na miejscu jako obrońcy cywilni).
- Trzecim istotnym czynnikiem jest stabilność zatrudnienia i ochrona praw pracowniczych osób zaangażowanych w obronność. W tym wypadku 39,8% pracowników przyznało, że motywowałby ich przywilej ochrony stosunku pracy (analogiczny do tego, jaki przysługuje żołnierzom Wojsk Obrony Terytorialnej) w okresie uczestnictwa w szkoleniach lub działaniach obronnych. Taki postulat jest zrozumiały. Pracownicy pragną mieć pewność, że udział w dodatkowych aktywnościach proobronnych

CO ZWIĘKSZA ZAANGAŻOWANIE?

PRACOWNICY

47,7% | 37,5%

dzielenie kosztów z państwem, czy to *ex post* w formie refundacji, czy *ex ante* w formie subsydiów, znacząco zwiększa akceptację udziału w szkoleniach i grupach obrony cywilnej

48,8% | 57,5%

przywilej **braku powołania do Sił Zbrojnych RP w razie mobilizacji**, pod warunkiem służby jako cywil w lokalnej grupie samoobrony

38,8%

PRACODAWCY AKCEPTOWALIBY NIEOBECNOŚĆ PRACOWNIKA JEŚLI WIĄZAŁABY SIĘ Z KORZYŚCIAMI LUB OBOWIĄZKIEM

stabilność zatrudnienia i ochrona praw pracowniczych dla osób zaangażowanych w obronność, czyli przywilej ochrony stosunku pracy (taki, jaki przysługuje żołnierzom WOT) w czasie szkoleń lub działań obronnych

19,0% | 4,2%

„**nic**” ich nie skłoni do udziału w grupach samoobrony (co zapewne pokrywa się z grupą 26% deklarujących wcześniej brak zainteresowania przynależnością).
brak zainteresowania przynależnością).

PRACODAWCY

PRACOWNICY
I PRACODAWCY
OCZEKUJĄ,
ŻE PAŃSTWO
WEZMIE NA SIEBIE
CZĘŚĆ
OBCIĄŻEN



INSTYTUT
SOBIESKIEGO



Instytut
Wschodniej Flanki



OLDMAN
SAGE



RADA POLSKICH
PRZEDSIĘBIORCÓW

INFOGRAFIKA: PIOTR PERZYNA



nie narazi ich na utratę etatu. Po stronie pracodawców kwestia ta wydaje się mniej paląca (nie była bezpośrednio mierzona w ankiecie do nich skierowanej), natomiast można zakładać, że przełożeni akceptowaliby nieobecność pracownika związaną ze szkoleniem, jeśli wiązałaby się z wymiernymi korzyściami (wspomnianymi wyżej) lub obowiązkiem prawnym.

- Część respondentów uzależnia swój udział od powagi sytuacji – tylko w przypadku realnego zagrożenia wojną byłiby skłonni zaangażować się w obronę. Taką odpowiedź (opcja „tylko w razie konfliktu zbrojnego”) zaznaczyło 27,6% pracowników i 29,2% pracodawców. Grupa ta niejako odkłada aktywność na czas *ad extrema*, obecnie woli nie podejmować dodatkowych zobowiązań, ale deklaruje gotowość obrony kraju, gdyby zaszła bezpośrednia konieczność.
- Zauważalny jest także segment osób niezainteresowanych dodatkowymi bodźcami – 19% pracowników stwierdziło, że „**nic**” ich nie skłoni do udziału w grupach samoobrony (co zapewne pokrywa się z grupą 26% deklarujących wcześniej brak zainteresowania przynależnością). Po stronie pracodawców odsetek firm, których „**nic** by nie przekonało” do wspierania takich inicjatyw, jest marginalny (4,2%), zdecydowana większość przynajmniej rozważyłaby udział, o ile spełnione byłyby powyższe warunki.

Podsumowując, zarówno pracownicy, jak i pracodawcy oczekują, że państwo weźmie na siebie część ciężaru, czy to przez zwolnienie kluczowych osób z obowiązku służby wojskowej na rzecz obrony cywilnej, czy przez dofinansowanie szkoleń i sprzętu. Taki układ bodźców postrzegany jest jako warunek sprawiedliwego podziału odpowiedzialności za bezpieczeństwo kraju, co zresztą znajduje odzwierciedlenie w postulatach, by koszty podnoszenia odporności były dzielone między sektor publiczny i prywatny.

WNIOSKI I REKOMENDACJE

Wyniki obu ankiet pozwalają sformułować szereg wniosków dotyczących roli sektora prywatnego w systemie bezpieczeństwa oraz rekomendacji działań, które mogą tę rolę wzmocnić.

- Po pierwsze, w polskim społeczeństwie, zarówno wśród przedsiębiorców, jak i pracowników, istnieje **silne poparcie dla inicjatyw mających na celu włączenie firm i obywateli w przedsięwzięcia z zakresu obrony cywilnej**. Wysoki odsetek pracowników chętnych do udziału w szkoleniach obronnych organizowanych przez pracodawców (83,5%) oraz znaczny odsetek firm dostrzegających wartość posiadania przeszkolonych załóg wskazują, że kapitał ludzki i gotowość społeczna są atutami, które warto wykorzystać. Kluczem jest przekucie tej deklarowanej gotowości w realne programy i działania.
- Po drugie, zidentyfikowane zostały konkretne bariery i obawy, które należy adresować, aby zaangażowanie sektora prywatnego mogło się urzeczywistnić. Najpoważniejszą z nich jest obawa przed mobilizacją wojskową – **zarówno pracownicy, jak i pracodawcy uważają, że uczestnictwo w szkoleniach czy grupach obrony cywilnej może spowodować automatycznie utratę tych pracowników w pierwszej kolejności na rzecz armii**. Rekomenduje się zatem rozważenie rozwiązań prawnych, które formalnie uregulują status członków cywilnych struktur obronnych, na przykład poprzez branie pod uwagę ich zaangażowania w firmach przy powoływaniu do służby wojskowej w razie kryzysu (przy jednoczesnym zobowiązaniu do obrony lokalnej). Takie rozwiązanie, choć oczywiście w tym zakresie „ostatnie słowo” zawsze będzie mieć państwo, mogłoby zwiększać poczucie bezpieczeństwa współpracy obu stron i prawdopodobnie przełożyłoby się na większą skłonność do tworzenia i wstępowania do grup samoobrony.
- Po trzecie, **istotnym czynnikiem warunkującym sukces tych inicjatyw jest kwestia finansowania i bodźców ekonomicznych**. Z perspektywy firm ważne jest, by koszty podnoszenia bezpieczeństwa były współdzielone z państwem, a nie w całości przerzucone na pracodawców. Dlatego zaleca się wdrożenie mechanizmów zachęt finansowych dla przedsiębiorstw inwestujących w szkolenia obronne pracowników. Mogłyby one obejmować np. lepsze wykorzystanie już istniejącego funduszu szkoleń czy preferencje przy przetargach publicznych dla tych firm, które angażują się samodzielnie w budowę systemu odporności państwa. Dla pracowników natomiast warto przewidzieć system dofinansowań lub refundacji kosztów kursów, tak aby kwestie finansowe nie powstrzymywały chętnych przed podnoszeniem kwalifikacji. Jednocześnie, uznając szkolenia obronne za działanie *pro publico bono*, można rozważyć częściowe ich finansowanie ze środków publicznych (np. poprzez programy dofinansowania szkoleń z zakresu ochrony ludności).

- Po czwarte, **edukacja i informacja powinny stać się integralnym elementem działań na rzecz zwiększenia odporności**. Badanie wykazało poważne luki w świadomości prawnej (75% pracowników nie zna przepisów dotyczących obrony cywilnej i dostępu do broni) oraz umiarkowaną ocenę własnych umiejętności w sytuacjach kryzysowych. Rekomenduje się zatem przygotowanie kampanii informacyjnych oraz programów szkoleniowych dostępnych w miejscu pracy, które podniosą wiedzę na temat praw i obowiązków obywateli oraz firm w kontekście obronności. Pracodawcy – szczególnie więksi – przy wsparciu odpowiednich służb mogliby organizować regularne warsztaty z pierwszej pomocy, szkolenia strzeleckie czy kursy samoobrony, które nie tylko zwiększyłyby kompetencje personelu, ale i świadomość zagrożeń. Warto również upowszechniać informacje o istniejących rozwiązaniach i procedurach (np. o zasadach funkcjonowania obrony cywilnej, roli Wojsk Obrony Terytorialnej, możliwości uzyskania pozwoleń na broń itp.), aby obywatele lepiej rozumieli kontekst swoich działań.
- Po piąte, **należy wykorzystać istniejące pozytywne nastawienie do budowania platform współpracy między sektorem prywatnym a publicznym w dziedzinie bezpieczeństwa**. Skoro większość firm deklaruje gotowość współdziałania z władzami przy tworzeniu lokalnych struktur samoobrony, władze samorządowe i państwowe powinny wyjść naprzeciw tym deklaracjom. Można rekomendować stworzenie formalnych ram współpracy, np. poprzez umożliwienie firmom zgłaszania chęci utworzenia przykładowych zespołów reagowania kryzysowego czy oddziałów obrony cywilnej, które byłyby szkolone i certyfikowane we współpracy z odpowiednimi służbami (Policją, Państwową Strażą Pożarną, Wojskami Obrony Terytorialnej). Takie grupy – złożone z pracowników wolontariuszy – mogłyby pełnić podwójną funkcję: z jednej strony zwiększać bezpieczeństwo zakładów pracy i lokalnych społeczności na co dzień, z drugiej stanowić rezerwę kadrową na wypadek poważnego kryzysu. Warunkiem jest jednak nadanie im oficjalnego statusu i zapewnienie wspomnianych wyżej gwarancji (prawnych, finansowych, pracowniczych), tak aby udział w nich był zarówno bezpieczny, jak i atrakcyjny.

Podsumowując, **ankiety ujawniły duży potencjał do zaangażowania sektora prywatnego w system bezpieczeństwa kraju przy jednoczesnym wskazaniu jasno określonych warunków brzegowych takiego udziału**. Polscy przedsiębiorcy i pracownicy wykazują gotowość do współuczestnictwa w budowaniu odporności państwa – chcą się szkolić, wspierać lokalne inicjatywy obronne i współpracować z administracją. Aby ten społeczny kapitał przekuć w realne działania, należy stworzyć odpowiednie mechanizmy zachęt i ochrony, tak by udział w systemie obrony cywilnej był postrzegany nie jako ryzyko, lecz jako wspólne przedsięwzięcie mające przynieść obopólne korzyści. Implementacja powyższych rekomendacji – opartych wyłącznie na danych z badań ankietowych – przyczyni się do wzrostu bezpieczeństwa państwa poprzez pełniejsze wykorzystanie potencjału firm i obywateli bez odwoływania się do rozwiązań zewnętrznych, a jedynie bazując na deklaracjach, obawach i motywacjach zgłoszonych przez samych zainteresowanych.

2. WYZWANIA ZWIĄZANE Z RYNKIEM PRACY

Bartosz Marczuk



Zanim przedstawimy szczegółowo koncepcję współpracy pracodawców z państwem w zakresie budowania odporności, zaprezentujemy pejzaż polskiego rynku pracy. Bo to tego segmentu będzie dotyczyć idea budowania synergii między firmami a administracją na wypadek kryzysów czy zagrożeń. Pokażemy w tym rozdziale, ilu Polaków pracuje, w jaki sposób, na jakich kontraktach wykonują swoje obowiązki i w jakich firmach są zatrudnieni.

ILU POLAKÓW PRACUJE

Najlepszym źródłem informacji o tym, co dzieje się na polskim rynku pracy, jest prowadzone już od ponad 30 lat przez GUS Badanie Aktywności Ekonomicznej Ludności (BAEL). Jego zaletą jest to, że jest badaniem ankietowym, realizowanym systematycznie, raz na kwartał. Zgodnie z metodologią Międzynarodowej Organizacji Pracy (ILO) BAEL obejmuje ono reprezentatywną próbę gospodarstw domowych i osób w wieku 15 lat i więcej. Dostarcza m.in. danych o liczbie pracujących, bezrobotnych, biernych zawodowo, a także o współczynniku aktywności zawodowej i wskaźniku zatrudnienia.

Na początek sprawdźmy, co pokazują dane BAEL, jeśli chodzi o liczbę osób pracujących w Polsce (dane te obejmują też pracujących w kraju cudzoziemców, choć można przyjąć, że są one w sporej mierze niedoszacowane). Obecnie (zob. Wykres 1) obserwujemy rekordowe poziomy zatrudnienia. Dotychczasowy szczyt przypadł na I kwartał 2023 r., gdy w naszej gospodarce pracowało ponad 17,3 mln osób. Obecnie ta liczba oscyluje wokół 17,2 mln (zaczyna tu działać demografia), ale warto pamiętać, że jeszcze w 2013 r. ledwo przekraczała 15 mln.

W efekcie wzrostu liczby pracujących znacząco poprawiły się podstawowe wskaźniki naszego rynku pracy. Na przykład stopa bezrobocia (liczona według metodologii BAEL, a więc inaczej niż w statystykach rządowych, które obejmują wyłącznie osoby zarejestrowane w urzędach pracy) spadła (zob. Wykres 2) w ciągu ostatnich 15 lat z 10% (II kwartał 2010 r.) do zaledwie 2,8% (II kwartał 2025). Liczba osób pozostających bez pracy, ale aktywnie jej poszukujących (taka jest definicja bezrobotnego w BAEL) zmalała w tym czasie ponad trzykrotnie – z blisko 1,7 mln do zaledwie 503 tys.

Podobnie jest ze wskaźnikiem zatrudnienia (odpowiada na pytanie, ile osób w wieku 15–89 lat pracuje), który wzrósł w tym czasie z 48% do blisko 57%.

Po drugiej stronie równania są tzw. osoby bierne zawodowo, tj. takie, które nie pracują, pracy nie szukają i nie są zainteresowane jej podjęciem (dzieje się tak z różnych przyczyn, np. ze względu na naukę, zniechęcenie poszukiwaniem zatrudnienia, chorobę, niepełnosprawność, emeryturę czy obowiązki rodzinne związane z prowadzeniem domu). Takich osób w 2010 r. było ponad 14,3 mln, obecnie ich liczba zmalała do 12,66 mln.

Na rynku pracy zaszła zatem, zwłaszcza w ostatniej dekadzie, zasadnicza, pozytywna zmiana. To ważne z perspektywy budowy systemu odporności państwa wspólnie z pracodawcami, bo oznacza, że zdecydowana większość Polaków w wieku do 60/65 lat jest obecna na rynku pracy.

NA JAKICH KONTRAKTACH

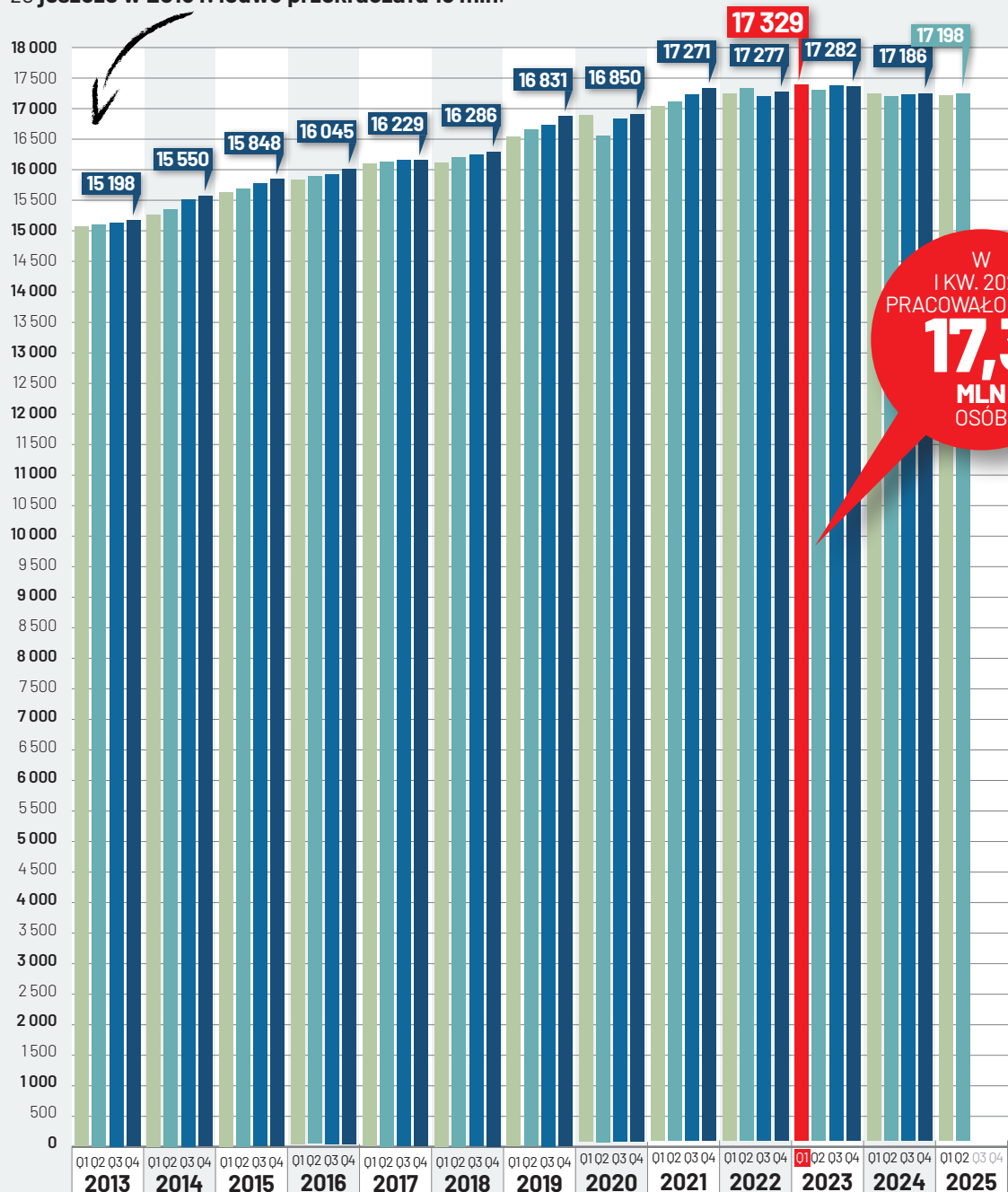
Przyjrzyjmy się teraz formom zatrudnienia i sektorom, w których są aktywne osoby pracujące w Polsce. Największą grupę ze wspomnianej liczby 17,2 mln stanowią tzw. osoby zatrudnione (czyli pracujące „dla kogoś”, zwykle na etacie). Jest ich ponad 13,9 mln, czyli blisko 81% wszystkich pracujących w kraju. To bardzo istotna informacja z perspektywy naszego raportu, bo to właśnie te osoby mogą być w łatwy sposób włączone do systemu odporności państwa ze względu na to, że mają jakiegoś pracodawcę. Spośród nich blisko 11,7 mln pracuje na stałych kontraktach (prawie 85%), reszta na czasowych – mogą to być zarówno czasowe etaty, jak i inne, cywilnoprawne kontrakty, choć zdecydowana większość to czasowe zatrudnienie etatowe.

Pozostała część pracujących w kraju osób to pracodawcy i osoby pracujące na własny rachunek (3,15 mln) oraz pomagający bezpłatnie członkowie rodzin (0,1 mln). W przeważającej większości są to osoby prowadzące działalność gospodarczą – blisko 2 mln w ramach działalności pozarolniczej (ZUS) oraz nieco ponad 1 mln (wraz z członkami rodzin) w ramach działalności rolnej (KRUS). Te osoby, co ważne z perspektywy budowy proponowanego przez nas systemu odporności, nie mają pracodawcy. Warto zastanowić się jednak, jak można je włączyć do tego systemu.

WYKRES 1.

LICZBA PRACUJĄCYCH POLAKÓW [TYS.]

Dotychczasowy **rekord padł dokładnie w I kwartale 2023 r.**, gdy w naszej gospodarce pracowało ponad 17,3 mln osób. Obecnie ta liczba oscyluje wokół 17,2 mln (zaczyna tu działać demografia), ale warto pamiętać, że **jeszcze w 2013 r. ledwo przekraczała 15 mln.**



W
I KW. 2023
PRACOWAŁO PONAD
17,3
MLN
OSÓB

Źródło danych: GUS, Podstawowe dane z Badania Aktywności Ekonomicznej Ludności wyrównane sezonowo w latach 2010-2025, <https://stat.gov.pl/obszary-tematyczne/rynek-pracy/pracujacy-bezrobotni-bierni-zawodowo-wg-bael/podstawowe-dane-z-badania-aktywnosci-ekonomicznej-ludnosci-wyrównane-sezonowo-w-latach-2010-2025,16,6.html>.

W JAKICH BRANŻACH

Przyjrzyjmy się jeszcze temu, kim są i gdzie wykonują swoje obowiązki aktywni pracujący. Spośród 17,2 mln takich osób prawie 9,3 mln stanowią mężczyźni, resztę (prawie 8 mln) kobiety. W miastach pracuje blisko 10,5 mln osób, reszta na wsi. Najliczniejszą grupę wiekową (blisko 7 mln pracujących) tworzą osoby w wieku 45–64 lat, drugą co do wielkości grupą (5 mln) – są pracujący w wieku 35–44 lata. Najmniej liczne grupy stanowią osoby najmłodsze i najstarsze w wieku odpowiednio 15–24 lata oraz 60–89 lat. Jest ich odpowiednio niespełna 1 mln i 0,8 mln.

Polacy w większości (75%) pracują w sektorze prywatnym. Takich osób jest blisko 13 mln. Pośród pracujących dominują osoby z wyższym wykształceniem. Jest ich blisko 7,5 mln. Kolejna duża grupa to osoby mające wykształcenie policealne i średnie zawodowe (4 mln). A zatem 2/3 pracujących w kraju to osoby dobrze lub nieźle wykształcone. Jest to także ważna informacja z perspektywy koncepcji współpracy w budowaniu odporności państwa z pracodawcami i pracownikami.

