INFRASTRUKTURA *DUAL-USE* W FORMULE PARTNERSTWA PUBLICZNO-PRYWATNEGO

RAPORT

AGATA KOZŁOWSKA
KACPER KOZŁOWSKI

INSTYTUT SOBIESKIEGO

INSTYTUT
SOBIESKIEGO

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

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

INFRASTRUKTURA *DUAL-USE*
W FORMULE PARTNERSTWA PUBLICZNO-PRYWATNEGO

978-83-966872-2-7

Projekt i produkcja: Piotr Perzyna

nowe media 24.pl

KOMITET
DO SPRAW
POŻYTKU
PUBLICZNEGO

NIW

Sfinansowano ze środków Narodowego Instytutu Wolności –
Centrum Rozwoju Społeczeństwa Obywatelskiego
Rządowego Programu Rozwoju Organizacji Obywatelskich
na lata 2018–2030 PROO

PROO

INFRASTRUKTURA *DUAL-USE* W FORMULE PARTNERSTWA PUBLICZNO-PRYWATNEGO

RAPORT

AGATA KOZŁOWSKA
KACPER KOZŁOWSKI

INSTYTUT SOBIESKIEGO

SPIS TREŚCI

SŁOWNIK 6

CEL I ZAKRES RAPORTU 7

KONKLUZJE I REKOMENDACJE 9

1. POJĘCIE INFRASTRUKTURY KRYTYCZNEJ ORAZ INFRASTRUKTURY OBRONNOŚCI I BEZPIECZEŃSTWA 11

1.1 POJĘCIE INFRASTRUKTURY KRYTYCZNEJ W REGULACJACH UNII EUROPEJSKIEJ 12

1.2 POJĘCIE INFRASTRUKTURY KRYTYCZNEJ W POLSKIM PRAWIE 14

1.3 POJĘCIE INFRASTRUKTURY BEZPIECZEŃSTWA I OBRONNOŚCI 19

1.4 POJĘCIE INFRASTRUKTURY TYPU DUAL-USE 20

2. PARTNERSTWO PUBLICZNO-PRYWATNE 23

2.1 CHARAKTERYSTYKA PARTNERSTWA PUBLICZNO-PRYWATNEGO 23

2.2 MOŻLIWOŚCI REALIZACJI I FINANSOWANIA INFRASTRUKTURY BEZPIECZEŃSTWA W FORMULE PPP 24

2.3 SZANSE I ZAGROŻENIA ZWIĄZANE Z WYKORZYSTANIEM PPP DO BUDOWY I UTRZYMANIA INFRASTRUKTURY ZAPEWNIENIA BEZPIECZEŃSTWA 28

3. PROJEKTY PPP W ZAKRESIE INFRASTRUKTURY KRYTYCZNEJ ORAZ BEZPIECZEŃSTWA PLANOWANE I REALIZOWANE W POLSCE I NA ŚWIECIE 30

3.1 PROJEKT W POLSCE 30

3.2 PROJEKTY NA ŚWIECIE 31

BIBLIOGRAFIA 34

O AUTORACH 35

SŁOWNIK

MFiPR
Ministerstwo Funduszy i Polityki Regionalnej

Polityka PPP
Polityka partnerstwa publiczno-prywatnego - polityka rządu w zakresie rozwoju partnerstwa publiczno-prywatnego, stanowiąca załącznik do uchwały na 116/2017 Rady Ministrów z dnia 26 lipca 2017 r. w sprawie przyjęcia dokumentu „Polityka Rządu w zakresie rozwoju partnerstwa publiczno-prywatnego" (aktualizowana).

PFR
Polski Fundusz Rozwoju

PPP
Partnerstwo Publiczno-Prywatne

Ustawa o PPP
ustawa z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym (t. j. Dz. U. z 2023 r., poz. 30 z późn. zm.)

Ustawa o planowaniu i zagospodarowaniu przestrzennym
ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (t. j. Dz. U. z 2022 r., poz. 503 z późn. zm.)