Najwięcej osób pracuje w sektorze usługowym (10,8 mln), duży jest także, ponad 30-procentowy, udział przemysłu, który zatrudnia 5,2 mln osób. Najmniejszą grupę stanowią osoby pracujące w rolnictwie (1,05 mln). Szczególnie istotna z perspektywy naszego raportu jest informacja o dużym udziale sektora przemysłowego w zatrudnieniu. Można przyjąć, że w wielu zakładach przemysłowych istnieją już jakieś komórki odpowiedzialne za bezpieczeństwo, a praca w tym sektorze jest zwykle lepiej regulowana i opisana procedurami. Będzie to miało duże znaczenie przy wdrażaniu nowego systemu odporności.

Jeśli dokładniej przeanalizujemy branże (zob. Tabela 1), w których pracują osoby zatrudnione w kraju (wg sekcji PKD), to znowu okaże się, że najwięcej jest pracowników przetwórstwa przemysłowego (blisko 20%). Druga duża grupa to pracownicy handlu i napraw pojazdów (12,6%), a kolejną stanowią osoby pracujące w edukacji i budownictwie. Mamy też ponad 1 mln osób zatrudnionych w sekcji administracja publiczna/ obrona narodowa/obowiązkowe zabezpieczenia społeczne, gdzie gros z nich jest naturalnymi kandydatami do odegrania kluczowych ról przy budowie modelu odporności państwa we współpracy z firmami.

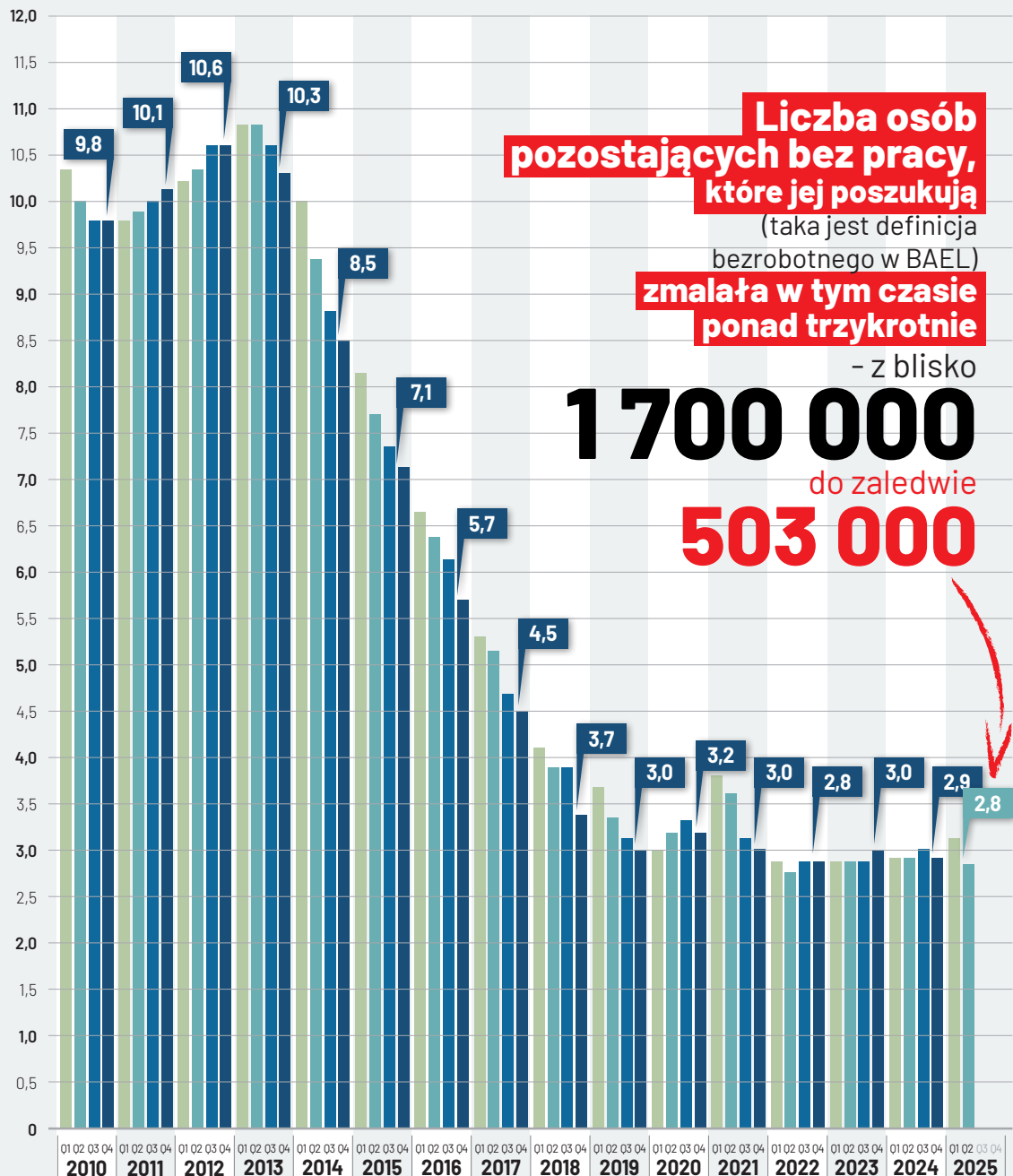
WYKRES 2.

WSKAŹNIK BEZROBOCIA (2010-2025) [%]

Na rynku pracy, zwłaszcza w ostatniej dekadzie, zaszła bardzo zasadnicza, pozytywna zmiana.

Bezrobocie* zmalało w ciągu ostatnich 15 lat z 10% (II kw. 2010 r.) do zaledwie 2,8% (II kw. 2025).

* liczone według metodologii BAEL, a więc inaczej niż w statystykach rządowych, które obejmują wyłącznie osoby zarejestrowane w urzędach pracy



Źródło danych: GUS.

TABELA 1. **W JAKICH BRANŻACH PRACUJĄ OSOBY ZATRUDNIONE W POLSCE**

WEDŁUG WYBRANYCH SEKCJI PKD	LICZBA PRACOWNIKÓW (W TYS.)	UDZIAŁ W LICZBIE PRACUJĄCYCH (W PRÓC)
Przetwórstwo przemysłowe	3326	19,3
Handel hurtowy i detaliczny; naprawa pojazdów samochodowych, włączając motocykle	2162	12,6
Edukacja	1387	8,1
Budownictwo	1323	7,7
Administracja publiczna i obrona narodowa; obowiązkowe zabezpieczenia społeczne	1227	7,1
Opieka zdrowotna i pomoc społeczna	1175	6,8
Transport i gospodarka magazynowa	1151	6,7
Rolnictwo, leśnictwo, łowiectwo i rybactwo (w tym indywidualne gospodarstwa rolne)	1057	6,1
Działalność profesjonalna, naukowa i techniczna	870	5,1
Informacja i komunikacja	673	3,9
Działalność finansowa i ubezpieczeniowa	487	2,8
Działalność w zakresie usług administrowania i działalność wspierająca	450	2,6
Działalność związana z zakwaterowaniem i usługami gastronomicznymi	421	2,4
Pozostała działalność usługowa	345	2
Działalność związana z kulturą, rozrywką i rekreacją	228	1,3
Górnictwo i wydobywanie	192	1,1
Dostawa wody; gospodarowanie ściekami i odpadami oraz działalność związana z rekultywacją	185	1,1
Wytwarzanie i zaopatrywanie w energię elektryczną, gaz, parę wodną, gorącą wodę i powietrze do układów klimatyzacyjnych	180	1
Działalność związana z obsługą rynku nieruchomości	165	1

Źródło: Opracowanie własne Autora na podstawie danych GUS.

ROZDROBNIENIE FIRM

Istotnym wyzwaniem przy wdrażaniu proponowanego modelu może okazać się rozdrobnienie rynku pracy, wynikające ze struktury wielkości firm zatrudniających pracowników w Polsce. Oczywiście łatwiej jest, gdy system jest wdrażany w większych firmach – działa wtedy efekt skali, duże przedsiębiorstwa mają wewnętrzne działy kadr i bezpieczeństwa, zwykle mają też określone procedury szkoleń, łatwiej też im zarządzić nieobecnością w firmie części pracowników. W kraju mamy jednak stosunkowo niewiele takich dużych, zatrudniających setki i tysiące osób, firm.

Według najnowszego raportu PARP – *Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce (2025)* – oraz publikacji GUS *Działalność przedsiębiorstw niefinansowych w 2023 r.*, którą posiłkuje się PARP przy swoich obliczeniach, w 2023 r. aktywnie działało w kraju blisko 2,31 mln tzw. przedsiębiorstw niefinansowych. Zatrudniały one 10,3 mln osób. Pojawia się więc pytanie, dlaczego dane te nie obejmują całości populacji zatrudnionych. Dzieje się tak dlatego, że definicja przedsiębiorstw niefinansowych jest specyficzna dla tych badań (nie obejmuje np. szkół wyższych czy SP ZOZ). Mimo tego ograniczenia dane te dobrze oddają strukturę zatrudnienia w Polsce i można je ekstrapolować na całą populację firm i pracowników w kraju.

W Polsce sektor MSP (mikro-, małych i średnich przedsiębiorstw) stanowi przytłaczającą większość działających firm, mowa tu o 99,8% (zob. Wykres 3). Najliczniejszą grupą (97,1%, 2,2 mln firm) są mikroprzedsiębiorstwa, następnie małe firmy 2,1% (48,7 tys.), średnie – 0,6% (14,4 tys.), dużych jest zaledwie 0,2% (3,8 tys.).

W 2023 r. w podmiotach zaliczanych, zgodnie z definicją przyjętą w cytowanych opracowaniach, do sektora MSP (zatrudniających do 249 osób) pracowało ponad 6,9 mln osób, co stanowi blisko 70% wszystkich pracujących.

Najwięcej z nich pracowało w mikrofirmach (do 9 zatrudnionych osób). Takich osób było 4,3 mln, tj. 42% ogólnej liczby pracujących. W małych przedsiębiorstwach (10–49 osób) było ich nieco ponad 1 mln, a w średnich (50–249 osób) ponad 1,5 mln.

Natomiast w dużych przedsiębiorstwach, ponad 250 osób, zatrudnionych było 3,4 mln osób, tj. 33% ogólnej liczby pracujących.

Jeśli te proporcje „rozciągniemy” (choć z zastrzeżeniem, że nie będzie to działać liniowo, bo w sektorze przedsiębiorstw mamy właściwie wszystkich pracowników największych firm) na cały polski rynek pracy, to możemy szacować, że w mikrofirmach pracuje ok. 8 mln osób, w małych firmach ok. 2 mln, w średnich ok. 3 mln, a w dużych ok. 4 mln. Widzimy zatem, że dominuje zatrudnienie w firmach najmniejszych, choć także w największych mamy zasób ok. 4 mln pracowników.

To ważne z perspektywy wdrożenia modelu współpracy z pracodawcami. Wydaje się, że dobrą rekomendacją byłoby tutaj „fazowanie”, tj. wprowadzanie etapami wdrożenia takiego modelu współpracy. Warto zacząć od firm największych, schodząc stopniowo w dół do coraz mniejszych. Podobne rozwiązanie zostało z powodzeniem zastosowane w latach 2019–2021 przy wdrażaniu w Polsce nowego systemowego modelu dodatkowego oszczędzania, tj. Pracowniczych Planów Kapitałowych (PPK). Ustawodawca i wdrażająca ten projekt instytucja, którą był Polski Fundusz Rozwoju, doszli do słusznego wniosku, że prościej jest zacząć od dużych firm, które niejako „przetną” ścieżkę proceduralną i instytucjonalną kolejnym, mniejszym podmiotom, niwelując przy okazji lęki – zarówno pracowników, jak i pracodawców – w mniejszych przedsiębiorstwach, z definicji gorzej przygotowanych do sprostania dodatkowym wymogom organizacyjnym.

WNIOSKI I KONKLUZJE

Polski rynek pracy przeszedł, zwłaszcza w ostatniej dekadzie, istotną pozytywną transformację. Liczba pracujących, bezrobotnych, biernych zawodowo, wskaźniki zatrudnienia – wszystkie te parametry notują wyraźną poprawę. Będzie to pozytywnie wpływać na plany wdrożenia dodatkowego modelu budowania odporności państwa we współpracy z pracodawcami i pracownikami. Korzyści mogą być obustronne – dla pracodawców, konkurujących na rynku o pracownika, włączenie elementów szkoleń obronnych do polityki personalnej może być dodatkowym atutem przy rekrutacji i utrzymaniu kadry. Pewnym wyzwaniem jest rozdrobnienie zatrudniających podmiotów, ale można tu wykorzystać model „fazowania”, czyli stopniowego wdrażania rozwiązań – od firm największych po najmniejsze.

2 300
[tys.]
2 200

2 100
2 000

1 900
1 800

1 700
1 600

1 500
1 400

1 300
1 200

1 100
1 000

900
800

700
600

500
450

400
350

300
250

200
150

100
50

0

W Polsce sektor MSP to przytłaczająca większość działających firm, mowa tu o

99,8%

W 2023 r. w podmiotach zaliczanych do MSP (do 249 osób) pracowało ponad **6,9 mln osób**, co stanowi blisko

70% **wszystkich pracujących**

W dużych firmach (ponad 250 osób) pracowało **3,4 mln. osób**

w średnich (50-249 osób) pracowało **ponad 1,5 mln. osób**

w małych (10-49 osób) pracowało **ponad 1 mln. osób**

w mikrofirmach (do 9 osób) pracowało **4,3 mln osób**, tj. 42% ogólnej liczby pracujących

W MIKROFIRMACH PRACUJE **42%** WSZYSTKICH ZATRUDNIONYCH W POLSCE

LICZBA FIRM

W POSZCZEGÓLNYCH GRUPACH WEDŁUG WIELKOŚCI 2014-2023

Rok	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
MIKROFIRMY	1 764,6	1 838,4	1 937,3	2 004,3	2 078,7	2 144,2	2 194,2	2 288,8	2 283,4	2 240,1
MAŁE FIRMY	59,2	56,7	57,2	53,8	52,7	48,9	49,5	48,7	48,2	48,7
ŚREDNIE FIRMY	15,5	15,6	15,4	15,3	15,2	14,8	14,4	14,6	14,3	14,4
DUŻE FIRMY	3,4	3,4	3,6	3,6	3,7	3,8	3,7	3,8	3,8	3,8

Najliczniejszą grupą są mikroprzedsiębiorstwa **97,1%, (2,2 mln firm)**

małe firmy **2,1% (48,7 tys.)**

średnie **0,6% (14,4 tys.)**

duże **0,2% (3,8 tys.)**

Jeśli te proporcje „rozciągniemy”* na cały polski rynek pracy, to możemy szacować, że **w mikrofirmach pracuje ok. 8 mln osób, w małych firmach ok. 2 mln, w średnich ok. 3 mln, a w dużych ok. 4 mln.**

Dominuje zatem zatrudnienie w firmach najmniejszych, choć także w największych mamy zasób ok. 4 mln pracowników.

* z zastrzeżeniem, że nie będzie to działać liniowo, bo w sektorze przedsiębiorstw mamy właściwie wszystkich pracowników największych firm.

INFOGRAFIKA: PIOTR PERZYNA

3. JAK JEST W INNYCH KRAJACH

Maciej Dachowski
Elżbieta Jakubiak
Krzysztof Michalski
Piotr Woyke



Sektor prywatny może być w sposób systemowy zaangażowany w budowę i funkcjonowanie systemu bezpieczeństwa państwa. Potwierdzają to doświadczenia państw o zróżnicowanych uwarunkowaniach geopolitycznych, potencjale gospodarczym czy ludnościowym, które zostały przeanalizowane przez autorów niniejszego raportu.

Państwa, które posłużyły za punkty odniesienia uchodzą w skali globalnej za wzorcowe przykłady organizacji systemu bezpieczeństwa państwa. Ich skuteczność potwierdziły m.in. obserwacje sposobu reagowania na wyzwania związane z pandemią COVID-19, zarówno w wymiarze polityki obronnej, jak i systemu zarządzania kryzysowego. Pomimo wszystkich różnic w modelach rozwoju, poziomie usług publicznych czy sprawności administracyjnej wszystkie przywołane państwa łączy wolnorynkowy charakter gospodarki (oparty na zróżnicowanej strukturze podmiotów prywatnych) oraz demokratyczny ustrój polityczny.

W związku z powyższym autorzy raportu przyjęli, iż opisane państwa mogą stanowić źródło inspiracji dla koncepcji systemowego zaangażowania sektora prywatnego w budowę i funkcjonowanie systemu bezpieczeństwa państwa w Polsce. Szczególnym przykładem jest w tym przypadku Ukraina, od dekad zmagająca się z istotnymi barierami rozwojowymi, ale jednocześnie będąca pod ogromną presją związaną z rozpoczętą w 2014 r. rosyjską agresją zbrojną (po 2022 r. zintensyfikowaną) oraz jej licznymi negatywnymi konsekwencjami. Przy zachowaniu licznych zastrzeżeń rozwiązania ukraińskie, wypracowane często już w trakcie konfliktu, stanowią źródło cennych lekcji dla każdego państwa planującego reformę systemu zarządzania kryzysowego.



SZWECJA – MODEL OBRONY TOTALNEJ

Szwecja od czasów zimnej wojny rozwija koncepcję *Totalförsvaret*, czyli obrony totalnej, która zakłada pełną mobilizację całego społeczeństwa na wypadek wojny. Po latach ograniczania tych przygotowań obecnie kraj ten reaktywuje planowanie obrony totalnej w odpowiedzi na pogorszenie się sytuacji bezpieczeństwa w regionie¹. Istotnym elementem tego modelu jest formalne włączenie przedsiębiorstw prywatnych w wysiłek obronny państwa.

¹ Ważnym elementem szwedzkiej ustawy o obronie totalnej z 2020 r. było wznowienie planowania i odbudowa zdolności w ramach *Totalförsvaret* (obrony totalnej). Szwecja jako jedno z najbardziej zmilitaryzowanych państw Europy Zachodniej w okresie zimnej wojny posiadała rozbudowaną koncepcję obrony totalnej, obejmującą zarówno komponenty wojskowe, jak i cywilne. Po zakończeniu zimnej wojny, w ramach tzw. pokojowej dywidendy, większość procesów planistycznych została wstrzymana, a priorytety obronne przesunięto w stronę misji ekspedycyjnych i reagowania kryzysowego. Zob. B. von Sydow, *Resilience – the Total Defence Concept: A Swedish Perspective*, NATO Review, 2020, <https://www.nato.int/docu/review/articles/2020/10/15/resilience-the-total-defence-concept-a-swedish-perspective/index.html>.

Prawo szwedzkie nakłada na firmy obowiązek uczestnictwa w procesie planowania obrony totalnej.

Oznacza to, że już w czasie pokoju kluczowe przedsiębiorstwa (np. z sektorów infrastruktury, energetyki, transportu, żywności, ochrony zdrowia) są identyfikowane i otrzymują przypisane role na wypadek kryzysu lub wojny. Władze w porozumieniu z sektorem prywatnym ustalają, jakie zasoby i działania muszą być przygotowane, by utrzymać funkcjonowanie kraju, np. planowane jest racjonowanie towarów i energii, tworzenie zapasów strategicznych żywności, awaryjne zasilanie dla firm krytycznych itp.

W razie ogłoszenia najwyższego stanu alarmowego wszystkie funkcje społeczeństwa mają być podporządkowane obronie, zarówno militarnej, jak i cywilnej, włączając w to przedsiębiorstwa prywatne i osoby cywilne. W praktyce oznacza to, że np. firmy transportowe, telekomunikacyjne czy logistyczne wejdą w tryb pracy na rzecz obronności kraju, realizując wcześniej przygotowane zadania. Rola prywatnych przedsiębiorstw rośnie wraz z rozwojem systemu, np. raport szwedzkiej Komisji Obrony sugeruje wyznaczenie listy **kluczowych przedsiębiorstw** i dalsze pogłębianie współpracy państwowo-prywatnej w przygotowaniach obronnych.

Szwedzkie doświadczenie pokazuje, że formalne zobowiązanie firm do udziału w systemie obronnym (poparte odpowiednim prawem i planowaniem) skutkuje lepszą koordynacją i świadomością w społeczeństwie. Firmy wiedzą, czego się od nich oczekuje w sytuacji kryzysowej, inwestują w zabezpieczenia i współpracują z administracją.

Dla Polski wniosek jest taki, że ustanowienie podobnych ram prawnych (np. poprzez ustawowe określenie obowiązków firm kluczowych dla bezpieczeństwa) mogłoby systemowo włączyć biznes w przygotowania obronne kraju.



FINLANDIA – BEZPIECZEŃSTWO POWSZECHNE

Finlandia uchodzi za wzór budowy odporności narodowej opartej na *comprehensive security* – fiń. *kokona-isturvallisuus* – czyli modelu bezpieczeństwa powszechnego. Wymaga ona ścisłej współpracy władz, biznesu, organizacji pozarządowych i obywateli w celu ochrony **żywotnych funkcji społeczeństwa**². Fińskie podejście wywodzi się z doświadczeń II wojny światowej i konieczności utrzymywania ciągłej gotowości na potencjalny konflikt z silniejszym przeciwnikiem.