Ustawa o zarządzaniu kryzysowym
ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t. j. Dz. U. z 2023 r., poz 122 z późn. zm.)

Ustawa Prawo zamówień publicznych
ustawa z dnia 11 września 2019 r. - Prawo zamówień publicznych (t. j. Dz. U. z 2022 r., poz. 1710 z późn. zm.)

CEL I ZAKRES RAPORTU

Ochrona podstawowych dóbr, takich jak życie, zdrowie i szeroko rozumiane bezpieczeństwo, należy do zadań administracji publicznej. Podmioty publiczne odpowiedzialne są za zapewnienie bezpieczeństwa i porządku publicznego oraz funkcjonowanie infrastruktury dla społeczeństwa, w tym infrastruktury krytycznej. Z tymi funkcjami bezpośrednio związane jest podejmowanie odpowiednich działań na wypadek wystąpienia niebezpieczeństwa i zagrożeń wobec dóbr prawnie chronionych.

Mając na względzie trwającą od ponad roku wojnę za naszą wschodnią granicą, będącą skutkiem napaści zbrojnej Rosji na Ukrainę, analizie poddano infrastrukturę służącą zapewnieniu bezpieczeństwa: zarówno infrastrukturę krytyczną, jak i obiekty, czy budynki, które mogą posłużyć wykorzystaniu na wypadek zagrożenia (obiekty infrastrukturalne o szerokim przeznaczeniu), a także infrastrukturę w zakresie obronności i bezpieczeństwa. Zapewnienie oraz eksploatacja (w tym utrzymanie, zarządzanie) tego typu infrastruktury wymaga niezwykle wysokich nakładów finansowych oraz wiedzy, które – w niektórych przedsięwzięciach – dostarczyć może partner prywatny.

O zastosowaniu formuły partnerstwa publiczno-prywatnego (dalej jako PPP) w dziedzinie bezpieczeństwa, w tym infrastrukturze krytycznej i obronności, dyskutuje się coraz częściej. Jednak ze względu na niewielką liczbę przeprowadzonych w tej formule projektów, coraz bardziej zaawansowany technicznie charakter tego rodzaju inwestycji przy jednoczesnej konieczności zachowania tajemnicy państwowej oraz różnego rodzaju obawy, stosuje się ją rzadko. PPP pozwala jednak na osiągnięcie nowatorskich rozwiązań (szczególnie w zakresie technologicznym i informatycznym), a także rozłożenie finansowania przedsięwzięcia w dłuższym horyzoncie czasowym.

Zdaniem autorów raportu nadszedł czas na szczegółową analizę koncepcji PPP i zastanowienie się jak można zastosować ją w realizacji i podjęciu działań w zakresie budowy i zarządzania szeroko rozumianą infrastrukturą, która mogłaby zostać wykorzystana w przypadku zagrożenia wojennego. Przy czym należy podkreślić, że niniejszy raport partnerstwo traktuje wyłącznie jako narzędzie zwiększające efektywność realizacji inwestycji wdrażane na podstawie Ustawy o PPP oraz Ustawy Prawo zamówień publicznych. Autorzy są zdania, że tylko taki tryb realizacji projektów PPP, zapewnia ich transparentność oraz poszanowanie interesu publicznego. Szeroko rozumiane PPP czyli zawiązywanie spółek publiczno-prywatnych poza reżimem Ustawy o PPP, zostało opisane oddzielnie tam, gdzie była taka potrzeba.

Podstawowym celem raportu jest dostarczenie podmiotom odpowiedzialnym za powstawanie, zarządzanie i ochronę infrastruktury rekomendacji w zakresie możliwości współpracy z partnerami prywatnymi w tym obszarze. Pobocznym celem, jednak nie mniej istotnym, wynikającym z uwzględnienia w raporcie możliwości współdziałania podmiotów publicznych z partnerami prywatnymi, jest doprowadzenie do zrozumienia przez prywatnych przedsiębiorców, jakie aspekty należy wziąć pod uwagę przy realizacji tego rodzaju infrastruktury.