Obecnie w ramach tej koncepcji funkcjonują m.in.: Narodowa Agencja Zaopatrzenia Kryzysowego (National Emergency Supply Agency – NES) oraz działające przy niej sektorowe *pooles*, czyli platformy współpracy publiczno-prywatnej dla poszczególnych sektorów krytycznych. **Platformy bezpieczeństwa dostaw** grupują przedsiębiorstwa prywatne i instytucje publiczne w takich dziedzinach jak: energetyka, transport, żywność, ochrona zdrowia, technologie cyfrowe czy media. Ich zadaniem jest wspólne planowanie ciągłości działania (*business continuity*) na wypadek kryzysów – firmy wymieniają się informacjami, przeprowadzają ćwiczenia razem z administracją, uzgadniają standardy zabezpieczeń. Prywatny sektor odgrywa

2 Fińska koncepcja bezpieczeństwa powszechnego (*comprehensive security*) zakłada współodpowiedzialność administracji publicznej, sektora prywatnego, organizacji pozarządowych i obywateli za ochronę kluczowych funkcji państwa. Model oparty jest na wspólnym przygotowaniu i zdolności całego społeczeństwa do szybkiej mobilizacji zasobów, elastycznego dostosowania się do kryzysu i szybkiego odtwarzania funkcji po jego zakończeniu. Fundamentem koncepcji jest powojenna doktryna obrony totalnej, której współczesny opis zawarto w *Strategii Bezpieczeństwa Społeczeństwa* z 2017 r. Zob. Government of Finland, *Security Strategy for Society*, 2017, <https://turvallisuuskomitea.fi/en/security-strategy-for-society/>.

w tym modelu bardzo ważną rolę, ponieważ to on operuje większością infrastruktury krytycznej i usług kluczowych dla społeczeństwa.

Rząd fiński podkreśla, że w przygotowaniu na kryzysy **każdy ma swoją rolę** – administracja koordynuje całość i zapewnia ramy prawne, ale biznes odpowiada za ciągłość działania swoich systemów i wsparcie państwa w sytuacji zagrożenia. Przykładowo, w Finlandii utrzymywane są strategiczne rezerwy pewnych towarów (paliw, zboża, leków), ale odbywa się to we współpracy z firmami. Część zapasów składowana jest w przedsiębiorstwach na normalnych zasadach rynkowych z zastrzeżeniem uruchomienia mechanizmów interwencji państwa w razie kryzysu.

Co ważne, Finlandia buduje też odporność poprzez szkolenia obronne dla cywilów i kadry kierowniczej. Od lat 60. XX wieku organizowane są kursy obrony państwa (Państwowe Kursy Obronności) dla urzędników, liderów biznesu i NGO. Ich uczestnicy poznają zasady działania systemu bezpieczeństwa, współpracy cywilno-wojskowej, procedury kryzysowe. Dzięki temu elity różnych sektorów zyskują wspólne zrozumienie zadań obronnych. Dla Polski fiński model jest cenną inspiracją: pokazuje, jak instytucjonalizować współpracę z firmami na co dzień (przez stałe platformy/pule), jak budować zaufanie między rządem a biznesem oraz jak edukować liderów cywilnych w zakresie bezpieczeństwa. Warto podkreślić, że włączenie sektora prywatnego w przygotowania społeczeństwa traktowane jest w Finlandii jako warunek utrzymania ciągłości funkcjonowania państwa, co w praktyce się sprawdza (przykładowo, fińska infrastruktura energetyczna czy telekomunikacyjna, choć prywatna, ma bardzo wysokie standardy zabezpieczeń na wypadek konfliktu). Jak ujął to sekretarz generalny fińskiej Rady Bezpieczeństwa: „sektor prywatny ma kluczową rolę w naszym modelu bezpieczeństwa i wspólnie będziemy nadal rozwijać przygotowania”³.



SZWAJCARIA – SUBSYDIARNOŚĆ JAKO MODEL

Szwajcaria od dziesięcioleci⁴ rozwija unikalny system obrony totalnej (*Gesamtverteidigung*), który w sposób kompleksowy włącza sektor prywatny w przygotowania obronne państwa. Model szwajcarski opiera się na konstytucyjnym mandacie zabezpieczenia gospodarczego kraju oraz rozwiniętym systemie współpracy między państwem a przedsiębiorstwami prywatnymi w zakresie zaopatrzenia narodowego.

Podstawą prawną systemu jest art. 102 Konstytucji Federalnej⁵, który stanowi, że Konfederacja zapewnia zaopatrzenie kraju w niezbędne towary i usługi w przypadku zagrożenia konfliktem polityczno-militarnym lub wojną. Przepis ten umożliwia odstępnie od zasady wolności gospodarczej, w sytuacji gdy wymaga tego bezpieczeństwo narodowe. Centralną instytucją systemu jest Federalny Urząd Zaopatrzenia Gospodarczego Kraju (Federal Office for National Economic Supply – FONES⁶), który przygotowuje środki zarządzania gospodarczego na wypadek kryzysu. FONES jest urzędem federalnym, lecz działa w ścisłej kooperacji z ok. 250 ekspertami z sektora prywatnego i branżowego, którzy wnoszą wiedzę specjalistyczną. Taka hybrydowa praktyka zapewnia bliską współpracę między administracją państwową a biznesem już w czasie pokoju. Dla każdego z obszarów (żywność, energia, surowce przemysłowe, produkty chemiczne i farmaceutyczne

3 Oświadczenie Sekretarza Generalnego Fińskiego Komitetu ds. Bezpieczeństwa (Turvallisuuskomitea), <https://turvallisuuskomitea.fi/en/>.

4 Szwajcaria po raz pierwszy przedstawiła kompleksową koncepcję obronną już w 1973 r.: Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz, 27.06.1973, <https://www.amtsdruckschriften.bar.admin.ch/viewOrigDoc/10045832.pdf?ID=10045832>.

5 Art. 102 Konstytucji Federalnej Szwajcarii: (cyt.) 1. Federacja zabezpiecza zaopatrzenie kraju w niezbędne do życia środki i usługi w wypadku zagrożenia politycznego lub wojennego, jak również w sytuacjach ciężkiego deficytu, z którym gospodarka sama nie jest w stanie się uporać. Podejmuje środki zapobiegawcze. 2. W razie konieczności może ona odstąpić od zasady wolności gospodarczej. Konstytucja Federalna Szwajcarii, <https://libr.sejm.gov.pl/tek01/txt/konst/szwajcaria-r3.html>.

6 Hub for National Economic Supply of Switzerland, Federal Office for National Economic Supply FONES, <https://www.bwl.admin.ch/en>.

oraz usługi transportowe) opracowane są szczegółowe plany zarządzania kryzysowego, które przewidują różne formy interwencji państwa – od zwiększenia dostaw poprzez uwolnienie obowiązkowych zapasów po ograniczenia popytu przez reglamentację i zakazy.

Szwajcaria utrzymuje również system ochrony ludności (*Zivilschutz*) oparty na pięciu filarach współpracy, którymi są policja, straż pożarna, służby medyczne, służby techniczne oraz ochrona ludności jako taka. System ten angażuje zarówno sektor publiczny, jak i prywatny w przygotowania obronne⁷, przy czym każdy kanton ma swobodę dostosowania swoich sił ochrony ludności do lokalnych zagrożeń i warunków.

Model szwajcarski pokazuje, jak można skutecznie połączyć liberalną gospodarkę rynkową z systemowymi przygotowaniami obronnymi. Kluczowe jest utrzymanie zasady subsydiarności – państwo interweniuje tylko wtedy, gdy sektor prywatny nie może samodzielnie zapewnić zaopatrzenia. System opiera się na partnerstwie z biznesem, a nie na zastępowaniu go strukturami państwowymi.

Dla Polski szwajcarskie doświadczenia wskazują na wartość konstytucyjnego umocowania obowiązków gospodarczego zabezpieczenia narodowego oraz stworzenia hybrydowych struktur łączących administrację państwową z ekspertyzą sektora prywatnego.



UKRAINA

– SZYBKA ADAPTACJA, PARTNERSTWO Z BIZNESEM

Ukraina, w obliczu brutalnej rosyjskiej agresji od 2022 r., przeprowadza szybką transformację prawnych i instytucjonalnych ram angażowania sektora prywatnego w wysiłek obronny. Proces ten obejmuje zarówno adaptację istniejących mechanizmów współpracy publiczno-prywatnej, jak i tworzenie zupełnie nowych instrumentów prawnych, dostosowanych do warunków gospodarki wojennej.

Jednym z najnowszych narzędzi mających na celu budowanie partnerstwa publiczno-prywatnego dostosowanego do potrzeb odbudowy powojennej i wzmocnienia zdolności obronnych jest uchwalona w czerwcu 2025 r. ustawa nr 7508⁸, która umożliwia realizację wspólnych projektów obronnych państwa i sektora prywatnego. Nowe prawo pozwala na przyciąganie prywatnych inwestycji do sektora wojskowo-przemysłowego, rozwój zdolności technologicznych kraju i modernizację produkcji. Ministerstwo Gospodarki oczekuje, że ustawa ta pozwoli na przyciągnięcie w nadchodzących latach do 1 mld dolarów inwestycji w konkretne projekty⁹.

W związku z trwającą wojną Ukraina znacząco rozszerzyła obowiązki przedsiębiorstw w zakresie ewidencji wojskowej. Uchwalona w 2024 r. ustawa o przygotowaniu mobilizacyjnym¹⁰ nakłada na pracodawców obowiązek prowadzenia ewidencji pracowników na podstawie aktualnych dokumentów wojskowych, uczestnictwa w powiadamianiu pracowników oraz zgłaszania naruszeń w tej kwestii do terytorialnych centrów

7 A. Gołębiowska, W. Jakubczak, *Constitutional Determinants of Local Government Responsibility for Civil Protection as a Part of Security System in the Confederation of Switzerland*, "European Research Studies Journal" 2021, Vol. XXIV, Issue 4, s. 930–940, <https://ersj.eu/journal/2643/download/Constitutional+Determinants+of+Local+Government+Responsibility+for+Civil+Protection+as+a+Part+of+S+ecurity+System+in+the+Confederation+of+Switzerland.pdf>.

8 Zelenskyy signed the law on public-private partnership: it will promote the development of joint weapons production, UNN, 30.07.2025, <https://unn.ua/en/news/zelenskyy-signed-the-law-on-public-private-partnership-it-will-promote-the-development-of-joint-weapons-production>.

9 B. Черевко, *The Ukrainian Parliament has opened the opportunity for cooperation between the state and business in the defense sector*, 19.06.2025, <https://mezha.media/en/oboronka/verhovna-rada-uhvalila-zakon-pro-dpp-302805/>.

10 J. Ber, *Ukraina: korekta polityki mobilizacyjnej*, Analizy OSW, 17.04.2024, <https://www.osw.waw.pl/pl/publikacje/analizy/2024-04-17/ukraina-korekta-polityki-mobilizacyjnej>.

rekrutacyjnych¹¹. Przedsiębiorstwa muszą wyznaczyć osoby odpowiedzialne za nadzór nad wypełnianiem obowiązków wojskowych przez pracowników, badaniami lekarskimi, szkoleniami i gotowością do mobilizacji.

W odpowiedzi na zagrożenia wojenne Narodowy Bank Ukrainy wprowadził rozwiązania umożliwiające ukraińskim bankom korzystanie z usług w chmurze opartych na sprzęcie znajdującym się w Unii Europejskiej, Zjednoczonym Królestwie, USA i Kanadzie¹². Mechanizm ten pozwolił instytucjom finansowym na natychmiastowe wznowienie podstawowej działalności oraz ochronę istotnych informacji w razie zniszczenia materialnej infrastruktury bankowej w kraju. Ucząc się na doświadczeniach z pierwszej fazy wojny, banki konsekwentnie udoskonalają procedury zarządzania sytuacjami nadzwyczajnymi, przechodząc od działań doraźnej stabilizacji do długofalowych strategii odporności¹³.

Po zakończeniu wojny Ukraina stanie przed wyzwaniem ponownego zintegrowania setek tysięcy weteranów z wyjątkowym doświadczeniem bojowym z życiem cywilnym w warunkach pokoju, a także potrzebą legalizacji działania ukraińskich prywatnych firm wojskowych i bezpieczeństwa. Projekt ustawy nr 13257 z maja 2025 r.¹⁴ ma na celu wykorzystanie unikalnego doświadczenia weteranów oraz zapewnienie im godnego, wysoko kwalifikowanego zatrudnienia po demobilizacji. Ukraińskie PMSCs (Private Military and Security Companies) mogłyby świadczyć usługi za granicą, obejmujące ochronę osób i mienia, szkolenie zagranicznego personelu wojskowego, działania rozminowywania oraz konsultacje w zakresie bezpieczeństwa.

Ukraiński model pokazuje, jak państwo może szybko adaptować ramy prawne i instytucjonalne do warunków wojny, jednocześnie przygotowując się na wyzwania okresu powojennego. Kluczowe jest połączenie bieżących potrzeb obronnych z długoterminową wizją odbudowy i rozwoju gospodarczego.



WIELKA BRYTANIA – MOCNE WŁĄCZANIE FIRM W SFERĘ BEZPIECZEŃSTWA

Od początku XXI wieku Wielka Brytania rozwija kompleksowy system odporności narodowej oparty na formalnej współpracy między sektorem publicznym a prywatnym. Podstawą prawną tego systemu jest ustawa Civil Contingencies Act z 2004 r.¹⁵, która wprowadziła dwustopniowy model odpowiedzialności za bezpieczeństwo narodowe i ciągłość działania w sytuacjach kryzysowych.

Pierwszy z nich, Category 1, obejmuje głównie organy publiczne (takie jak władze lokalne, policja, NHS, służby ratunkowe), które mają pełny zakres obowiązków wynikających z CCA. Category 2 to m.in. prywatne przedsiębiorstwa użyteczności publicznej, firmy transportowe i telekomunikacyjne. Ich rola polega przede wszystkim na współpracy z organami Category 1 – udział w planowaniu, udostępnianiu informacji i wspieraniu działań w ramach Local Resilience Forums (LRF)¹⁶.

11 K. Sakharova, *Employer's compliance with Ukrainian military regulations*, Legal Analysis, <https://frishberg.com/explained-employers-compliance-with-ukrainian-military-regulations/>.

12 A. Podyerogin, *Payments in wartime: the story of the National Bank of Ukraine*, 28.02.2023, <https://www.europeanpaymentscouncil.eu/news-insights/insight/payments-wartime-story-national-bank-ukraine>.

13 *Central banking in wartime. Lessons from Ukraine*, 1.07.2024, <https://www.hhs.se/en/houseoffinance/outreach/news-press/news/2024/central-banking-in-wartime-lessons-from-ukraine/>.

14 T. Tarasenko, *A new mission for veteran soldiers. Why Ukraine needs its own private military and security companies*, <https://en.interfax.com.ua/news/blog/1072959.html>.

15 *Preparation and planning for emergencies: responsibilities of responder agencies and others*, 20.02.2013, <https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others>.

16 *Local resilience forums: contact details*, 20.02.2013, <https://www.gov.uk/guidance/local-resilience-forums-contact-details>.

Local Resilience Forums (LRF) są lokalnymi platformami współpracy i koordynacji wszystkich kategorii podmiotów zaangażowanych w zarządzanie kryzysowe oraz przygotowania do sytuacji nadzwyczajnych. To właśnie w ramach LRF ustala się konkretne wymogi, wymienia informacje i przygotowuje wspólne działania na wypadek sytuacji kryzysowych. Natomiast w praktyce działania związane z bezpieczeństwem ludności coraz częściej przenikają się z szerszym kontekstem strategii bezpieczeństwa państwa – rząd odwołuje się do koncepcji „whole-of-society resilience”.

Nowa Strategia Bezpieczeństwa Narodowego z 2025 r.¹⁷ znacząco wzmacnia rolę sektora prywatnego w systemie bezpieczeństwa. Dokument przewiduje wydatki na bezpieczeństwo narodowe w wysokości 5% PKB, co stanowi historyczny wzrost inwestycji obronnych. Strategia podkreśla konieczność ścisłego połączenia celów bezpieczeństwa narodowego z planami wzrostu gospodarczego. Ma to obejmować wykorzystanie narodowych potencjałów produkcyjnych, przemysłowych, technologicznych i naukowych dla celów bezpieczeństwa oraz budowania odporności całego społeczeństwa. Rząd brytyjski wprowadza także nowe narzędzia współpracy z sektorem prywatnym poprzez UK Government Resilience Action Plan. Przewiduje on rozszerzenie szkoleń dla pracowników sektora prywatnego przez UK Resilience Academy, która ma kształcić do 4000 osób rocznie z obu sektorów – publicznego i prywatnego. Dodatkowo tworzone jest nowe Supply Chain Centre oraz Economic Security Advisory Service, które będą współpracować z biznesem w diagnozowaniu zagrożeń i podatności łańcuchów dostaw¹⁸.

Wielka Brytania dysponuje także nadzwyczajnymi uprawnieniami do interwencji państwa w działalność przedsiębiorstw strategicznych, co pokazuje na przykład ustawa Steel Industry (Special Measures) Act z 2025 r.¹⁹. Daje ona rządowi uprawnienia do wydawania poleceń zarządom firm stalowych, zapewniania wypłat wynagrodzeń i zamawiania surowców do utrzymania działania pieców hutniczych, gdy jest to w interesie publicznym, tj. np. dla zachowania istotnej z punktu widzenia bezpieczeństwa bazy przemysłowej²⁰.

Brytyjski model pokazuje ewolucję od tradycyjnego planowania kryzysowego w kierunku zintegrowanego systemu odporności narodowej, w którym sektor prywatny ma jasno określone obowiązki prawne oraz otrzymuje wsparcie rządowe w przygotowaniach. System jest oparty na partnerstwie publiczno-prywatnym z zachowaniem subsydiarności – państwo interweniuje tylko wtedy, gdy sektor prywatny nie może sam sprostać wyzwaniom.

Dla Polski brytyjskie doświadczenia wskazują na wartość formalnego uregulowania obowiązków firm kluczowych oraz stworzenia stałych platform współpracy między administracją a biznesem na poziomie lokalnym i regionalnym.

17 National Security Strategy 2025. Security for the British People in a dangerous world, 29.08.2025, <https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world.html>.

18 UK Government Resilience Action Plan, 14.07.2025, <https://www.gov.uk/government/publications/uk-government-resilience-action-plan/uk-government-resilience-action-plan.html>.

19 Steel Industry (Special Measures) Act 2025, <https://www.legislation.gov.uk/ukpga/2025/13/contents>.

20 Government acts to save British steel production, 12.04.2025, <http://www.gov.uk/government/news/government-acts-to-save-british-steel-production>.



KOREA POŁUDNIOWA – PEŁNA INTEGRACJA Z BIZNESEM

W Korei Południowej bezpieczeństwo narodowe rozumiane jest jako zadanie całego społeczeństwa, w którym przedsiębiorcy wszystkich sektorów mają określone role i obowiązki. Model południowokoreański integruje biznes nie tylko w obszarze obronnym, ale także w zarządzaniu ryzykiem naturalnym, cyberzagrożeniami, kryzysami zdrowotnymi oraz ciągłością funkcjonowania państwa. Przedsiębiorcy aktywnie uczestniczą w narodowych debatach o kształcie polityki bezpieczeństwa, innowacji i odporności cyfrowej.

Konglomeraty IT, takie jak Samsung czy LG, oraz setki startupów w ekosystemie technologii są włączone w mechanizmy reagowania na cyberzagrożenia. Ministerstwo Nauki i ICT (MSIT) prowadzi z nimi ćwiczenia typu Red Team, a firmy uczestniczą w wymianie informacji o podatnościach i incydentach w ramach Korea Internet & Security Agency (KISA). System obejmuje obowiązkowe certyfikacje ISMS (Information Security Management System) dla określonych dużych firm, np. dostawców usług internetowych lub szkół z ponad 10 tys. uczniów²¹. Dzięki temu sieci telekomunikacyjne i platformy e-commerce utrzymują wysoki poziom odporności na zakłócenia.

Banki i instytucje finansowe są zobowiązane do uczestnictwa w systemie zapewniającym ciągłość działania, który gwarantuje nieprzerwane funkcjonowanie systemów płatności i dostęp do środków dla obywateli i instytucji państwowych. Regularnie testowane są procedury awaryjnej łączności i odtwarzania danych, a cyberochrona bankowa współdziała z narodowym CSIRT w zakresie zapobiegania atakom²².

National Civil Defense and Disaster Management Training Institute (NDTI) organizuje co roku kursy i warsztaty dla kadry menedżerskiej w firmach z różnych branż – od logistyki po IT – w ramach programu szkoleń z zarządzania kryzysowego²³. Uczestnicy poznają procedury zarządzania kryzysowego, zasady współpracy międzysektorowej i komunikacji kryzysowej, budując kulturę proaktywnego zarządzania ryzykiem.

Przykład Korei Południowej pokazuje, jak w warunkach podwyższonego zagrożenia bezpieczeństwo narodowe staje się sprawą wszystkich przedsiębiorców, od sektora obronnego i ICT po logistykę, energetykę i opiekę zdrowotną. Rząd kształtuje system, w którym biznes jest nie tylko wykonawcą zamówień państwowych, ale i aktywnym współtwórcą i uczestnikiem strategii bezpieczeństwa całego kraju.

Przykład ten może być inspiracją dla takich państw jak Polska przy projektowaniu modelu „whole-of-society resilience”: kluczowa jest szeroka codzienna współpraca administracji i biznesu w budowie odporności narodowej.

21 Achieve Korea Personal Information and Information Security Management System (ISMS-P) Compliance, May 2023, https://cpl.thalesgroup.com/sites/default/files/content/compliance_brief/field_document/2023-06/2023-isms-p-kr-cb-a4.pdf.

22 About FSI, <https://www.fsec.or.kr/bbs/448>.

23 About NDTI, <https://dcab.co.kr/web/ndti/whoweare>.

KONKLUZJE I WNIOSKI

Analiza przytoczonych przykładów pozwala sformułować kilka wniosków i wskazać cechy łączące omówione modele. Jakie zasady powinny stanowić fundament systemowego włączania sektora prywatnego w struktury bezpieczeństwa państwa? Czego możemy nauczyć się od innych?

- Zaangażowanie sektora prywatnego w system bezpieczeństwa państwa jest kluczowe dla zwiększenia odporności całego państwa i społeczeństwa.** Podmioty biznesowe odpowiadają dzisiaj za realizację szeregu kluczowych z punktu widzenia funkcjonowania państwa i społeczeństwa procesów, takich jak m.in. funkcjonowanie systemów: energetycznego, transportowego, logistycznego, finansowego. Podmioty prywatne zazwyczaj odgrywają również istotną rolę w świadczeniu usług edukacyjnych, zdrowotnych czy produkcji podstawowych dóbr, jak żywność czy leki. Przygotowanie tych procesów i ich najważniejszych interesariuszy na sytuacje kryzysowe (w tym przedłużające się i intensywne, jak konflikt zbrojny) może okazać się decydujące dla przetrwania państwa oraz jego obywateli. W przypadku demokratycznych, wolnorynkowych systemów oznacza to konieczność planowania z wyprzedzeniem i komunikowania klarownych oczekiwań państwa i stworzenia przewidywalnych ram postępowania dla przedsiębiorstw, tak jak w Finlandii czy Korei Południowej. Powinny to być nie tylko obowiązkowe świadczenia wynikające z regulacji, ale również pakiet działań wspierających ze strony państwa (ułatwienia dla szczególnie istotnych podmiotów biznesowych, np. operatorów infrastruktury krytycznej, szkolenia dla wybranych grup kadr) czy tworzenie bodźców na rzecz wsparcia bezpieczeństwa państwa (np. stymulowanie wpisywania działań na rzecz odporności w społeczną odpowiedzialność biznesu).
- W sytuacjach kryzysowych sektor prywatny jest istotnym rezerwuarem zasobów materiałowych, ludzkich, usługowych i organizacyjnych – rząd musi wiedzieć, czym dysponuje i w jaki sposób może z wymienionych zasobów korzystać.** Bezpieczeństwo narodowe jako absolutny priorytet to zasada, która powinna organizować działania nie tylko klasy politycznej, ale również obywateli i tworzonych przez nich przedsiębiorstw. Już obecnie w Polsce obowiązują przepisy dotyczące obowiązkowych świadczeń na rzecz państwa w czasie kryzysu. Nie są one jednak przystosowane do współczesnych uwarunkowań technologicznych (takich jak możliwość szybkiej komunikacji, agregowania i przetwarzania dużych zbiorów danych) ani przyjazne dla sektora prywatnego: większość przedsiębiorców nie ma obecnie dostatecznej wiedzy o obowiązkach oraz możliwościach wsparcia państwa, służb czy samorządu w obszarze zarządzania kryzysowego. Warto studiować doświadczenia brytyjskie, fińskie czy szwajcarskie w tej kwestii.
- Przedsiębiorcy mogą oczekiwać od państwa przewidywalności procedur zarządzania kryzysowego oraz wsparcia w utrzymaniu gotowości na sytuacje kryzysowe.** O ile same sytuacje kryzysowe zawsze mają nieprzewidywany przebieg, o tyle istnieją efektywne sposoby przygotowania się na ich konsekwencje, związane np. z brakiem ciągłości dostaw energii, ustaniem możliwości świadczenia usługi, produkcji danego typu towarów czy wykorzystania poszczególnych komponentów. Organy państwowe, dysponując unikalną, często niedostępną w warunkach rynkowych wiedzą o ryzykach, kompetencjami w zakresie zabezpieczeń infrastruktury czy systemów informatycznych oraz zobowiązaniami prawnymi i zasobami służącymi reagowaniu kryzysowemu, mogą wyjść z inicjatywą i pomagać sektorowi prywatnemu w przygotowaniu na czas kryzysu. To kluczowy warunek udanego zaangażowania przedsiębiorstw w budowę systemu bezpieczeństwa państwa, co odzwierciedlają m.in. odpowiednie regulacje prawne wdrożone w Szwecji czy – stosunkowo niedawno, w czerwcu 2025 r. – na Ukrainie.

4. KONCEPCJA WŁĄCZENIA SEKTORA PRYWATNEGO W TWORZENIE SYSTEMU BEZPIECZEŃSTWA PAŃSTWA

Maciej Dachowski
Michał Dworczyk
Bartosz Marczuk
Piotr Woyke
Robert Draba



Przedsiębiորcy stanowią fundament gospodarki narodowej, który w trakcie kryzysów bezpieczeństwa narodowego (z zagrożeniem wojennym włącznie) będzie szczególnie narażony na ich negatywne konsekwencje. Są one nieuniknione, a sektor prywatny musi być jednocześnie gotowy do solidarnego ponoszenia kosztów reagowania kryzysowego. W szerszej perspektywie możliwość zachowania ciągłości procesów gospodarczych stanowi istotny element podnoszenia odporności państwa i społeczeństwa na kryzysy.

Podmioty sektora prywatnego potrzebują transparentnego, dobrze skomunikowanego systemu mobilizowania ich zasobów na wypadek kryzysów (szczególnie pracowników), aby móc lepiej przygotować się pod względem zarządczym. Bezpieczeństwo państwa to złożone zagadnienie, które obejmuje znacznie więcej niż tylko obronność. W czasach kryzysów, takich jak konflikt zbrojny, masowy kryzys migracyjny czy akty sabotażu na dużą skalę, konieczne jest zadbanie o sprawne funkcjonowanie systemów logistycznych, finansowych czy komunikacyjnych.

W związku z powyższym wypracowano zestaw rekomendacji w zakresie polityki publicznej, inspirowanych rozwiązaniami przyjętymi w innych państwach oraz analizą uwarunkowań polskich. W naszej ocenie ich wdrożenie pozwoli na większą stabilność regulacyjną oraz organizacyjną zarówno struktur państwowych, jak i prywatnych w obliczu potencjalnych kryzysów, szczególnie w kluczowym obszarze personalnym. Propozycje rozwiązań, będące efektem wspólnych prac badawczych Instytutu Wschodniej Flanki, Instytutu Sobieskiego i Oldman Sage nawiązują do opublikowanego w czerwcu 2025 r. raportu analitycznego pt. *Powszechna Służba Państwowa. Program budowy rezerw osobowych na rzecz bezpieczeństwa RP*.

Twórcy wymienionego dokumentu postulowali „stworzenie kompleksowego rozwiązania, tj. Powszechnej Służby Państwowej (PSP), przewidującego szkolenie młodych Polaków do tej służby. Choć ma być ona obojętna, to zakłada element wyboru, atrakcyjność szkoleń, funkcję ich godzenia z karierą zawodową czy edukacją, a nawet dodatkowe benefity z jej odbycia do wykorzystania na rynku pracy. Proponujemy zupełnie nowe rozwiązanie i podejście, oparte na doświadczeniach innych krajów. To nie żadna «branka» ani znany z PRL-u «pobór», ale nowoczesna i elastyczna forma szkolenia rezerw dla armii i w celu budowania odporności państwa”²⁴. Zaprezentowane rekomendacje dotyczące współpracy z sektorem prywatnym są komplementarne wobec koncepcji utworzenia PSP i stanowią drugi filar budowania osobowych rezerw na rzecz wspierania odporności państwa, niemniej wybrane elementy mogą zostać wdrożone nawet szybciej przy odpowiednim porozumieniu w trójkącie: regulator – pracodawcy – pracownicy.

FIRMY WESPRĄ BEZPIECZEŃSTWO

Analiza wykazała, że prywatni przedsiębiorcy już dziś odgrywają istotną rolę w bezpieczeństwie państwa, a przy odpowiednim wsparciu mogą tę rolę znacząco zwiększyć. Sektor prywatny dysponuje większością zasobów infrastrukturalnych i ludzkich kraju, od sieci energetycznych przez systemy teleinformatyczne po wykwalifikowany personel techniczny, dlatego w sytuacji kryzysu lub wojny nie można skutecznie bronić państwa bez zaangażowania tych podmiotów.

Co więcej, wysoki poziom deklarowanej gotowości firm i pracowników do udziału w szkoleniach i strukturach obronnych jest kapitałem społecznym, który należy wykorzystać. Przytoczone wcześniej dane i przykłady dowodzą, że sektor prywatny w Polsce jest gotów wziąć na siebie tę odpowiedzialność, jeśli państwo stworzy przejrzyste reguły gry i zapewni odpowiednie wsparcie. Niezbędne jest uchwalenie rozwiązań, które umożliwią firmom szkolenie pracowników na masową skalę, wspomaganie struktur ochrony ludności i obrony cywilnej oraz utrzymanie działania infrastruktury w warunkach kryzysu.

Wdrożenie proponowanych zmian wzmocni etos odporności w społeczeństwie i realnie zwiększy zdolności obronne kraju. Pokazując obywatelom, że bezpieczeństwo jest wspólną sprawą, zyskujemy solidne podstawy do obrony.

Dzięki temu Polska będzie lepiej przygotowana na wrogie działania hybrydowe i potencjalny konflikt konwencjonalny. Możliwe będzie pełne wykorzystanie potencjału i patriotyzmu polskiego biznesu, co dodatkowo wzmocni nasz system obronny.

Pożądane jest doskonalenie niżej opisanych rekomendacji w ramach dialogu trójstronnego. Większość z nich wiąże się ze zmianami regulacji prawnych (w tym ustawowych), ale również zmianami o charakterze systemowym, często sięgającymi wrażliwych aspektów systemu bezpieczeństwa państwa, jak np. system mobilizacyjny. W związku z powyższym każda rekomendacja została opatrzona konkretnym przykładem instrumentów prawnych, organizacyjnych lub finansowych pozwalających zrozumieć stojące za nią intencje. W potencjalnym procesie legislacyjnym należy uwzględnić ekspertyzy zarówno wojskowe, jak i ekonomiczne, tak aby projektowane prawo było proporcjonalne, realistyczne i sprawiedliwe, dokładnie tak, jak postulowano w apelu z lipca 2024 r.

24 Powszechna Służba Państwowa. Program budowy rezerw osobowych na rzecz bezpieczeństwa RP, Instytut Sobieskiego, Instytut Wschodniej Flanki, Warszawa 2025, <https://wschodniaflanka.pl/raport-o-powszechnej-sluzbie-panstwowej-zapoznaj-sie-z-publicacja/>.

APEL ORGANIZACJI PRZEDSIĘBIORCÓW

W lipcu 2024 r. organizacje przedsiębiorców wystąpiły z apelem do ministra spraw wewnętrznych i administracji w sprawie projektowanej ustawy o ochronie ludności i obronie cywilnej. W apelu podkreślono, że proponowane rozwiązania w obecnym kształcie nakładają na firmy nieproporcjonalne obciążenia finansowe i organizacyjne, które mogą sparaliżować inwestycje i działalność gospodarczą. Przedsiębiorcy wskazali na konieczność wydłużenia *vacatio legis* do co najmniej sześciu miesięcy, doprecyzowania używanych pojęć oraz usunięcia przepisów sprzecznych z ustawą Prawo budowlane. Podkreślono również, że koszty związane z budową i utrzymaniem obiektów ochronnych powinny być finansowane przez państwo, a rola sektora prywatnego powinna polegać na partnerskim udziale w dialogu i wdrażaniu rozwiązań, nie zaś na ponoszeniu nowych obciążeń.

Pełny tekst apelu dostępny jest pod adresem:

www.bcc.org.pl/apel-do-ministra-spraw-wewnetrznych-i-administracji-o-pilne-wprowadzenie-zmian-w-projektowanych-przepisach-o-ochronie-ludnosci.

GŁÓWNE ZAŁOŻENIA NOWEGO SYSTEMU

Zanim przejdziemy do omówienia rekomendacji oraz mechanizmów wdrażających system budowy odporności państwa we współpracy z pracodawcami, zaprezentujemy krótko kluczowe obszary takiej kooperacji. Wychodząc z założenia, że obecna sytuacja jest niepożądana – brakuje m.in. koordynacji współpracy, zachęt systemowych dla pracowników i firm, by angażować się w budowanie odporności, system jest rozproszony, jeśli chodzi o kompetencje i zadania, przez co realnie nie funkcjonuje – proponujemy oprzeć go na czterech głównych filarach:

Filar współpracy z firmami dotyczący wykorzystania pracowników i zasobów firm na wypadek kryzysów/wojny. Chodzi o przejrzyste zasady, modele współpracy, przepływ informacji na linii państwo–pracodawcy, by służby państwa wiedziały, jakimi zasobami osobowymi i materiałowymi dysponują w przedsiębiorstwach, a pracodawcy mieli wgląd w przewidywalny dla nich system mobilizacji ich zasobów na wypadek sytuacji kryzysowych. Chodzi też o racjonalne, ze strony państwa, wykorzystywanie zasobów firm, by nie utraciły one ciągłości działania. W ten obszar wchodzi także system „kontyngentów” ze strony firm na rzecz państwa w razie sytuacji kryzysowych, ale nie mobilizacyjnych, takich jak na przykład cyberataki czy powódzie. Dotyczy to bieżącej współpracy na linii państwo–firmy, w której obie strony wiedzą, czego mogą się po sobie spodziewać, i działają w trybie ciągłym, a nie nadzwyczajnym, i wykorzystują zdobyte doświadczenie także w razie zagrożeń czy kryzysów.

Filar szkoleniowy, który zakłada wykorzystanie pracodawców do prowadzenia licencjonowanych szkoleń dla firm i ich pracowników, organizowanych i nadzorowanych przez państwo.

Filar certyfikacji firm, jako sposób ich „wyróżniania” i „nagradzania” za wysiłek włożony w budowę odporności państwa. Tutaj także postulujemy wprowadzenie preferencji dla firm, które podejmują taki wysiłek.

Filar komunikacyjny, czyli wykorzystanie infrastruktury i środków komunikacji firm na wypadek sytuacji zagrożeń czy kryzysów jako sprawny i szybki kanał komunikacji na linii państwo–obywatele.

TRZY OGÓLNE MECHANIZMY WDRAŻAJĄCE, KTÓRE NADAJĄ RAMY SYSTEMOWI

SKĄD MAJĄ POCHODZIĆ ŚRODKI NA REALIZACJĘ DZIAŁAŃ

FUNDUSZ ODPORNOŚCI PAŃSTWOWEJ

Polska już dziś wydaje ogromne kwoty na działania związane z ochroną ludności, modernizacją, cyber i edukacją. Środki te są rozproszone – należy je skonsolidować – dzięki temu powstanie stabilny, przejrzysty i elastyczny instrument finansowania, który zapewni ramy wdrożenia wszystkich rekomendacji szczegółowych niniejszego raportu.

SYSTEM CERTYFIKACJI WYZNACZA
PRZEJRZYSTE STANDARDY I ZASADY PREMIOWANIA PRZEDSIĘBIORSTW

SYSTEM CERTYFIKACJI ODPORNOŚCI (COP)

System certyfikacji odporności (COP) mógłby objąć docelowo kilkadziesiąt tysięcy przedsiębiorstw i miliony pracowników, tworząc jednolite, państwowe narzędzie weryfikacji i premiowania zaangażowania biznesu w bezpieczeństwo i odporność.

WPROWADZENIE COP ROZWIĄDUJE TRZY KLUCZOWE PROBLEMY:

BRAK SPÓJNYCH STANDARDÓW OCENY ODPORNOŚCI FIRM

który dziś sprawia, że wysiłki biznesu nie są ani mierzalne, ani porównywalne

BRAK MOTYWACJI DLA PRZEDSIĘBIORSTW

które bez systemu zachęt traktują działania obronne jako koszt, a nie inwestycję

BRAK INTEGRACJI

bo działania szkoleniowe, inwestycyjne i CSR funkcjonują równolegle, a COP pozwoli je spiąć w jedną strukturę

Powstałby stabilny mechanizm, pozwalający mierzyć wkład firm w budowę odporności, a jednocześnie zapewniający im korzyści – finansowe, prestiżowe i organizacyjne.

W POLSCE
DZIAŁA 50 TYS.
FIRM
ŚREDNICH I DUŻYCH.
TO **7 000 000**
PRACOWNIKÓW
- NATURALNY
TARGET
DLA COP

FORUM NATOMIAST ZAPEWNIŁBY INSTYTUCJONALNY MECHANIZM KOORDYNACJI I DIALOGU

FORUM DS. WSPÓŁPRACY PUBLICZNO-PRYWATNEJ W OBSZARZE ODPORNOŚCI I BEZPIECZEŃSTWA

Dzisiaj dialog państwo-biznes w obszarze bezpieczeństwa jest rozproszony i ma charakter incydentalny. Forum wypełnia tę lukę, zapewniając regularny mechanizm wymiany informacji, planowania ćwiczeń i opracowywania wspólnych standardów.

W jego skład wchodziłoby przedstawicieli:



Ministerstwo
Obrony Narodowej



Ministerstwo Spraw
Wewnętrznych i Administracji



Ministerstwo
Cyfryzacji

RARS

RCB

oraz reprezentanci sektorów krytycznych:

energetyka

transport

logistyka

teleko-
munikacja

farmacja

finanse

TRZY MECHANIZMY SPINAJĄCE SYSTEM

Zanim przejdziemy do szczegółowych rekomendacji sektorowych, konieczne jest wskazanie trzech ogólnych mechanizmów wdrażających, które nadają ramy całemu systemowi. Chodzi o:

- Fundusz Odporności Państwowej jako centralny instrument finansowania;
- System certyfikacji odporności (COP) jako narzędzie weryfikacji i premiowania zaangażowania firm;
- Forum ds. współpracy publiczno-prywatnej w obszarze odporności i bezpieczeństwa jako stałą platformę koordynacji współpracy między państwem a biznesem.

Proponujemy je jako odrębne rekomendacje, ponieważ przenikają wszystkie obszary szczegółowych rozwiązań opisanych w rekomendacjach od 1 do 6 (R1–R6). Fundusz stanowi odpowiedź na pytanie, skąd mają pochodzić środki na realizację działań; system certyfikacji wyznacza przejrzyste standardy i zasady premiowania przedsiębiorstw; forum natomiast zapewnia instytucjonalny mechanizm koordynacji i dialogu. Wprowadzenie tych trzech narzędzi daje spójność całemu modelowi i pozwala uniknąć rozproszenia działań między różne instytucje i branże.

Dzięki temu wszystkie dalsze rekomendacje sektorowe – od ochrony ludności przez szkolenia i obronę cywilną po modernizację infrastruktury i cyberbezpieczeństwo – mają wspólne ramy finansowe, certyfikacyjne i organizacyjne. To one stanowią fundament, na którym można budować odporność państwa przy aktywnym udziale sektora prywatnego.

I. FUNDUSZ ODPORNOŚCI PAŃSTWOWEJ

Fundusz Odporności Państwowej mógłby rocznie dysponować kwotą 5–7 mld zł, które Polska już dziś wydaje na działania związane z ochroną ludności, modernizacją, cyberbezpieczeństwem i edukacją. Dzięki temu powstanie stabilny, przejrzysty i elastyczny instrument finansowania, który zapewni ramy wdrożenia wszystkich rekomendacji szczegółowych raportu.

Obecnie te środki są rozproszone. W budżecie MON (159 mld zł w 2025 r.) ok. 30–35 mld zł przeznacza się na modernizację techniczną i infrastrukturę. Z tej puli 1–2 mld zł rocznie wydaje się na działania bezpośrednio związane z odpornością państwa – np. infrastrukturę mobilizacyjną czy wspólne ćwiczenia z sektorem prywatnym. W MSWiA roczne wydatki na bezpieczeństwo publiczne i ochronę przeciwpożarową sięgają 15 mld zł, z czego 3–4 mld zł przypada na PSP/OSP i ochronę ludności. Z tego co najmniej 1 mld zł można by było przeznaczyć na moduł ochrony ludności w ramach Funduszu. Rządowa Agencja Rezerw Strategicznych (RARS) dysponuje budżetem rzędu 3–4 mld zł na rezerwy rzeczowe, z czego 0,5–1 mld zł mogłoby zasilić Fundusz – na rezerwy żywnościowe, medyczne i paliwowe. Fundusz Pracy o wartości 16 mld zł rocznie finansuje szkolenia i aktywizację zawodową – 0,5–1 mld zł można byłoby przeznaczyć na szkolenia obronne i działania w ramach PSP. Dodatkowe środki można pozyskać z funduszy unijnych – Polska otrzymuje kilka miliardów złotych rocznie na odporność i cyfryzację w ramach KPO i FEnIKS, a dodatkowo setki milionów złotych z programów Digital Europe, Horizon Europe i CEF Digital. Realnie w ramach Funduszu można by spiąć 2–3 mld zł z tych źródeł. Warto podkreślić, że niezależnie od powyższych strumieni finansowania rządowy Program Ochrony Ludności i Obrony Cywilnej na lata 2025–2026 przewiduje dodatkowe środki – 16,7 mld zł w 2025 r. i 17,2 mld zł w 2026 r. – które mogą stanowić kolejny komponent zasilający Fundusz Odporności Państwowej.

Środki konieczne do zasilenia funduszu są już w systemie, ale rozproszone. Należy je skonsolidować – dzięki temu **powstanie stabilny, przejrzysty i elastyczny instrument finansowania**, który zapewni ramy wdrożenia wszystkich rekomendacji szczegółowych niniejszego raportu.