Główne cele raportu to:

1. rekomendacje w zakresie realizacji projektów dotyczących infrastruktury na wypadek wojny w formule PPP;

2. określenie czynników zagrożenia i sukcesu projektów w formule PPP;

3. zaprezentowanie najważniejszych aspektów do uwzględnienia w ramach współpracy publiczno-prywatnej;

4. przygotowanie propozycji działań.

Partnerstwo publiczno-prywatne jako narzędzie do realizacji inwestycji infrastrukturalnych, również w zakresie infrastruktury na wypadek wojny, nie pojawiło się w raporcie przypadkowo. Obecnie podmioty, w tym organy administracji publicznej, odpowiedzialne za realizację zadań publicznych w zakresie obronności i bezpieczeństwa, poszukują sposobów na sfinansowanie planów inwestycyjnych oraz przeprowadzenie ich w sposób jak najbardziej efektywny z wykorzystaniem najnowszych osiągnięć technologicznych. Dostarczenie tych rozwiązań (w zakresie finansowania i *know-how*) jest podstawowym celem współpracy publiczno-prywatnej. Jednak w celu realizacji przedsięwzięć z zakresu obronności i bezpieczeństwa w tej formule, należy na podstawie regulacji prawnych oraz doświadczeń innych państw, określić czynniki bezpiecznej i efektywnej współpracy.

Rekomendacje powstały na podstawie analizy różnych aspektów związanych z procesem inwestycyjnym, jakiemu podlega każdy rodzaj infrastruktury, w tym infrastruktury krytycznej i bezpieczeństwa, z uwzględnieniem jej specyficznego charakteru. Aspekty te uwzględniają polskie regulacje prawne w zakresie omawianej infrastruktury oraz partnerstwa publiczno-prywatnego. Odrębnie, tam gdzie była taka potrzeba, dookreślono obowiązki prawne związane z realizacją infrastruktury obronności. Z kolei *case studies* prezentowane są poglądowo, na podstawie doświadczeń międzynarodowych, ponieważ polskie przedsięwzięcia realizowane w formule PPP są na razie pojedyncze.

Struktura raportu koresponduje z jego założeniami w zakresie celów. W pierwszej kolejności na podstawie pogłębionych studiów nad polskimi aktami prawnymi oraz międzynarodowymi raportami zaprezentowano prawne i organizacyjne aspekty infrastruktury na wypadek wojny, uwzględniając odmienności rozumienia i regulacji pojęć wchodzących w jej zakres (w tym podział na infrastrukturę krytyczną, obronności i bezpieczeństwa oraz infrastrukturę typu *dual -use*).

Druga część raportu dotyczy charakterystyki formuły partnerstwa publiczno-prywatnego, a także szans i zagrożeń wynikających z zastosowania tej koncepcji w realizacji przedsięwzięć dotyczących realizacji różnego rodzaju infrastruktury na wypadek wojny.

Trzecia część raportu prezentuje przykłady projektów z zakresu szeroko rozumianej infrastruktury bezpieczeństwa: jedno przedsięwzięcie, obecnie realizowane w Polsce oraz kilka międzynarodowych inwestycji przeprowadzonych w różnych państwach.

Raport wpisuje się w ogólną dyskusję nad wykorzystaniem formuły PPP w kontekście rozwoju infrastruktury w Polsce, zainicjowaną przyjęciem przez Radę Ministrów Polityki Rządu w zakresie rozwoju partnerstwa

publiczno-prywatnego[1] w 2017 r. (dalej jako Polityka PPP) oraz debatę na temat efektywnej realizacji i sfinansowania pilnych przedsięwzięć infrastrukturalnych na wypadek wojny, w tym z zakresu bezpieczeństwa i obronności.