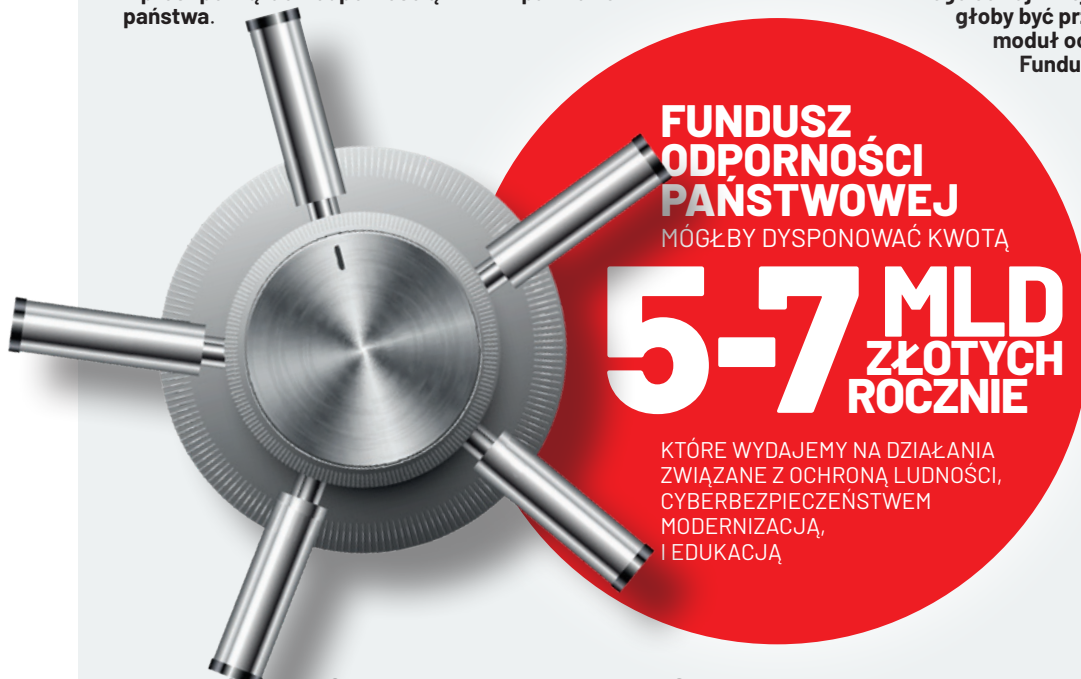
FUNDUSZ ODPORNOŚCI PAŃSTWOWEJ – MOŻLIWE ŹRÓDŁA FINANSOWANIA

DZIŚ ŚRODKI TE SĄ W SYSTEMIE, ALE ROZPROSZONE **NALEŻY JE SKONSOLIDOWAĆ**

W budżecie **MON** około 30–35 mld zł trafia na modernizację techniczną i infrastrukturę. Z tej puli **1–2 mld zł** rocznie wydaje się na działania, które można wprost powiązać z odpornością państwa.

RARS dysponuje budżetem rzędu 3–4 mld zł na rezerwy rzeczowe, a **do Funduszu mogłoby trafić 0,5–1 mld zł** na rezerwy żywnościowe, medyczne i paliwowe.

W **MSWiA** roczne wydatki na bezpieczeństwo publiczne i ochronę przeciwpożarową sięgają 15 mld zł, z czego 3–4 mld zł to PSP/OSP i ochrona ludności. Z tego co najmniej **1 mld zł** mogłoby być przeznaczane na moduł ochrony ludności Funduszu.



FUNDUSZ PRACY o wartości 16 mld zł rocznie finansuje szkolenia i aktywizację zawodową – **0,5–1 mld zł** mogłoby zostać przeznaczone na szkolenia obronne i w ramach PSP.

FUNDUSZE UNIJNE – Polska otrzymuje kilka miliardów zł rocznie na odporność i cyfryzację w ramach KPO i FENIKS, a dodatkowo setki mln zł z programów Digital Europe, Horizon Europe i CEF Digital. **Realnie w ramach Funduszu można by spiąć 2–3 mld zł z tych źródeł.**

FUNDUSZ
MIAŁBY
CZTERY
MODUŁY

ochronę
ludności
1-1,5 mld zł

modernizację
i infrastrukturę
2-3 mld zł

cyber-
bezpieczeństwo
1-1,5 mld zł

edukację
i świadomość
0,5-1 mld zł

Struktura
modułowa pozwala
na elastyczne
zarządzanie środkami

Fundusz powinien zostać umocowany ustawowo – w ustawie o ochronie ludności i obronie cywilnej z odrębnym rozdziałem regulującym jego cele, źródła finansowania i moduły.

W sumie daje to stabilną pulę 5–7 mld zł rocznie, która już dziś jest w systemie, ale wydawana fragmentarycznie i bez spójnej koordynacji. Proponowany Fundusz obejmowałby cztery moduły:

- ochronę ludności (1–1,5 mld zł);
- modernizację i infrastrukturę (2–3 mld zł);
- cyberbezpieczeństwo (1–1,5 mld zł);
- oraz edukację i świadomość (0,5–1 mld zł).

Struktura modułowa pozwala na elastyczne zarządzanie środkami – np. w czasie nasilonych cyberataków można większą część alokować do modułu cyberbezpieczeństwa, a w przypadku katastrof naturalnych – do ochrony ludności.

Fundusz powinien zostać umocowany ustawowo – w ustawie o ochronie ludności i obronie cywilnej – poprzez odrębny rozdział regulujący jego cele, źródła finansowania i strukturę modułową. Rozporządzenia wykonawcze powinny wydać MSWiA (ochrona ludności i edukacja), MON (modernizacja i infrastruktura) oraz Ministerstwo Cyfryzacji (cyberbezpieczeństwo). Dokumenty te powinny być przygotowywane we współpracy międzyresortowej, zapewniającej spójność merytoryczną. Koordynację całości należałoby powierzyć Rządowemu Centrum Bezpieczeństwa, które – jako instytucja podlegająca Prezesowi Rady Ministrów – pełniłoby rolę nadrzędną w zakresie integracji działań, rozwiązywania potencjalnych konfliktów interesów i eliminowania dublujących się rozwiązań.

Wprowadzenie Funduszu rozwiązuje trzy kluczowe problemy: po pierwsze – brak koordynacji rozproszonych środków; po drugie – brak przejrzystości dla biznesu i samorządów, które dziś nie wiedzą, gdzie aplikować o wsparcie; po trzecie – brak elastyczności, bo obecny system budżetowy nie pozwala łatwo przesuwąć środków między różnymi obszarami. Dzięki Funduszowi powstałoby jedno źródło finansowania, stabilne i przewidywalne, z jasnymi regułami. Integracja środków krajowych i unijnych w jednym instrumencie zwiększyłaby ich efektywność i ograniczyła biurokrację. Wreszcie wpisanie Funduszu do ustawy zapewniłoby mu trwałość prawną i polityczną – nie byłby już doraźnym projektem, lecz trwałym elementem systemu bezpieczeństwa państwa.

Fundusz wymaga dodania odrębnego rozdziału w ustawie o ochronie ludności i obronie cywilnej, który określi jego cele, źródła finansowania oraz moduły. Tylko takie rozwiązanie zapewni mu trwałość ustawową i spójność z systemem ochrony ludności.

II. SYSTEM CERTYFIKACJI ODPORNOŚCI (COP)

System certyfikacji odporności (COP) mógłby objąć docelowo kilkadziesiąt tysięcy przedsiębiorstw i miliony pracowników, tworząc jednolite państwowe narzędzie weryfikacji i premiowania zaangażowania biznesu w budowanie bezpieczeństwa i odporności państwa. Dzięki temu powstałby stabilny i przejrzysty mechanizm pozwalający mierzyć wkład firm w budowę odporności, a jednocześnie zapewniający im wymierne korzyści – finansowe, prestiżowe i organizacyjne.

Obecnie nie ma jednolitego systemu oceny. Państwo stosuje rozproszone mechanizmy (np. kryteria w zamówieniach publicznych czy normy ISO w niektórych sektorach), ale brakuje spójnego standardu. Tymczasem potencjał jest ogromny: w Polsce działa ponad 2,3 mln przedsiębiorstw, z czego ok. 50 tys. to firmy średnie i duże, zatrudniające łącznie 7 mln pracowników. To właśnie ta grupa stanowi naturalny target dla COP. Jeśli przyjąć, że już w pierwszej fazie 10% z nich osiągnie poziom podstawowy, to daje

to 700 tys. certyfikowanych pracowników. Przy średnim koszcie szkolenia podstawowego rzędu 500–1000 zł wartość rynku związanego z COP można szacować na 350–700 mln zł rocznie – finansowanych częściowo przez pracodawców, a częściowo z Funduszu Odporności Państwowej.

System COP zakłada trzy poziomy certyfikacji i dodatkowy moduł dotyczący cyberbezpieczeństwa:

1. Poziom podstawowy (Pracodawca Bezpieczeństwa) oznacza wdrożenie minimalnych obowiązków – szkolenia z pierwszej pomocy, ewakuacji, ochrony ppoż. i cyberhigieny dla części pracowników oraz opracowanie planu ciągłości działania.
2. Poziom średni (Pracodawca Wspierający Obronę Cywilną) to aktywne zaangażowanie w Powszechną Służbę Państwową, współpraca z lokalnymi grupami OC, delegowanie części załogi i działania CSR w obszarze bezpieczeństwa.
3. Poziom zaawansowany (Firma Odporna) oznacza pełne wdrożenie systemów ISO 22301, procedur cyberbezpieczeństwa (zgodnych z NIS2 i KSC), tworzenie rezerw, schronów lub zapasów oraz integrację systemów bezpieczeństwa firmy z państwowymi.
4. Moduł cyberbezpieczeństwa przyznawany byłby firmom spełniającym najwyższe wymogi cyfrowe – pełne wdrożenie NIS2, udział w CTI, sektorowy CSIRT.

System certyfikacji musi być umocowany ustawowo, w ustawie o ochronie ludności i obronie cywilnej jako odrębny rozdział o COP. Szczegółowe kryteria i procedury określałoby rozporządzenie MSWiA i RCB w porozumieniu z MON i Ministerstwem Cyfryzacji. System COP musi być także powiązany z Powszechną Służbą Państwową, tak aby certyfikacja pozwalała monitorować i dokumentować realizację obowiązków w PSP.

Każdy poziom COP – podstawowy, średni i zaawansowany – powinien być powiązany z trzema mechanizmami: premiowaniem w zamówieniach publicznych (PZP, art. 242), priorytetowym dostępem do środków Funduszu Odporności Państwowej oraz monitoringiem realizacji obowiązków w ramach Powszechnej Służby Państwowej.

Wprowadzenie COP rozwiązuje trzy kluczowe problemy. Po pierwsze – brak spójnych standardów oceny odporności firm, który dziś sprawia, że wysiłki biznesu nie są ani mierzalne, ani porównywalne. Po drugie – brak motywacji dla przedsiębiorstw, które bez systemu zachęt traktują działania obronne jako koszt, a nie inwestycję. Po trzecie – brak integracji, bo obecnie działania szkoleniowe, inwestycyjne i CSR funkcjonują równolegle, a COP pozwoli je spiąć w jedną strukturę. Dzięki certyfikacji państwo zyska jasne narzędzie oceny i premiowania firm, a przedsiębiorcy realne korzyści: dodatkowe punkty w zamówieniach publicznych (PZP, art. 242), priorytetowy dostęp do Funduszu Odporności Państwowej, preferencje ubezpieczeniowe i kredytowe oraz publiczne wyróżnienie w corocznych raportach o stanie odporności.

Wreszcie, COP gwarantuje zgodność z prawem UE. Mechanizmy premiowania muszą być zgodne z art. 107–108 TFUE, a w razie potrzeby notyfikowane do Komisji Europejskiej. Wpisanie systemu do ustawy daje mu trwałość i stabilność prawną, a zarazem chroni przed zarzutem naruszania zasad konkurencji na rynku.

III. FORUM DS. WSPÓŁPRACY PUBLICZNO-PRYWATNEJ W OBSZARZE ODPORNOŚCI I BEZPIECZEŃSTWA

Forum to trzeci filar horyzontalny, obok Funduszu i COP, który stwarza państwu i biznesowi stałe miejsce współpracy i koordynacji. Dzięki niemu przedstawione poniżej rekomendacje szczegółowe R1-R6 będą miały wspólne zaplecze instytucjonalne, gwarantujące ich wdrożenie w praktyce.

Dziś dialog państwo-biznes w obszarze bezpieczeństwa jest rozproszony i ma charakter incydentalny. Forum wypełnia tę lukę, zapewniając regularny mechanizm wymiany informacji, planowania ćwiczeń i opracowywania wspólnych standardów. W jego skład wchodziłoby przedstawiciele MON, MSWiA, Ministerstwa Cyfryzacji, RARS i RCB oraz reprezentanci sektorów krytycznych: energetyki, transportu, logistyki, telekomunikacji, farmacji czy finansów.

Forum powinno być umocowane ustawowo w ustawie o zarządzaniu kryzysowym (art. 14) jako organ opiniotwórczo-doradczy przy Prezesie Rady Ministrów z obsługą organizacyjną zapewnianą przez Rządowe Centrum Bezpieczeństwa. Do czasu nowelizacji mogłoby funkcjonować na mocy zarządzenia Prezesa Rady Ministrów, ale w długim horyzoncie wymaga trwałego umocowania w ustawie. Spotkania powinny odbywać się regularnie, a raz w roku forum mogłoby publikować raport o stanie współpracy państwo-biznes w obszarze bezpieczeństwa.

Forum pełniłoby także funkcję integracyjną dla dwóch pozostałych mechanizmów horyzontalnych – opinowałoby reguły działania Funduszu Odporności Państwowej oraz kryteria systemu certyfikacji COP. Dzięki temu wszystkie trzy narzędzia byłyby spójne, a działania państwa i biznesu w zakresie budowy odporności miałyby wspólną platformę instytucjonalną.

Spośród trzech mechanizmów horyzontalnych szczególnego podkreślenia wymaga Fundusz Odporności Państwowej. Jego powołanie wymaga zmiany ustawy o ochronie ludności i OC poprzez dodanie odrębnego rozdziału. To w tej ustawie powinny być zapisane cele Funduszu, jego moduły oraz źródła finansowania (MON, MSWiA, RARS, Fundusz Pracy, środki unijne).

REKOMENDACJA NR 1

JEDNOLITY SYSTEM DANYCH OSOBOWYCH NA POTRZEBY BEZPIECZEŃSTWA PAŃSTWA – PERSPEKTYWA SEKTORA PRYWATNEGO

Rządowe rejestry informacji o obywatelach warto rozszerzyć o dane dotyczące kwalifikacji istotnych dla bezpieczeństwa państwa – od ukończonych form usług cywilnych i wojskowych przez dyplomy czy szkolenia specjalistyczne aż po statusy poświadczeń bezpieczeństwa. Taki scentralizowany katalog, inspirowany koncepcją Powszechnej Służby Państwowej (opracowaną przez Instytut Wschodniej Flanki i Instytut Sobieskiego), mógłby znacząco usprawnić zarządzanie rezerwami osobowymi w sytuacjach kryzysowych oraz zwiększyć efektywność wykorzystania zasobów ludzkich państwa.

Wdrożenie eIDAS 2 i Europejskiego Portfela Tożsamości Cyfrowej pozwoliłoby obywatelom na dostęp do swoich danych poprzez aplikację mObywatel, pod warunkiem że system uwzględni rygorystyczne normy ochrony informacji niejawnych, bezpieczeństwa narodowego oraz RODO.

Szybki rozwój współczesnych technologii w zakresie zabezpieczania danych (np. poprzez ich decentralizację na poziomie architektury) oraz ich przetwarzania pozwala nam skuteczniej zarządzać wiedzą, a przez to oszczędzać czas, pieniądze i inne zasoby. Wdrożenie zarysowanej wyżej rekomendacji mogłoby się wiązać z istotnymi korzyściami dla państwa, pracodawców i pracowników w zakresie reagowania kryzysowego, które obejmowałyby m.in.:

- Usprawnienie procesu mobilizacyjnego poprzez komunikowanie pracodawcy podstawowych informacji o obowiązkach mobilizacyjnych pracownika (np. w zakresie podjętej służby wojskowej), potencjalnych kosztach i benefitach z tym związanych.
- Poświadczanie informacji o uzyskanych kwalifikacjach, potencjalnie przydatnych z perspektywy pracodawcy (np. ukończone kursy specjalistyczne, dyplomy ukończenia studiów, innego rodzaju kwalifikacje). Pracodawcy, którzy szkolą u siebie kadry, mogliby (za zgodą pracowników) rejestrować te kompetencje w systemie.
- Moduł umożliwiający transparentne zarządzanie procesem wnioskowania o reklamacje od służby wojskowej, np. w przypadku pracowników utrzymujących ciągłość kluczowych procesów z perspektywy funkcjonowania państwa (np. funkcjonowanie obiektów infrastruktury krytycznej, najważniejszych systemów logistycznych czy szpitali). Choć proces w dalszym ciągu wymagałby decyzji administracyjnej Ministerstwa Obrony Narodowej (wydanej w uregulowanym prawnie terminie), można by go było prowadzić w sposób ułatwiający zarządzanie personalne sektorowi prywatnemu.
- Możliwość szybkiego informowania w czasie sytuacji kryzysowych:
 - pracodawcy, że pracownik zostaje zaangażowany w realizację obowiązków (np. w zakresie służby wojskowej czy obrony cywilnej);
 - pracownika, że został skierowany do wykonywania ww. obowiązków;
 - administracji samorządowej/centralnej/służb specjalistycznych, jaka liczba osób o odpowiednich kwalifikacjach (np. ratowniczych lub do kierowania pojazdami specjalistycznymi) znajduje się na określonym terytorium i jak je można skutecznie skomunikować.

- W razie centralizacji i większego otwarcia systemu rezerw rzeczowych na wypadek kryzysu (w większości gromadzonych obecnie przez Rządową Agencję Rezerw Strategicznych) system mógłby służyć podmiotom sektora prywatnego do wiarygodnego ofertowania wobec strony publicznej (np. wskazywania możliwości utrzymywania rezerw żywnościowych wraz z obsługą dzięki zatrudnieniu osób nieposiadających przydziałów mobilizacyjnych związanych z priorytetowym zaangażowaniem do służby wojskowej).
- Platforma mogłaby także pełnić funkcję kanału komunikacji między państwem a pracodawcami w sytuacjach kryzysowych. Dzięki niej możliwe byłoby szybkie i przejrzyste przekazywanie informacji dotyczących wykorzystania zasobów pozostających w dyspozycji firm – np. pojazdów dostawczych czy innej infrastruktury – które w razie potrzeby mogłyby zostać udostępnione państwu. Takie rozwiązanie sprzyjałoby lepszemu obiegowi informacji i dokumentów oraz pozwalało na bardziej przejrzyste rozliczanie deklaracji wsparcia ze strony biznesu. Aktywne uczestnictwo przedsiębiorstw w tym procesie mogłoby być odzwierciedlone w systemie certyfikacji odporności (COP), który – zgodnie z naszymi propozycjami – znajduje przełożenie na zamówienia publiczne (art. 242 PZP). Dzięki temu wsparcie udzielane przez firmy byłoby nie tylko widoczne dla państwa, ale również premiowane w praktyce rynkowej.

PRZYKŁADOWY INSTRUMENT WDRAŻAJĄCY:

UTWORZENIE FORUM WSPÓŁPRACY PUBLICZNO-PRYWATNEJ W OBSZARZE ODPORNOŚCI ORAZ CENTRALNEGO REJESTRU KWALIFIKACJI ODPORNOŚCIOWYCH

Realizacja tej rekomendacji wymaga wydania aktu wykonawczego (rozporządzenia Rady Ministrów lub MSWiA). Akt ten ustanowi zarówno ramy organizacyjne, jak i techniczne planowanego systemu. Rozporządzenie powinno *explicite* rozszerzać istniejące przepisy wynikające z ustawy o obronie Ojczyzny (art. 11 ust. 2 pkt 11) oraz ustawy o ochronie ludności i obronie cywilnej (art. 14). Wspomniane przepisy nakładają obecnie obowiązek prowadzenia ewidencji wojskowej oraz rejestrów personelu obrony cywilnej na organy administracji publicznej, co stanowi podstawę prawną do rozbudowy systemu.

Na mocy takiego rozporządzenia powołane zostałoby forum ds. współpracy publiczno-prywatnej w obszarze odporności i bezpieczeństwa. W skład forum weszliby przedstawiciele kluczowych resortów (MON, MSWiA, Ministerstwa Cyfryzacji, Rządowego Centrum Bezpieczeństwa) oraz reprezentanci głównych sektorów gospodarki (energetyki, transportu, telekomunikacji, logistyki). Forum pełniłoby funkcję stałej platformy wymiany informacji i doświadczeń oraz wspólnego wypracowywania standardów bezpieczeństwa dla przedsiębiorstw. Dodatkowo odpowiadałoby za organizację corocznych ćwiczeń łączących administrację publiczną i biznes, które pozwoliłyby lepiej zgrywać współpracę na wypadek sytuacji kryzysowych.

Wpisanie tej instytucji w ramy Powszechnej Służby Państwowej (PSP) pozwoliłoby wykorzystać PSP jako systemową podstawę prawną i organizacyjną. Przewiduje ona bowiem obowiązkową, ale elastyczną służbę dla obywateli, której częścią jest zarówno kwalifikacja wojskowa, jak i budowanie rezerw kadrowych dla obrony cywilnej i ochrony ludności. Centralny Rejestr Kwalifikacji Obronnych, będący kluczowym elementem PSP, mógłby zostać poszerzony o dane i kwalifikacje gromadzone w ramach forum, zapewniając spójność systemu oraz integrację wysiłku państwa, obywateli i biznesu. Dzięki temu forum i rejestr nie byłyby nową instytucją, oderwaną od istniejących koncepcji, lecz praktycznym narzędziem realizacji założeń PSP i wzmacniania kultury odporności państwa.

Drugim filarem rozporządzenia byłoby ustanowienie Centralnego Rejestru Kwalifikacji Obronnych jako elementu platformy teleinformatycznej zarządzanej przez Ministerstwo Cyfryzacji we współpracy z RCB. Rejestr ten integrowałby już istniejące bazy danych (ewidencja wojskowa, rejestry personelu OC, bazy Ochotniczej

Straży Pożarnej) i rozszerzał je o informacje o cywilnych kwalifikacjach przydatnych w sytuacjach kryzysowych. Do rejestru trafiałyby m.in. dane o ukończonych kursach pierwszej pomocy, szkoleniach z cyberbezpieczeństwa czy posiadanych uprawnieniach technicznych istotnych z punktu widzenia obronności.

Aby rozwiązanie miało charakter systemowy, należy przewidzieć nowelizację ustawy o obronie Ojczyzny (Dział VI – rejestracja i kwalifikacja wojskowa) w kierunku dodania przepisu umożliwiającego wpisywanie do ewidencji także kwalifikacji cywilnych istotnych dla bezpieczeństwa państwa. Analogicznie, ustawa o ochronie ludności i obronie cywilnej powinna otrzymać nowy artykuł w rozdziale dotyczącym zadań administracji, który ustanowi Centralny Rejestr Kwalifikacji Obronnych jako narzędzie ochrony ludności.

Dostęp obywateli do rejestru powinien być zapewniony poprzez aplikację mObywatel, a docelowo także Europejski Portfel Tożsamości Cyfrowej (eIDAS 2). Wdrożenie takiej integracji wymaga wydania rozporządzenia Ministra Cyfryzacji określającego zakres danych udostępnianych przez system i zasady ich uwierzytelniania.

Kluczowe jest zapewnienie pełnej zgodności tworzonego systemu z RODO. Zakres danych gromadzonych w rejestrze należy ograniczyć do niezbędnego minimum, a ich przetwarzanie oprzeć na podstawie obowiązku prawnego (art. 6 ust. 1 lit. c/e RODO) oraz ważnego interesu publicznego w dziedzinie obronności (art. 9 ust. 2 lit. g RODO). Rozporządzenie powinno także wskazywać organy odpowiedzialne za bieżące wprowadzanie i aktualizację danych (np. wojskowe centra rekrutacji, komendy Państwowej Straży Pożarnej, akredytowane firmy szkoleniowe) oraz określać tryb dostępu do rejestru dla poszczególnych uprawnionych instytucji.

REKOMENDACJA NR 2

UTWORZENIE CENTRALNEGO SYSTEMU SZKOLENIOWEGO

Rekomendujemy utworzenie centralnego serwisu szkoleniowego w zakresie bezpieczeństwa. Bazą serwisu byłaby platforma szkoleniowa, obejmująca możliwość nauki podstawowych zagadnień bezpieczeństwa, zorganizowana wokół zaawansowanego serwisu e-learningowego wyposażonego w moduły gamifikacji i adaptacyjnego uczenia się. Platforma powinna stanowić zintegrowany system zarządzania nauczaniem. Drugą istotną jej funkcjonalnością byłby serwis informacyjny, gdzie publikowane byłyby programy, harmonogramy, certyfikowane kursy online oraz lista akredytowanych podmiotów szkolących. Serwis ułatwiłby koordynację szkoleń w skali kraju i zwiększył przejrzystość systemu, co jest istotne z perspektywy prywatnych firm szkoleniowych chcących włączyć się w realizację zadań z zakresu ochrony ludności. Ponadto część aktywności szkoleniowych mogłaby być wprowadzona wspólnie z regularną działalnością ćwiczeniową służb mundurowych – na podobnych zasadach jak obecnie angażowane są wybrane organizacje pozarządowe czy firmy zbrojeniowe.

Serwis mógłby również ułatwić sprawne wdrożenie Powszechnej Służby Państwowej dzięki realizacji części szkoleń przez uprawnione podmioty szkoleniowe (np. w zakresie ochrony przeciwpożarowej).

System powinien nagradzać podmioty sektora prywatnego szczególnie zaangażowane w działania na rzecz bezpieczeństwa państwa, np. poprzez szkolenie wyjątkowo dużej liczby pracowników oraz gotowość do znaczących świadczeń osobowych czy rzeczowych w razie kryzysu. Potencjalne wsparcie dla ww. pracodawców mogłoby obejmować m.in. dodatkową punktację w systemie zamówień publicznych, ułatwienia (np. przyspieszony tryb realizacji) w zakresie inwestycji związanych z bezpieczeństwem państwa (np. budowa nowego zakładu produkcyjnego dostarczającego produkty istotne dla funkcjonowania

służb mundurowych) czy ekskluzywny katalog szkoleń dla podmiotów ze szczególnie wrażliwych branż (np. w zakresie cyberbezpieczeństwa).

- Należy stworzyć **ramowy program szkoleń** z zakresu bezpieczeństwa (pierwsza pomoc, ochrona przeciwpożarowa, elementy samoobrony, podstawowe wyszkolenie strzeleckie) dostępny dla pracowników cywilnych za pośrednictwem pracodawców. Państwo (np. poprzez Rządowe Centrum Bezpieczeństwa, MON czy MSWiA) mogłoby certyfikować te szkolenia i współfinansować je, szczególnie dla sektorów uznanych za kluczowe.
- Pracodawca deklarujący ponadnormatywną i udokumentowaną gotowość do wsparcia reagowania kryzysowego – np. poprzez organizację szkoleń dla większej liczby pracowników lub udostępnienie własnej infrastruktury na rzecz szkoleń w ramach PSP – powinien uzyskiwać dodatkowe punkty w systemie certyfikacji odporności (COP). Certyfikat ten, zgodnie z naszymi propozycjami, znajduje przełożenie na zamówienia publiczne (art. 242 PZP), co pozwala premiować firmy szczególnie zaangażowane w działania proobronne w sposób przejrzysty i zgodny z prawem. Dzięki temu mechanizm zachęt nie ma charakteru uznaniowego, lecz jest częścią jednolitego systemu łączącego COP, Fundusz Odporności Państwowej i Powszechną Służbę Państwową.
- Siły Zbrojne RP i inne służby mundurowe mogłyby rozbudować działalność szkoleniową o ćwiczenia związane z ochroną obiektów szczególnie ważnych z punktu widzenia interesu państwa (np. obiektów infrastruktury krytycznej). Przedsiębiorcy byłiby zobowiązani do czynnego uczestnictwa w wymienionych działaniach, przez co mogliby uzyskiwać szereg korzyści związanych ze zmniejszeniem ryzyka operacyjnego, np. poprzez płynną integrację swoich systemów bezpieczeństwa z wojskowymi (np. zmniejszając ryzyko skutecznego rażenia danego obiektu w razie konfliktu zbrojnego).
- Pracownicy, którzy ukończą pełen cykl szkoleń, mogliby otrzymywać oficjalne certyfikaty kompetencji obronnych (serwis byłby zintegrowany z aplikacją mObywatel w zakresie weryfikacji tożsamości i przechowywania certyfikatów – zgodnie z rekomendacją nr 1), co z jednej strony zwiększyłoby ich wartość na rynku pracy (przenoszalne kwalifikacje z zakresu bezpieczeństwa), a z drugiej zasilaloby bazę danych osób przeszkolonych na potrzeby obrony kraju. Taki program pozwoliłby zwiększyć liczbę osób przygotowanych do reagowania w sytuacjach kryzysowych, a jednocześnie odpowiadałby na realne zapotrzebowanie społeczne (ponad 83% pracowników wyraziło chęć uczestnictwa w szkoleniach w zakładzie pracy). Ważne jest, aby szkolenia te odbywały się w czasie pracy lub z dofinansowaniem pracodawcy, co wymaga wprowadzenia zachęt finansowych ze strony państwa dla firm angażujących się w takie działania. Można też rozważyć wprowadzenie certyfikatu „Pracodawca Bezpieczeństwa”, przyznawanego przedsiębiorstwom prowadzącym regularne treningi obronne. Certyfikat taki, potwierdzany przez instytucje państwowe, podnosiłby prestiż firmy i wzmacniał jej pozytywny wizerunek (analogicznie do certyfikatów typu „Investors in People” czy „Firma Przyjazna Wojsku”).

PRZYKŁADOWY INSTRUMENT WDRAŻAJĄCY:

UTWORZENIE CENTRALNEGO SYSTEMU SZKOLENIOWEGO DS. ODPORNOŚCI PAŃSTWA

Realizacja rekomendacji nr 2 wymaga ujęcia centralnego systemu szkoleniowego w obowiązującym porządku prawnym. Podstawę stanowią m.in. Ustawa z 11 marca 2022 r. o obronie Ojczyzny (Dz.U. 2022 poz. 655), której art. 11 ust. 2 pkt 11 akcentuje kompleksowe podejście do obowiązku obrony państwa, oraz Ustawa z 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907), która nakłada na administrację obowiązek przygotowania społeczeństwa na sytuacje kryzysowe poprzez ćwiczenia i edukację ochronną. Najbardziej właściwym rozwiązaniem byłoby dodanie odrębnego rozdziału do ustawy o ochronie

ludności i obronie cywilnej, określającego centralny charakter systemu szkoleniowego, powierzającego koordynację Rządowemu Centrum Bezpieczeństwa we współpracy z MON, MSWiA i Ministerstwem Cyfryzacji, a także definiującego prawa i obowiązki pracodawców, akredytowanych podmiotów szkoleniowych i instytucji publicznych.

Na podstawie delegacji ustawowej powinno zostać wydane rozporządzenie Rady Ministrów lub MSWiA, które doprecyzuje minimalny zakres programów szkoleniowych, obejmujących m.in. pierwszą pomoc, ochronę przeciwpożarową, podstawowe szkolenie strzeleckie, samoobronę czy elementy cyberbezpieczeństwa. Rozporządzenie powinno również określać tryb akredytacji i certyfikacji podmiotów szkolących, zasady raportowania aktywności szkoleniowej oraz mechanizmy premiowania przedsiębiorstw szczególnie zaangażowanych w działania na rzecz bezpieczeństwa państwa.

W systemie certyfikacji odporności (COP) szkolące się przedsiębiorstwa mogłyby uzyskać COP – poziom podstawowy („Pracodawca Bezpieczeństwa”), potwierdzający prowadzenie regularnych szkoleń i posiadanie minimalnych planów bezpieczeństwa. Certyfikat ten mógłby być premiowany w zamówieniach publicznych (art. 242 PZP) oraz w ramach programów grantowych.

Centralnym elementem instrumentu byłoby powołanie Centralnej Platformy Szkoleniowej ds. Bezpieczeństwa, zarządzanej przez Rządowe Centrum Bezpieczeństwa przy wsparciu MON i Ministerstwa Cyfryzacji. Platforma ta integrowałaby serwis e-learningowy z modułami adaptacyjnymi i gamifikacyjnymi, publiczny serwis informacyjny zawierający listę akredytowanych podmiotów i harmonogramy kursów, a także cyfrowy rejestr kompetencji obywateli powiązany z aplikacją mObywatel i Europejskim Portfelem Tożsamości Cyfrowej (eIDAS 2). Rozwiązanie to zapewniłoby obywatelom szybki dostęp do certyfikatów kwalifikacji, ułatwiło monitorowanie stopnia przeszkolenia populacji i stworzyło spójne ramy dla wdrożenia Powszechnej Służby Państwowej.

Finansowanie systemu powinno opierać się na istniejących instrumentach, takich jak: Fundusz Pracy, który może finansować szkolenia pracowników; środki Unii Europejskiej przeznaczone na rozwój kompetencji i odporności (np. programy PARP, PFR, NCBR, KPO); a także programy budżetowe w ramach MON i MSWiA, które już dziś obejmują modernizację służb, ochronę przeciwpożarową czy działania RCB w zakresie edukacji i kampanii informacyjnych. Część środków mogłaby również pochodzić z rezerw zarządzanych przez Rządową Agencję Rezerw Strategicznych oraz z budżetów samorządowych, które mają ustawowe obowiązki w obszarze ochrony ludności. Takie rozwiązanie pozwoliłoby na koordynację już istniejących strumieni finansowania w ramach modułu „szkolenia” Funduszu Odporności Państwowej bez potrzeby tworzenia nowych ulg podatkowych, co zminimalizowałoby ryzyka prawne i fiskalne. Wdrożenie certyfikacji bezpieczeństwa w zamówieniach publicznych wymagać będzie jednak starannego zaprojektowania, aby uniknąć zarzutów naruszenia zasad konkurencji określonych w art. 107–108 TFUE. Jeśli mechanizm zostanie uznany za pomoc publiczną, konieczna może być jego notyfikacja do Komisji Europejskiej lub wykorzystanie dopuszczalnych wyłączeń (np. pomoc na szkolenia).

System szkoleniowy powinien także w pełni respektować przepisy o ochronie danych osobowych oraz standardy cyberbezpieczeństwa określone w unijnym Cybersecurity Act. Zakres gromadzonych danych musi być ograniczony do niezbędnego minimum, a ich przetwarzanie uzasadnione obowiązkiem prawnym oraz ważnym interesem publicznym w obszarze obronności.

REKOMENDACJA NR 3

ROZSZERZENIE MOŻLIWOŚCI ŚCIEŻKI OBRONY CYWILNEJ I OCHRONY LUDNOŚCI W RAMACH PSP

Postulujemy wprowadzenie nowelizacji przepisów (np. w ustawie o ochronie ludności i obronie cywilnej), tak aby umożliwić formowanie grup obrony cywilnej i ochrony ludności spośród osób kończących wskazaną ścieżkę w ramach Powszechnej Służby Państwowej lub chcących wolontariacko dołączyć do formacji ochrony ludności. Mogłyby one w sytuacjach kryzysowych współdziałać z Policją, Ochotniczą i Powszechną Strażą Pożarną czy Wojskami Obrony Terytorialnej.

Członkowie takich grup otrzymywaliby dodatkowe szkolenie i wyposażenie przy wsparciu państwa i samorządów. Należy przewidzieć dodatkowy mechanizm finansowania z Funduszu Ochrony Ludności – np. dotacje dla samorządów na organizację szkoleń tych grup, możliwość pozyskania sponsorów wśród lokalnego biznesu, a także ubezpieczenie członków na wypadek udziału w akcjach.

Taka kategoria przydziału mobilizacyjnego częściowo zmniejszy obawy pracodawców przed szkoleniem (zgodnie z wynikami ankiety 57,5% firm chętnie przyjąłoby rozwiązania umożliwiające pozostawianie pracownika w bliskości miejsca pracy). Dzięki otwarciu na wolontariuszy będzie ona szansą na włączenie do wysiłków na rzecz bezpieczeństwa starszych pracowników, których nie obejmie PSP. Wsparciem prawnym dla tej idei mógłby być zapis w ustawie, że czas poświęcony na szkolenia i służbę w grupach samoobrony jest usprawiedliwioną nieobecnością w pracy, analogicznie do zasad dotyczących ćwiczeń rezerwistów czy OSP, co wymaga ewentualnego dostosowania Kodeksu pracy.

Jednocześnie, w celu priorytetyzacji służby wojskowej jako podstawowej ścieżki w ramach PSP (przedstawiającej również największe potrzeby kadrowe wynikające z dynamicznej rozbudowy Sił Zbrojnych RP), zachęty do uczestnictwa w szkoleniu wojskowym powinny się wiązać z dodatkową premią dla pracodawcy.

PRZYKŁADOWY INSTRUMENT WDRAŻAJĄCY:

ROZSZERZENIE ŚCIEŻKI OBRONY CYWILNEJ I OCHRONY LUDNOŚCI W RAMACH PSP

Realizacja rekomendacji nr 3 wymaga przede wszystkim nowelizacji Ustawy z 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907). Ustawa powinna wprowadzić wyraźną podstawę prawną do tworzenia lokalnych grup obrony cywilnej i ochrony ludności, w których skład wchodziłoby absolwenci ścieżki cywilnej Powszechnej Służby Państwowej oraz lokalni ochotnicy. Grupy te, działając pod auspicjami samorządu i we współpracy z Policją, Państwową i Ochotniczą Strażą Pożarną oraz Wojskami Obrony Terytorialnej realizowałyby zadania ochronne i ratownicze w sytuacjach kryzysowych – takie jak: ewakuacja ludności, zabezpieczenie mienia, pomoc logistyczna czy utrzymanie porządku publicznego.

Instrument finansowo-organizacyjny dla nowych formacji powinien wykorzystywać istniejące mechanizmy. Środki na szkolenia, podstawowe wyposażenie oraz ubezpieczenie członków mogłyby pochodzić z budżetu MSWiA (dział 754 – bezpieczeństwo publiczne i ochrona przeciwpożarowa), z dotacji celowych dla samorządów, które już dziś mają obowiązki w obszarze obrony cywilnej, oraz z rezerw zarządzanych przez Rządową Agencję Rezerw Strategicznych. Część finansowania mogłaby zostać zapewniona ze środków unijnych (np. KPO, FEnKS, fundusze UE na odporność społeczną). Wszystkie te źródła powinny zostać skoordynowane w ramach modułu „ochrona ludności” Funduszu Odporności Państwowej.

Wprowadzenie nowych form zaangażowania obywateli w obronę cywilną wymaga także zmian w Kodeksie pracy i ustawie o służbie wojskowej, które nadadzą temu rozwiązaniu realny charakter. Do rozważenia jest w szczególności: dodanie w art. 92 Kodeksu pracy nowego ust. 3, przewidującego, że pracownikowi powołanemu do udziału w ćwiczeniach w ramach Powszechnej Służby Państwowej w ścieżce obrony cywilnej przysługuje prawo do urlopu szkoleniowego, za który wynagrodzenie wypłaca pracodawca, a koszty są refundowane z budżetu państwa; rozszerzenie katalogu usprawiedliwionych nieobecności w pracy (art. 177 Kodeksu pracy) o czas przeznaczony na służbę w certyfikowanych grupach obrony cywilnej, analogicznie do zasad stosowanych wobec ochotników OSP i rezerwistów; a także wprowadzenie do ustawy o służbie wojskowej przepisu gwarantującego ochronę stosunku pracy pracownika pełniącego służbę w ramach grup ochrony ludności, tak aby pracodawca nie mógł wypowiedzieć ani rozwiązać umowy w czasie jej trwania.

Ponadto w celu zwiększenia akceptacji pracodawców należy wprowadzić nową kategorię przydziału mobilizacyjnego – „lokalna obrona cywilna”. Przydział ten umożliwiłby formalne utrzymanie przeszkolonych pracowników w gminie lub powiecie zamieszkania lub pracy na potrzeby obrony ludności w sytuacji kryzysowej, zamiast ich automatycznego wcielania do regularnych jednostek wojskowych. Aby rozwiązanie to miało moc prawną, konieczne są zmiany w kilku aktach:

- w ustawie o obronie Ojczyzny (art. 58) – dodanie przydziału mobilizacyjnego „lokalna obrona cywilna”;
- w ustawie o ochronie ludności i obronie cywilnej – dopisanie, że osoby z takim przydziałem realizują zadania OC w miejscu zamieszkania/pracy w ramach grup organizowanych przez samorządy i nadzorowanych przez Policję, PSP i WOT;
- w Kodeksie pracy – rozszerzenie art. 92 i 177 o urlop szkoleniowy i usprawiedliwione nieobecności dla osób z przydziałem;
- w ustawie o służbie wojskowej – dodanie przepisu gwarantującego ochronę stosunku pracy dla osób pełniących obowiązki w ramach przydziału „lokalna obrona cywilna”.

Ostateczna decyzja w sprawie miejsca mobilizacyjnego zawsze należałaby do Ministerstwa Obrony Narodowej. MON zachowywałby pełną kompetencję do określania, czy dana osoba powinna zostać powołana do służby wojskowej w jednostkach liniowych, czy też utrzymana w miejscu zamieszkania i przypisana do „lokalnej obrony cywilnej”. Takie rozwiązanie daje gwarancję, że system nie będzie ograniczać zdolności mobilizacyjnych armii, a jednocześnie pozwala na efektywne wykorzystanie części zasobów kadrowych w działaniach ochrony ludności.

Przedsiębiorcy angażujący się w tę ścieżkę mogliby uzyskać COP – poziom średni („Pracodawca Wspierający Obronę Cywilną”), potwierdzający aktywny udział w PSP i wsparcie lokalnych grup OC. Certyfikat taki mógłby się wiązać z określonymi preferencjami – w tym dodatkowymi punktami w zamówieniach publicznych. Jednocześnie, aby nie osłabiać priorytetu ścieżki wojskowej, pracodawcy wspierający szkolenie pracowników w ramach PSP w formie wojskowej powinni korzystać z dodatkowej premii.

REKOMENDACJA NR 4

PREMIOWANIE PRZEDSIĘBIORCÓW WZMACNIAJĄCYCH ODPORNOŚĆ PAŃSTWA, SPOŁECZEŃSTWA I WŁASNYCH BIZNESÓW

W celu stymulowania oddolnego wzmocnienia odporności przedsiębiorstw i społeczności lokalnej warto stworzyć katalog zachęt dla podmiotów, które podejmują określone wysiłki na rzecz bezpieczeństwa. Mógłby on obejmować następujące rozwiązania:

- Na poziomie regionalnym należy wzmocnić wojewódzkie zespoły zarządzania kryzysowego z udziałem przedstawicieli lokalnego biznesu, np. duże firmy przemysłowe mogłyby delegować swoich pracowników do współpracy z centrami zarządzania kryzysowego. Tego typu fora mogłyby również służyć kooperacji przy wspólnej działalności ćwiczeniowej, opracowywaniu okresowych celów w zakresie szkolenia pracowników czy konsultacji nowych rozwiązań prawnych.
- Państwo powinno zawczasu zawierać umowy lub porozumienia z firmami transportowymi, spożywczymi, farmaceutycznymi itd., aby zabezpieczyć łańcuchy dostaw w sytuacji kryzysowej. Może to przybrać formę dobrowolnych porozumień (jak fińskie pule bezpieczeństwa dostaw) lub bardziej zobowiązujących umów ramowych z klauzulami uruchamianymi w sytuacji wyjątkowej. W polskich realiach sensowne byłoby np. zaangażowanie spółek energetycznych i paliwowych (także prywatnych dystrybutorów) we wspólne planowanie dystrybucji paliw na wypadek niedoborów albo współpraca z sieciami handlowymi w zakresie zapewnienia żywności dla ewakuowanej ludności.
- Firmy budujące schrony, ukrycia lub wzmacniające infrastrukturę w swoich obiektach (ponad wymogi prawa) mogłyby liczyć na skróconą ścieżkę inwestycyjną, dodatkową punktację w systemie zamówień publicznych czy dostęp do ekskluzywnego katalogu szkoleń. Szczególne regulacje w tym zakresie powinny dotyczyć deweloperów, którzy odgrywają zasadniczą rolę w kształtowaniu zabudowy miejskiej i mogą się istotnie przyczynić do wzrostu dostępności schronów dla mieszkańców miast. Potencjalne zmiany w prawie budowlanym mogłyby nałożyć na ww. firmy obowiązki w zakresie lokowania schronów w nowych inwestycjach (np. w ramach budowy garaży podziemnych) czy instalowania nowych środków komunikacyjnych w ramach Krajowego Systemu Ostrzegania i Alarmowania przy jednoczesnej możliwości dofinansowania tego typu działań ze środków budżetu państwa przeznaczonych na ochronę ludności.
- Warto rozważyć preferencje przy zamówieniach publicznych dla przedsiębiorstw, które uzyskają certyfikat „Firma Odporna” lub podobny (np. posiadają systemy awaryjnego zasilania, zapasy, plany ciągłości działania i przeszkolony personel). Taki mechanizm rynkowy spowoduje, że bezpieczeństwo stanie się elementem konkurencyjności – firmy będą konkurować w pozytywny sposób: kto lepiej zabezpieczony i przygotowany, ten bardziej wiarygodny dla kontrahentów (zwłaszcza jeśli kontrahentem jest instytucja publiczna).
- Rząd mógłby ustanowić formalne forum współpracy z kluczowymi przedsiębiorstwami prywatnymi z sektorów infrastruktury krytycznej (energia, telekomunikacja, transport, finanse, żywność itp.). O ile istnieją już sektorowe zespoły ds. cyberbezpieczeństwa czy centra reagowania (CERT), postulujemy ich rozszerzenie o aspekt szerszej obrony i odporności. Forum, takie jak np. Rada ds. Odporności Gospodarczej przy ministrze spraw wewnętrznych lub przy RCB, gromadziłoby przedstawicieli największych operatorów prywatnych oraz agend rządowych w celu regularnej wymiany informacji i koordynacji planów awaryjnych.