KONKLUZJE I REKOMENDACJE

Przede wszystkim należy podkreślić, że formuła partnerstwa publiczno-prywatnego nie we wszystkich projektach może być wdrażana. Należy traktować ją jako narzędzie poprawiające efektywność realizacji inwestycji, biorąc pod uwagę cały cykl życia projektu. Ta wartość dodana musi zostać udowodniona zarówno dla interesu publicznego, jak i po stronie partnera prywatnego. W innym przypadku należy stosować odmienne rozwiązania.

Mając jednak na względzie obecne potrzeby inwestycyjne w Polsce oraz brak środków publicznych na realizację niezbędnych projektów infrastrukturalnych, partnerstwo publiczno-prywatne może okazać się metodą na przyspieszenie realizacji niektórych z nich lub pozwolić na zrealizowanie równocześnie większej liczby inwestycji poprzez zastosowanie do części PPP, a w pozostałym zakresie wykorzystanie środków budżetowych.

Wobec trwającej obecnie wojny w Ukrainie, rekomenduje się poniższe działania w zakresie infrastruktury na wypadek wojny, w tym infrastruktury krytycznej.

Rekomendacje w zakresie koordynacji działań administracji:

- ukierunkowanie i zwiększenie zaangażowania organów administracji na wszystkich szczeblach w zakresie wsparcia oraz udziału w finansowaniu i opracowaniu wytycznych i zasad realizacji projektów z zakresu infrastruktury na wypadek wojny, w tym z uwzględnieniem formuły partnerstwa publiczno-prywatnego;

- poszerzenie współpracy międzynarodowej państwa z potencjalnymi partnerami prywatnymi zainteresowanymi współpracą przy projektach infrastrukturalnych z zakresu infrastruktury na wypadek wojny;

- zaproponowanie priorytetów w zakresie inwestycji obejmujących szeroko rozumianą infrastrukturę bezpieczeństwa, w tym planowaną do realizacji z udziałem partnerów prywatnych;

- opracowanie strategicznego dokumentu na poziomie administracji rządowej w kontekście zastosowania PPP w infrastrukturze typu *dual-use*, w tym ujednolicenie nazewnictwa prawnego szeroko rozumianej infrastruktury na wypadek wojny, obiektów i instalacji infrastruktury krytycznej;

- stworzenie centrum współpracy administracji z przedstawicielami biznesu w formie forum dyskusyjno-intelektualnego;

- wprowadzenie przedsięwzięć z zakresu infrastruktury typu *dual-use* do Polityki PPP.

1 Uchwała Nr 116/2017 Rady Ministrów z dnia 26 lipca 2017 roku w sprawie przyjęcia dokumentu „Polityka Rządu w zakresie rozwoju partnerstwa publiczno-prywatnego", zaktualizowana.

Rekomendacje w zakresie finansowania i audytu przedsięwzięć:

- opracowanie programu współfinansowania bądź gwarancji finansowych kluczowych inwestycji infrastrukturalnych na wypadek wojny, planowanych do realizacji w formule PPP;

- przeprowadzenie audytu przedsięwzięć z zakresu szeroko rozumianej infrastruktury bezpieczeństwa realizowanych w formule PPP w celu pozyskania informacji o doświadczeniach z zakresu realizowanych projektów i popełnionych błędów w celu ich wyeliminowania w przyszłości.

Rekomendacje w zakresie zmian w prawie:

- uporządkowanie w prawie pojęć dotyczących infrastruktury bezpieczeństwa, obronności, krytycznej oraz pojęć odnoszących się do obiektów takich jak np. schrony;

- prawne uregulowanie pojęć z zakresu infrastruktury zapewnienia bezpieczeństwa (w tym schronów) oraz opracowanie przepisów prawnych dotyczących norm technicznych dla obiektów budowanych na podstawie koncepcji *dual-use* (punktem wyjścia mogą być „Warunki techniczne, jakim powinny odpowiadać budowle ochronne", stanowiące załącznik nr 1 do wytycznych Szefa Obrony Cywilnej Kraju z 4 grudnia 2018 r. w sprawie zasad postępowania z zasobami budownictwa ochronnego);

- uregulowanie w prawie pojęcia infrastruktury *dual-use*, czyli infrastruktury mogącej spełniać równocześnie funkcje cywilne i na wypadek zagrożenia wojennego;

- opracowanie tzw. mapy drogowej dla prywatnych inwestorów (w tym zagranicznych) prezentującej prawne regulacje w zakresie zamówień publicznych oraz partnerstwa publiczno-prywatnego w Polsce.