**PRZYKŁADOWY INSTRUMENT WDRAŻAJĄCY:
PREMIOWANIE PRZEDSIĘBIORCÓW WZMACNIAJĄCYCH ODPORNOŚĆ PAŃSTWA,
SPOŁECZEŃSTWA I BIZNESU**

Realizacja rekomendacji nr 4 wymaga stworzenia kompleksowego pakietu legislacyjno-organizacyjnego, który pozwoli premiować przedsiębiorców podejmujących działania wzmacniające odporność państwa, społeczeństwa i własnych organizacji. Kluczowe znaczenie mają tu nowelizacje ustawy o zarządzaniu kryzysowym, ustawy o ochronie ludności i obronie cywilnej, Prawa budowlanego oraz ustawy Prawo zamówień publicznych.

W obecnym stanie prawnym wojewódzkie zespoły zarządzania kryzysowego (WZZK) działają na podstawie art. 14 ustawy o zarządzaniu kryzysowym i skupiają przedstawicieli administracji rządowej, samorządowej oraz służb, inspekcji i straży. Ustawa przewiduje możliwość zapraszania innych osób, ale nie daje przedsiębiorcom statusu stałych uczestników. Nowelizacja art. 14 powinna więc wprost wskazywać, że wojewoda może powoływać przedstawicieli sektora prywatnego – w szczególności operatorów infrastruktury krytycznej – jako ekspertów w składzie zespołu. Dałoby to biznesowi formalny status uczestnika planowania kryzysowego.

Równocześnie Krajowy Plan Zarządzania Kryzysowego (KPZK), regulowany w art. 5 ustawy o zarządzaniu kryzysowym, powinien zostać przekształcony w dokument o konstrukcji modularnej. Do KPZK wprowadzono by załączniki sektorowe, opracowywane we współpracy z przedsiębiorcami, obejmujące m.in. procedury zabezpieczenia dostaw w energetyce, transporcie czy farmacji. Takie rozwiązanie zapewniłoby większą szczegółowość i operacyjność planów, a równocześnie umożliwiłoby ich częściowe utajnienie (klauzulowanie), by chronić dane wrażliwe.

W ustawie o ochronie ludności i obronie cywilnej konieczne jest doprecyzowanie roli sektora prywatnego. W rozdziale II (określającym zadania i obowiązki podmiotów) powinny się znaleźć zapisy gwarantujące przedsiębiorcom realny czas dostosowania się do nowych obowiązków technicznych – poprzez wydłużenie *vacatio legis* do co najmniej sześciu miesięcy. Ustawa powinna także zostać uzupełniona o jasne definicje pojęć, takich jak „obiekt ochronny” czy „ukrycie doraźne”, aby uniknąć niejasności interpretacyjnych. Ponadto w art. 14–15 można dodać obowiązek konsultacji z reprezentantami przedsiębiorców przy opracowywaniu lokalnych planów obrony cywilnej i ochrony ludności, w tym planów ewakuacji i zaopatrzenia.

W obszarze prawa budowlanego istotne znaczenie ma uchwalona w 2025 r. tzw. ustawa schronowa, która od 2026 r. nakłada na deweloperów obowiązek budowy schronów lub miejsc doraźnego ukrycia w podziemiach nowych budynków mieszkalnych i obiektów użyteczności publicznej. Nowelizacja Prawa budowlanego powinna stopniowo rozszerzać ten obowiązek także na duże obiekty przemysłowe i biurowe. W art. 5–7 Prawa budowlanego można wskazać, że inwestorzy realizujący takie zabezpieczenia mają prawo do uproszczonych procedur administracyjnych (specjalny tryb pozwolenia na budowę) oraz współfinansowania ze środków publicznych przeznaczonych na ochronę ludności.

W ustawie Prawo zamówień publicznych należy doprecyzować art. 242, wprowadzając możliwość stosowania kryteriów odporności. Na najwyższym poziomie certyfikacji odporności przedsiębiorstwa mogłyby uzyskać COP – poziom zaawansowany („Firma Odporna”), obejmujący spełnienie standardów ISO 22301, norm cyberbezpieczeństwa, posiadanie zapasów i schronów, udział w ćwiczeniach państwowych oraz aktywną współpracę z RCB. Wprowadzenie takiego mechanizmu – obok istniejących już kryteriów społecznych i środowiskowych – uczyni bezpieczeństwo istotnym elementem konkurencji w zamówieniach publicznych, zniżek ubezpieczeniowych czy poprawy reputacji. W perspektywie kilku lat posiadanie certyfikatu mogłoby

stać się obowiązkowe dla operatorów infrastruktury krytycznej, zgodnie z kierunkiem wyznaczonym przez unijną dyrektywę CER dotyczącą odporności podmiotów kluczowych.

W ramach forum ds. współpracy publiczno-prywatnej w obszarze bezpieczeństwa powinna funkcjonować sektorowa Rada ds. Odporności Gospodarczej, skupiająca przedstawicieli administracji i kluczowych przedsiębiorstw. Jej zadaniem byłoby opiniowanie planów awaryjnych w gospodarce, zawieranie porozumień ramowych w sprawie łańcuchów dostaw oraz organizacja ćwiczeń gospodarczych.

REKOMENDACJA NR 5

UDZIAŁ SEKTORA PRYWATNEGO W BUDOWANIU ŚWIADOMOŚCI SPOŁECZNEJ

Budowanie odporności społecznej wymaga też zmiany świadomości. Rząd wraz z organizacjami przedsiębiorców powinien prowadzić kampanie informujące o roli każdego podmiotu w systemie bezpieczeństwa, który promowałby dobre praktyki: np. posiadanie AED w każdej firmie, przeszkolenie min. 25% załogi z pierwszej pomocy, opracowanie planu ewakuacji i funkcjonowania firmy w razie wojny (coś w rodzaju biznesowego planu ciągłości działania rozszerzonego o aspekty obronne). Program mógłby być wsparty przez instytucje rozwoju jako element społecznej odpowiedzialności biznesu (CSR). Publiczne pokazywanie przykładów firm, które **aktywnie wnoszą wkład w bezpieczeństwo** (poprzez szkolenia, udział w ćwiczeniach obrony cywilnej, sponsorowanie lokalnych jednostek OSP czy grup samoobrony) zachęci innych do naśladowania. W ten sposób buduje się kulturę odporności – podobnie jak w Finlandii, gdzie wszyscy rozumieją, że „bezpieczeństwo to sprawa wspólna”. Państwo powinno też udostępnić firmom eksperckie materiały i poradniki (np. jak przygotować zakład pracy na sytuację kryzysową, jak zabezpieczyć cyfrowe dane firmy przed cyberatakami – tu można korzystać z istniejących inicjatyw jak Disinfo Radar czy certyfikacje ISO). Synergia edukacyjna między sektorem publicznym a prywatnym wzmocni społeczną świadomość zagrożeń hybrydowych (np. kampanie przeciw dezinformacji w intranetach firmowych, treningi reagowania na incydenty dla personelu ochrony w przedsiębiorstwach itd.).

PRZYKŁADOWY INSTRUMENT WDRAŻAJĄCY:

UDZIAŁ SEKTORA PRYWATNEGO W BUDOWANIU ŚWIADOMOŚCI SPOŁECZNEJ

Realizacja rekomendacji nr 5 wymaga wprowadzenia zmian legislacyjnych i organizacyjnych, które nadadzą edukacji i budowaniu świadomości społecznej charakter systemowy. Najbardziej właściwe jest uzupełnienie ustawy o zarządzaniu kryzysowym o przepisy nakładające na Rządowe Centrum Bezpieczeństwa, we współpracy z MSWiA oraz organizacjami pracodawców, obowiązek prowadzenia regularnych kampanii informacyjnych. Najlepszym miejscem do wpisania takiego obowiązku jest art. 14 ustawy o zarządzaniu kryzysowym, który reguluje zadania wojewódzkich zespołów zarządzania kryzysowego. Warto dodać nowy ustęp, w którym znalazłby się zapis, że RCB prowadzi co najmniej raz w roku ogólnokrajową kampanię informacyjną z udziałem organizacji pracodawców, promującą dobre praktyki w zakresie bezpieczeństwa i odporności.

Kampanie te powinny być finansowane w ramach modułu „edukacja i świadomość” Funduszu Odporności Państwowej oraz z dostępnych środków unijnych (np. KPO, FEnIKS, programy cyfrowe). Ich celem byłoby podnoszenie świadomości obywateli i firm w zakresie przygotowania na sytuacje kryzysowe. Mogłyby promować dobre praktyki w przedsiębiorstwach, takie jak posiadanie AED w zakładach pracy, przeszkolenie części załogi z pierwszej pomocy, opracowanie planów ewakuacyjnych czy wdrożenie planów ciągłości

działania. Państwo powinno także udostępniać firmom poradniki i materiały eksperckie – obejmujące procedury awaryjne, zabezpieczenie danych cyfrowych i ochronę przed dezinformacją – z wykorzystaniem istniejących narzędzi, takich jak Disinfo Radar czy normy ISO.

W tym celu należałoby wydać rozporządzenie Ministra Cyfryzacji, oparte na delegacji ustawowej zawartej w art. 14 ustawy o zarządzaniu kryzysowym (UoZK). Rozporządzenie powinno określać minimalne standardy kampanii edukacyjnych prowadzonych z udziałem przedsiębiorców, w tym zakres tematyczny (pierwsza pomoc, procedury awaryjne, ochrona danych, przeciwdziałanie dezinformacji), formaty materiałów edukacyjnych oraz zasady ich dystrybucji. Finansowanie działań wynikających z rozporządzenia powinno być realizowane z modułu „edukacja i świadomość” Funduszu Odporności Państwowej.

Stała platforma dialogu publiczno-prywatnego przy RCB, o której mowa w tej rekomendacji, powinna funkcjonować jako część forum ds. współpracy publiczno-prywatnej w obszarze bezpieczeństwa. Jej wyspecjalizowany mandat obejmowałby planowanie i realizację kampanii edukacyjnych oraz włączanie pracodawców w system komunikacji kryzysowej (np. realizację działań CSR w obszarze bezpieczeństwa, zgodnych z potrzebami państwa w obszarze komunikacji kryzysowej). Forum zapewniałoby ramy ogólnopaństwowe, a jego komponent edukacyjny koordynowałby działania informacyjne i CSR.

Kluczowe jest, aby system komunikacyjny RCB został wzmocniony przez pracodawców. Komunikaty kryzysowe nie powinny być kierowane wyłącznie kanałami państwowymi, ale również docierać do obywateli poprzez wewnętrzne kanały komunikacyjne firm – mailing, systemy HR czy komunikatory wewnętrzne. Pracodawca, który na co dzień komunikuje się ze swoimi pracownikami, może skutecznie wzmacniać sygnały wysyłane przez RCB, co znacząco zwiększyłoby skuteczność wczesnego ostrzegania.

Aby rozwiązanie to miało charakter systemowy i obowiązkowy, konieczne są zmiany legislacyjne:

- w ustawie o zarządzaniu kryzysowym należy zmienić art. 14, dodając obowiązek włączania organizacji pracodawców w kampanie RCB, oraz art. 21a, dopisując ustęp, w którym znalazłby się zapis, że pracodawcy są zobowiązani do przekazywania swoim pracownikom komunikatów ostrzegawczych i informacyjnych otrzymanych od RCB za pośrednictwem wewnętrznych systemów komunikacyjnych przedsiębiorstwa;
- w Kodeksie pracy należy rozszerzyć art. 94 (obowiązki pracodawcy) o nowy punkt: „Pracodawca jest obowiązany przekazywać pracownikom komunikaty ostrzegawcze i informacyjne dotyczące bezpieczeństwa pochodzące od organów administracji publicznej, w szczególności Rządowego Centrum Bezpieczeństwa”, oraz art. 207 (obowiązki BHP), dopisując ustęp, który stwierdzałby, że pracodawca ma obowiązek niezwłocznego informowania pracowników o zagrożeniach na podstawie komunikatów organów państwowych.

W ramach systemu certyfikacji odporności (COP) przedsiębiorstwa realizujące działania edukacyjne i CSR w obszarze bezpieczeństwa mogłyby uzyskiwać dodatkowe punkty na poziomie podstawowym i średnim. COP stałby się narzędziem formalnego premiowania firm, które nie tylko spełniają wymogi techniczne, ale aktywnie wspierają państwo w komunikacji kryzysowej i budowaniu kultury odporności.

REKOMENDACJA NR 6

WZMOCNIENIE CYBERODPORNOŚCI SEKTORA PRYWATNEGO

Unijna dyrektywa NIS2 wprowadza nowe, bardziej rygorystyczne wymagania dotyczące cyberbezpieczeństwa dla firm działających w kluczowych sektorach gospodarki, takich jak energetyka, transport, bankowość, zdrowie czy administracja publiczna. Mają one na celu zwiększenie odporności na cyberzagrożenia oraz ujednolicenie standardów ochrony sieci i systemów informatycznych w całej Unii Europejskiej. W praktyce dyrektywa nakłada na przedsiębiorstwa obowiązek wdrożenia systemów zarządzania ryzykiem cybernetycznym, zapewnienia odpowiednich środków ochronnych (takich jak uwierzytelnianie wieloskładnikowe czy kryptografia), monitorowania zagrożeń oraz raportowania incydentów do odpowiednich organów. Ponadto nakłada wymogi dotyczące ciągłości działania firm w sytuacjach kryzysowych oraz obowiązek kontroli łańcuchów dostaw pod kątem potencjalnych zagrożeń.

Aby skutecznie zrealizować te wymagania, rekomenduje się wzmocnienie odporności cyfrowej sektora prywatnego przez:

- utworzenie publiczno-prywatnych centrów reagowania na incydenty cybernetyczne (regionalnych zespołów, które będą działać wspólnie dla sektora prywatnego i administracji państwowej), co pozwoli na szybszą i bardziej efektywną reakcję na zagrożenia, prowadzenie analiz oraz wymianę wiedzy i doświadczeń;
- uruchomienie programów dzielenia się informacjami o zagrożeniach (Cyber Threat Intelligence), które umożliwią firmom i organom publicznym szybkie przekazywanie informacji o nowych atakach, metodach ich wykrywania i przeciwdziałaniom, co zwiększy skuteczność ochrony przez wczesne ostrzeżenie.

INSTRUMENTY WDRAŻAJĄCE REKOMENDACJĘ 6: WZMOCNIENIE CYBERODPORNOŚCI SEKTORA PRYWATNEGO.

Realizacja rekomendacji nr 6 powinna zostać oparta na nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560 z późn. zm.), tak aby dostosować polskie przepisy do dyrektywy NIS2 i wzmocnić udział sektora prywatnego w podnoszeniu odporności cyfrowej.

W pierwszej kolejności należy uzupełnić ustawę o przepisy dotyczące regionalnych centrów reagowania na incydenty cyberbezpieczeństwa – jako jednostek działających w formule publiczno-prywatnej i powiązanych organizacyjnie z CSIRT NASK, CSIRT GOV i CSIRT MON. Propozycja mogłaby zostać ujęta w osobnym rozdziale, po art. 26, wyznaczając ramy funkcjonowania, zadania (obsługa incydentów, analiza zagrożeń, wspólne ćwiczenia) i odpowiedzialność za współpracę z biznesem.

Kolejna zmiana powinna dotyczyć art. 8 ustawy o KSC, regulującego obowiązki podmiotów kluczowych i istotnych. Artykuł ten należy rozszerzyć o:

- obowiązek udziału w systemie Cyber Threat Intelligence (CTI), tj. wymiany informacji o zagrożeniach i podatnościach w ramach krajowej platformy;
- obowiązek zapewnienia dostępu do certyfikowanych szkoleń z zakresu cyberbezpieczeństwa pracownikom z branż strategicznych (energetyka, transport, logistyka, finanse) oraz ze średnich przedsiębiorstw rozwijających działalność. Szkolenia te powinny być współfinansowane z Funduszu Odporności Państwowej, certyfikowane przez państwo i powiązane z systemem COP – moduł cyber.

Nowelizacja ustawy o KSC powinna również wprowadzić mechanizm kontyngentów w obszarze cyber. Firmy uczestniczące w systemie nie ponosiłyby kosztów dostępu do krajowych zasobów informatycznych (np. narzędzi analitycznych CTI, repozytoriów zagrożeń), ale w zamian zobowiązywałyby się do udziału w działaniach prewencyjnych i udostępniania własnych zasobów kadrowych czy informacyjnych w razie poważnego incydentu. Koszt utrzymania systemu pokrywałoby państwo, a firmy zyskiwałyby dostęp do infrastruktury i wiedzy, której samodzielnie nie mogłyby zbudować.

Środki na wzmocnienie cyberodporności powinny pochodzić z istniejących programów finansowanych z budżetu państwa (obsługa CSIRT NASK, GOV i MON), z programów rozwojowych prowadzonych przez NASK i PARP (np. Cyberbezpieczny Samorząd w ramach KPO), a także z funduszy unijnych (CEF Digital, Digital Europe, Horizon Europe). Część kosztów ponoszą już dziś przedsiębiorstwa z sektorów objętych dyrektywą NIS2, inwestując we własne systemy bezpieczeństwa. Proponowany moduł „cyber” w ramach Funduszu Odporności Państwowej powinien koordynować i łączyć te strumienie finansowania, zapewniając zwłaszcza wsparcie dla małych i średnich firm, które mają największe problemy z dostosowaniem się do wymogów NIS2.

Wreszcie, cyberodporność należy powiązać z systemem zamówień publicznych. W ustawie Prawo zamówień publicznych (art. 242) należy dodać możliwość stosowania kryteriów związanych z bezpieczeństwem informatycznym i ciągłością działania. Pozwoli to premiować firmy posiadające certyfikaty zgodności (np. ISO 27001, normy krajowe KSC, COP – moduł cyber), czyniąc cyberbezpieczeństwo jednym z parametrów konkurencyjności rynkowej.

W ramach systemu certyfikacji odporności (COP) firmy spełniające wymogi dyrektywy NIS2 oraz krajowych przepisów o cyberbezpieczeństwie mogłyby uzyskiwać certyfikat COP – moduł cyber. Byłoby to uzupełnienie poziomu zaawansowanego certyfikacji, potwierdzające spełnianie najwyższych standardów w zakresie zarządzania ryzykiem, ciągłości działania i bezpieczeństwa cyfrowego. Certyfikat taki powinien być premiowany zarówno w zamówieniach publicznych, jak i przy przyznawaniu środków z Funduszu Odporności Państwowej (moduł „cyberbezpieczeństwo”).

Doprecyzowanie powyższych rozwiązań powinno nastąpić w aktach wykonawczych – m.in. w rozporządzeniu Ministra Cyfryzacji, które określi minimalne wymagania dla platformy CTI, sposób organizacji centrów reagowania, program szkoleń dotyczących cyberbezpieczeństwa oraz kryteria przyznawania środków z Funduszu.

0 AUTORACH





Michał Dworczyk

Historyk, samorządowiec, polityk. Przewodniczący Rady Programowej Instytutu Wschodniej Flanki. Absolwent Wydziału Historii UW oraz Wydziału Bezpieczeństwa Akademii Sztuki Wojennej.

Poseł na Sejm RP VII, VIII, IX i X kadencji. W latach 2017–2023 wiceminister obrony narodowej, szef Kancelarii Prezesa Rady Ministrów – M. Morawieckiego, członek Rady Ministrów RP. Od 2024 r. poseł do Parlamentu Europejskiego. Wiceprzewodniczący Komisji Bezpieczeństwa i Obrony PE.

Jako wiceminister obrony narodowej odpowiadał m.in. za utworzenie Wojsk Obrony Terytorialnej, natomiast jako szef KPRM w pierwszych miesiącach rosyjskiej pełnoskalowej inwazji na Ukrainę koordynował pomoc humanitarną i militarną części polskiej administracji.



Bartosz Marczuk

Menedżer, ekspert ds. polityki społecznej, członek zarządu Instytutu Sobieskiego. W „Gazecie Prawnej” zajmował się polityką społeczną i kierował działem Praca. Był też m.in. zastępcą redaktora naczelnego w „Rzeczpospolitej” i „Wprost”.

W latach 2015–2018 wiceminister rodziny. Wdrożył m.in. programy 500+, 300+, rozwinął sieć instytucji opieki nad małym dzieckiem, był członkiem zespołu ds. opracowania „Polityki imigracyjnej RP”. Następnie w PFR odpowiadał m.in. za wdrożenia PPK i tarcz finansowych dla MSP.

Od 2008 r. ekspert ds. polityki społecznej w Instytucie Sobieskiego, był też ekspertem w Związku Dużych Rodzin 3+ i współautorem powstałej w latach 2006–2007 polityki rodzinnej rządu. Ukończył socjologię na UW, studia doktoranckie z ekonomii w IPiSS, podyplomowe studia o migracjach w Ośrodku Badań nad Migracjami i ze stosunków międzynarodowych na UW. Współautor książki *Jak uniknąć demograficznej katastrofy*. Żonaty, ma pięcioro dzieci.



Rafał Brzoska

Rafał Brzoska – przedsiębiorca, inwestor i filantrop, jeden z najbardziej wpływowych liderów polskiego biznesu nowej generacji. Założyciel i prezes zarządu InPost S.A., jednej z największych i najnowocześniejszych firm logistyczno-technologicznych w Europie. Zbudował od podstaw globalną organizację, która zrewolucjonizowała rynek dostaw, wprowadzając sieć maszyn Paczkomat® InPost – rozwiązanie, które stało się symbolem polskiej innowacyjności i technologicznego przyspieszenia.

Pod jego kierownictwem InPost prowadzi działalność na rynkach europejskich, w tym w Wielkiej Brytanii, Francji, Hiszpanii, Włoszech i krajach Beneluksu, obsługując każdego dnia miliony klientów i stale rozszerzając zasięg międzynarodowy. Firma jest uznawana za jeden z największych sukcesów polskiej przedsiębiorczości ostatnich dekad, a sam Rafał Brzoska – za lidera, który potrafił połączyć wizję z pragmatyzmem i globalną skalą działania.

W 2025 r. stanął na czele inicjatywy deregulacyjnej, skupiającej niezależnych ekspertów i przedsiębiorców, której celem było uproszczenie przepisów, ograniczenie biurokracji oraz odbudowa zaufania pomiędzy państwem a biznesem. Zespół opracował szeroki pakiet propozycji legislacyjnych obejmujących m.in. skrócenie procedur administracyjnych, uproszczenie prawa podatkowego oraz wprowadzenie zasady „milczącego załatwienia sprawy”.

Rafał Brzoska od lat promuje ideę odpowiedzialnej wolności gospodarczej i partnerstwa publiczno-prywatnego jako fundamentu nowoczesnego państwa. Jest orędownikiem współpracy opartej na zaufaniu, innowacji i wspólnej odpowiedzialności za rozwój gospodarczy i społeczny kraju.

Jako inwestor prywatny (tzw. anioł biznesu) aktywnie wspiera rozwój młodych przedsiębiorstw i projektów technologicznych, angażując się kapitałowo i doradczo w inicjatywy z potencjałem międzynarodowym. Fundator Rafał Brzoska Foundation, wspierającej edukację, naukę i przedsiębiorczość społeczną, tworzy przestrzeń dla nowych pokoleń liderów i promuje przywództwo oparte na wartościach.

Laureat licznych wyróżnień, w tym Nagrody Polskiej Rady Biznesu im. Jana Wejcherta w kategorii *Wizja i Innowacje*, tytułu *Wizjonera Roku* przyznanego przez „Dziennik Gazetę Prawną”, finalistą konkursu EY Przedsiębiorca Roku oraz laureat plebiscytu Tygrysy Polskiego Biznesu magazynu „Newsweek”.

Postrzegany jako wizjoner i strateg, Rafał Brzoska reprezentuje nowy typ polskiego przywództwa – opartego na innowacji, zaufaniu i odpowiedzialności. Łączy wrażliwość społeczną z pragmatyzmem biznesu i przekonaniem, że silna gospodarka jest fundamentem odpornego państwa.



dr Piotr Woyke

Ekspert w zakresie polityki obronnej z doświadczeniem pracy w sektorze publicznym (m.in. Ośrodek Studiów Wschodnich im. Marka Karpia, Ministerstwo Obrony Narodowej, Kancelaria Prezesa Rady Ministrów) oraz pionach bezpieczeństwa i analiz biznesowych w sektorze prywatnym. Od 2025 r. pełni funkcję dyrektora Instytutu Wschodniej Flanki. W 2023 r. obronił na Uniwersytecie Jagiellońskim doktorat poświęcony strategii odstraszenia niewielkich państw na przykładzie Finlandii i Izraela. Absolwent nauk politycznych na Uniwersytecie Warszawskim. Uczestnik międzynarodowych programów „Hoover Institution International Seminar” i „The James S. Denton Transatlantic Fellowship”.



Ines Biegaj

Prawniczka, aplikantka radcowska specjalizująca się w prawie pracy oraz ochronie danych osobowych. Absolwentka Wydziału Prawa i Administracji Uniwersytetu Marii Curie-Skłodowskiej w Lublinie oraz studiów podyplomowych z zakresu ochrony danych osobowych i zarządzania zasobami ludzkimi.

Posiada kilkunastoletnie doświadczenie w obszarze HR oraz administracji. Jako menedżer HR i inspektor ochrony danych koordynowała procesy kadrowe, tworzyła strategię *employer branding*, wdrażała procedury RODO oraz prowadziła audyty zgodności. Obecnie, jako młodszy prawnik w kancelarii, odpowiada za zarządzanie procesami wewnętrznymi, opracowywanie dokumentacji i wsparcie klientów w zapewnieniu zgodności z przepisami prawa pracy i ochrony danych osobowych.



Maciej Dachowski

Ekspert w zakresie dyplomacji, bezpieczeństwa i doradztwa strategicznego, z blisko 20-letnim doświadczeniem w administracji publicznej, kancelariach doradczych oraz organizacjach międzynarodowych – ONZ, UE, OBWE – i polskim MSZ. Karierę międzynarodową rozpoczął jako zastępca szefa Ambasady RP w Gruzji, następnie pracował m.in. w Misji Wsparcia Narodów Zjednoczonych w Afganistanie (UNAMA), Biurze ds. Zwalczania Terroryzmu ONZ (UNOCT) w Nowym Jorku i Dosze, a także w OBWE i EU External Action Service. Specjalizuje się w strategii instytucjonalnej, komunikacji w sytuacjach kryzysowych oraz prowadzeniu dialogu w środowiskach wysokiego ryzyka. Współtworzy kancelarię Oldman Sage, gdzie doradza w zakresie relacji międzynarodowych, zarządzania ryzykiem reputacyjnym i budowania wizerunku instytucji publicznych i prywatnych.

Obecnie pełni funkcję Program Director of the Foreign Policy and European Integration Programme w Casimir Pulaski Foundation.



Robert Draba

Doktor nauk prawnych, radca prawny oraz doświadczony menedżer. W latach 2004–2005 pełnił funkcję wiceprezydenta m.st. Warszawy, a w latach 2005–2008 był wiceszefem oraz p.o. szefa Kancelarii Prezydenta RP. Kierował pionem prawnym, współtworzył ponad 20 prezydenckich inicjatyw legislacyjnych, brał udział w projektach międzynarodowych (Możejki, Ignalina, Odessa–Brody–Płock) i reformach ustrojowych Warszawy. Doradzał zarządom największych firm, m.in. PKN Orlen i InPost, prowadził strategiczne spory gospodarcze i regulacyjne. Był partnerem PwC Legal. Współautor raportu *Sprawdzamy*, członek Komitetu Sterującego projektu oraz doradca Pracodawców RP.

W kancelarii Oldman Sage specjalizuje się w doradztwie strategicznym i reprezentowaniu klientów w złożonych sprawach sądowych i administracyjnych.



Elżbieta Jakubiak

Ekspertka z wieloletnim doświadczeniem w administracji publicznej i zarządzaniu projektami strategicznymi. Pracowała w Kancelarii Sejmu (1991–1998), m.in. jako sekretarz Komisji Spraw Zagranicznych, a w latach 2007–2011 była posłanką na Sejm RP. Pełniła funkcję ministra sportu, odpowiadając za przygotowanie Polski do EURO 2012, a wcześniej szefowała gabinetom Prezydenta RP i Prezydenta Warszawy. Koordynowała m.in. budowę Muzeum Powstania Warszawskiego i tworzenie „Wielkiej Warszawy”. Współtworzyła podstawy prawne powstania Muzeum POLIN oraz raport Straty Warszawy.

Odnaczona Krzyżem Kawalerskim Orderu Odrodzenia Polski i medalem Gloria Artis za wkład w kulturę i służbę publiczną. W kancelarii doradza klientom z sektora publicznego i prywatnego w zakresie inwestycji infrastrukturalnych, polityki miejskiej, projektów kultury oraz współpracy samorządowo-rządowej i społecznej.



Krzysztof Konrad Michalski

Ekspert i menedżer z wieloletnim doświadczeniem w biznesie międzynarodowym, administracji publicznej, spółkach Skarbu Państwa. Jako wiceprezes Agencji Rozwoju Przemysłu oraz kierujący zespołem ds. współpracy z inwestorami w Ministerstwie Rozwoju odpowiadał za realizację największych projektów inwestycyjnych w Polsce. Specjalizuje się w finansowaniu przemysłu i wspieraniu strategicznych projektów inwestycyjnych, które kształtują kierunki rozwoju gospodarczego Polski.

Absolwent stosunków międzynarodowych na UMCS, Stanford Graduate School of Business, a także kursów podyplomowych SGH, ALK i UW.

O WYDAWCACH





Instytut Sobieskiego jest polskim prywatnym ośrodkiem analitycznym typu think tank, którego misją jest „Tworzenie idei dla Polski”. Został zarejestrowany w 2005 r. jako fundacja, choć rozpoczął swoją działalność w 2003 r. W latach 2003–2010 Instytut wydawał kwartalnik „Międzynarodowy Przegląd Polityczny”. W latach 2011–2015 był organizatorem corocznego kongresu „Polska – Wielki Projekt”. W 2017 zorganizował edycję Krajowej Ligi Innowacji. Od 2017 r. Instytut kładzie duży akcent w swojej działalności na publikację opracowań i rekomendacji, których celem jest pokazywanie w jaki sposób polska gospodarka powinna wykorzystywać szanse związane z czwartą rewolucją przemysłową, innowacyjnością i nowymi technologiami.

Instytut Sobieskiego prowadzi także działalność edukacyjną poprzez realizację projektu „Akademia Młodych Ekspertów”, który wspiera młodych ludzi w rozwijaniu kompetencji przywódczych i umiejętności miękkich. Każda edycja programu koncentruje się na innym kluczowym zagadnieniu, odpowiadając na aktualne potrzeby młodego pokolenia. Obecnie, podczas 6. edycji, projekt koncentruje się na tematyce Unii Europejskiej, przekazując wiedzę oraz przygotowując uczestników do udziału w konkursach Europejskiego Urzędu Doboru Kadr (EPSO). Program otwiera uczestnikom drzwi do międzynarodowej kariery w instytucjach unijnych. To wyjątkowa okazja do zdobycia praktycznych umiejętności i rozwoju zawodowego na najwyższym poziomie.

Jednym z najnowszych projektów Instytutu Sobieskiego jest „Kanał Sobieski”, do którego subskrypcji zapraszamy na YouTube. Kanał został stworzony z myślą o inspirujących rozmowach na ważne tematy dla Polski. Spotykamy się z tam ciekawymi osobowościami, by wspólnie kształtować przestrzeń do merytorycznej debaty.

W swojej działalności Instytut Sobieskiego współpracował z wieloma podmiotami. Do tej pory były to m.in.:

- organizacje pozarządowe: Forum Automatyki i Robotyki Polskiej, Fundacja Wspierania Ubezpieczeń Wzajemnych, Fundacja Republikańska, Instytut Jagielloński, Nowa Konfederacja, Ambitna Polska, Młodzi dla Polski, Studenci dla Rzeczypospolitej, Fundacja Konrada Adenauera, Central European Energy Partners, Fundacja im. Sławomira Skrzypka, Fundacja im. Wacława Felczaka, Institute for Foreign Affairs and Trade (Külügyi és Külgazdasági Intézet), Institute for Politics and Society (Institut pro politiku a společnost), The F. A. Hayek Foundation Bratislava;
- firmy komercyjne: Aiut, Assay Group, Rohde&Schwarz, WB Electronics, Asseco, Samsung, Lotos, Google, Procter and Gable, PWC, Cisco, EY, Phoenix Systems, Uber, USP Zdrowie, Fortum, Orange, Energa, Zysk i Ska, Collegium Wratislaviense, 4CF;
- instytucje państwowe/ponadnarodowe: Ministerstwo Spraw Zagranicznych, Przedstawicielstwo Komisji Europejskiej w Polsce, Ministerstwo Klimatu i Środowiska, Fundacją Platforma Przemysłu Przyszłości, Agencja Rozwoju i Przemysłu, Giełda Papierów Wartościowych, Bank Gospodarki Krajowego, Kancelaria Prezesa Rady Ministrów, Ministerstwo Cyfryzacji, Prawo i Sprawiedliwość, Ambasada Węgier, Senat RP, Europejska Partia Konserwatystów i Reformatorów, Biuro Parlamentu Europejskiego w Polsce.

Pełną listę raportów i publikacji oraz informacje o działalności Instytutu można znaleźć na stronie www.sobieski.org.pl.

Zapraszamy także do subskrybowania Kanału Sobieski na platformie youtube.com/kanalSobieski. Dołączcie do nas – warto!



Instytut
Wschodniej Flanki

Jaka jest nasza misja?

Instytut Wschodniej Flanki stawia sobie za cel kompleksową analizę polityki bezpieczeństwa w Europie Środkowo-Wschodniej, ze szczególnym uwzględnieniem doświadczeń rosyjskiej inwazji na Ukrainie.

Polska odgrywa szczególną rolę jako jedna z największych sił wojskowych w Europie, a jej znaczenie na wschodniej flance NATO jest szczególnie istotne. W dotychczasowej refleksji strategicznej w Polsce brakowało szerszej perspektywy, pokazującej wyzwania stojące nie tylko przed Warszawą, ale również innymi stolicami regionu, które muszą dbać o swoją podmiotowość na arenie międzynarodowej.

Efektom prac Instytutu jest:

1. agregowanie danych i upowszechnianie wiedzy o wyzwaniach dla polityki bezpieczeństwa i obronnej w Europie Środkowo-Wschodniej;
2. sformułowanie realistycznych rekomendacji zmian systemowych (zarówno na poziomie strategicznym, jak i operacyjnym) w polityce bezpieczeństwa i obronnej, uwzględniających m.in. specyfikę regionu, doświadczenia ukraińskiej wojny obronnej i szanse wynikające ze współpracy sojuszniczej;
3. tworzenie platformy dialogu przedstawicieli środowisk mundurowych, urzędniczych, eksperckich, biznesowych, zainteresowanych problematyką bezpieczeństwa.

Kim jesteśmy?

Instytut Wschodniej Flanki jest apolitycznym ośrodkiem analitycznym typu think tank zarejestrowanym w Brukseli, który integruje działania sieci ekspertów reprezentujących przede wszystkim państwa wschodniej flanki NATO i Ukrainy.

W Radzie Instytutu Wschodniej Flanki zasiadają:

- Jadwiga Emilewicz, b. wicepremier i minister rozwoju Rzeczypospolitej Polskiej;
- Michał Dworczyk, b. szef KPRM i wiceminister obrony narodowej; wiceprzewodniczący Komisji Bezpieczeństwa i Obrony Parlamentu Europejskiego;
- Oleksandr Kubrakow, b. wicepremier i minister infrastruktury Ukrainy;
- Oleksij Reznikow, b. wicepremier i minister obrony Ukrainy.

Jak działamy?

Instytut prowadzi działalność analityczną we współpracy z renomowanymi ekspertami i koncentruje się na działalności publicystycznej oraz organizowaniu debaty publicznej w formatach umożliwiających swobodną wymianę myśli. Efekty prac analitycznych Instytutu będą publikowane na stronie internetowej www.wschodniaflanka.pl. Zachęcamy do kontaktu ekspertów i osoby z doświadczeniem pracy w sektorze bezpieczeństwa narodowego.

Do obszarów szczególnego zainteresowania Instytutu zaliczają się zagadnienia związane z:

- organizacją systemu obronnego państwa i działalnością służb mundurowych;
- transformacją działania sił zbrojnych, w tym modernizacją techniczną;
- wzmacnianiem odporności struktur państwowych i społeczeństwa w warunkach kryzysowych;
- skoordynowanym wsparciem dla rozwoju przemysłu obronnego;
- ochroną infrastruktury krytycznej.



Kancelaria Oldman Sage Draba, Ginel i Wspólnicy Sp.k. to zespół doświadczonych prawników łączących wiedzę prawniczą z doświadczeniem menedżerskim. Misją kancelarii jest dostarczanie klientom kompleksowego wsparcia prawnego połączonego ze strategicznym doradztwem biznesowym. Dzięki temu proponowane rozwiązania są nie tylko zgodne z prawem, ale również efektywne z punktu widzenia zarządzania. Kancelaria obsługuje zarówno podmioty prywatne, jak i publiczne, zapewniając doradztwo w kluczowych obszarach prawnych związanych z prowadzeniem działalności oraz funkcjonowaniem instytucji.

Partnerzy kancelarii to prawnicy z wieloletnim doświadczeniem zdobytym na najwyższych szczeblach administracji publicznej i biznesu. Pełnili funkcje w administracji prezydenckiej, rządowej i samorządowej, pracowali w międzynarodowych firmach doradczych (m.in. PwC) oraz zajmowali stanowiska kierownicze w spółkach giełdowych. Brali udział w zarządzaniu kryzysowym, prowadzili strategiczne spory, wdrażali systemy compliance i nadzorowali kluczowe projekty inwestycyjne.

Kancelaria posiada również wyspecjalizowaną praktykę w zakresie prawa międzynarodowego i ekspansji zagranicznej. Świadczy doradztwo w zakresie zgodności z sankcjami międzynarodowymi (prowadzenie audytów sankcyjnych, wdrażanie *compliance* i ocena ryzyka regulacyjnego) oraz wspiera firmy planujące wejście na rynki zagraniczne (analiza ryzyka prawnego, strukturyzacja inwestycji, przygotowanie kontraktów transgranicznych). Oferuje także strategiczne doradztwo w obszarze dyplomacji publicznej, współpracy międzysektorowej oraz relacji międzynarodowych. Reprezentuje klientów w postępowaniach przed organami Unii Europejskiej i instytucjami międzynarodowymi, prowadzi *due diligence* dla inwestorów spoza UE oraz doradza przy tworzeniu partnerstw publiczno-prywatnych o charakterze transgranicznym.



Rada Polskich Przedsiębiorców (RPP) to ciało doradcze Pracodawców RP najstarszej i największej organizacji pracodawców w Polsce, składające się z przedstawicieli największych prywatnych firm w naszym kraju. RPP prowadzi transparentny dialog z rządem oraz dąży do budowania silnej, innowacyjnej i zrównoważonej przyszłości Polski. Przewodniczącym RPP jest przewodniczący Rady Pracodawców RP **Rafał Brzoska**.

Od momentu powstania w 2024 r. RPP stała się głosem polskich przedsiębiorców w dialogu z administracją i partnerem rządu w procesach deregulacyjnych.

W 2025 r. RPP współtworzy projekt **#SprawdzaMY**. Angażuje się również w projekty międzynarodowe, w tym odbudowę Ukrainy, oraz wspiera inicjatywy społeczne – jak akcja „**Przedsiębiorcy dla powodzi**”.

Bezpieczeństwo państwa jest wartością fundamentalną, a reformy powinny zmierzać w kierunku zaangażowania zasobów wszystkich istotnych interesariuszy – Sił Zbrojnych RP, pozostałych służb mundurowych, administracji centralnej i samorządowej, organizacji społecznych, a także przedsiębiorstw.

Istotny kontekst dla tych wysiłków stworzyło opublikowanie w czerwcu 2025 r. raportu Instytutu Sobieskiego i Instytutu Wschodniej Flanki, zawierającego propozycję całościowej reformy tworzenia rezerw osobowych na potrzeby bezpieczeństwa państwa. Postulowane jest utworzenie Powszechnej Służby Państwowej (PSP), której architektura ma być oparta na wspólnej bazie danych obywateli świadczących różne formy służby na rzecz Ojczyzny.

Pogłębiając tę propozycję, eksperci obu Instytutów we współpracy z kancelarią Oldman Sage i Radą Polskich Przedsiębiorców zainicjowali projekt, który ma odpowiadać na pytanie: jak biznes może wspomóc system bezpieczeństwa.

W efekcie powstał raport formułujący szereg rekomendacji dla instytucji państwowych i propozycji ich praktycznej realizacji przez odpowiednie zmiany prawne, organizacyjne i funkcjonalne. Ich wspólną cechą jest jak największe wykorzystanie zasobów już obecnie dostępnych z perspektywy administracji rządowej, bez tworzenia dodatkowych obciążeń budżetowych. Koncepcja ma charakter przekrojowy i pozwoli:

- efektywnie zaangażować przedsiębiorców w proces zarządzania kryzysowego;
- stworzyć otoczenie regulacyjne w wymiarze zarządzania kryzysowego, zarówno dla państwa, pracodawców, jak i pracowników;
- uporządkować przepisy i rozwiązania na rzecz efektywnej kooperacji między państwem a przedsiębiorcami.

To pierwsza w Polsce, spójna koncepcja włączenia prywatnego biznesu w system budowy odporności państwa.



Instytut
Sobieskiego
ul. Lipowa 1a lok. 20
00-316 Warszawa

sobieski@sobieski.org.pl
www.sobieski.org.pl



Instytut
Wschodniej Flanki

Institut du flanc
est de l'OTAN
/ Chau.d'Alseberg 8971180 Uccle,
Belgia

kontakt@wschodniaflanka.pl
www.wschodniaflanka.pl



OLDMAN
SAGE

OLDMAN SAGE
– Draba, Ginel i Wspólnicy, sp.k.
ul. Jasna 7/37
00-007 Warszawa

sekretariat@oldmansage.org
www.oldmansage.org



RADA POLSKICH
PRZEDSIĘBIORCÓW

Rada Polskich
Przedsiębiorców



©Copyright by
Instytut Sobieskiego 2025

ISBN 978-83-68374-14-8
Warszawa 2025



@InstSobieskiego



Instytut Sobieskiego



Instytut Sobieskiego



Kanał Sobieski



Kanał Sobieski