1. POJĘCIE INFRASTRUKTURY KRYTYCZNEJ ORAZ INFRASTRUKTURY OBRONNOŚCI I BEZPIECZEŃSTWA

Pojęcie infrastruktury zapewnienia bezpieczeństwa na wypadek wojny jest bardzo szerokie. Znacząco wykracza poza ustawowe pojęcie infrastruktury krytycznej, które w Polsce i w Unii Europejskiej jest ściśle uregulowane. Intuicyjnie nawiązuje do infrastruktury z zakresu obronności i bezpieczeństwa, chociaż nie zawsze pełni takie funkcje.

Problematyka infrastruktury zapewnienia bezpieczeństwa to stosunkowo nowe zagadnienie w publicznej dyskusji w Polsce. Jakkolwiek w ustawodawstwie i w literaturze pojęcie „infrastruktury krytycznej" ma swoje ugruntowane znaczenie (por. punkty poniżej), to zakres pojęcia infrastruktury bezpieczeństwa zależy od autora wypowiedzi, który się do niej odnosi. Często oznacza ono zakres infrastruktury krytycznej (szczególnie cyfrowej) i jest używane zamiennie. Niekiedy tym określeniem obejmuje się również zaplecze techniczne dla działania służb ratunkowych.

Poniżej opisano różnice pomiędzy tymi pojęciami, oraz brak doprecyzowania niektórych z nich, czemu służy m.in. brak kompletnych regulacji ustawowych. W związku z tym oraz mając na względzie, że w formule partnerstwa publiczno-prywatnego inne projekty realizowane są w kraju a inne, w o wiele szerszym zakresie, na świecie, przedsięwzięcia infrastrukturalne omówiono w trzech obszarach i w kontekście poniższego podziału zostaną również zaprezentowane koncepcje wykorzystania formuły partnerstwa publicznego.

Podział ten dotyczy:

- Infrastruktury krytycznej;
- Infrastruktury obronności i bezpieczeństwa;
- Infrastruktury typu *dual-use*.

Warto przy tym zwrócić uwagę, że wraz z rozwojem nowych technologii, część infrastruktury krytycznej obejmuje tzw. infrastrukturę cyfrową (sieci teleinformatyczne, infrastruktura rynków finansowych) a istotna większość infrastruktury krytycznej i jej współzależnych systemów funkcjonują w formie cyfrowej. Coraz większe uzależnienie działania infrastruktury bezpieczeństwa od rozwiązań cyfrowych i ciągłe zmiany, jakie mają miejsce w systemach teleinformatycznych, powodują pilną potrzebę zapewnienia cyberbezpieczeństwa. Jest to konieczne dla zapewnienia ciągłości dostarczania usług dla ludności, poprzez uchronienie ich przed awariami technicznymi, przerwami konserwacyjnymi, a nawet konsekwencjami ludzkich błędów, czy katastrof środowiskowych. Jednak, równie istotne, a może obecnie nawet bardziej znaczące, jest także zapewnienie bezpieczeństwa funkcjonowania samych sieci teleinformatycznych, które coraz częściej stają obszarem ataków, czy wrogich działań prowadzonych w cyberprzestrzeni.

1.1 POJĘCIE INFRASTRUKTURY KRYTYCZNEJ W REGULACJACH UNII EUROPEJSKIEJ

Zainteresowanie zagadnieniem infrastruktury krytycznej pojawiło się w literaturze światowej pod koniec XX wieku, a nabrało znaczenia po zamachach terrorystycznych w 2001 r., gdy Kongres Stanów Zjednoczonych w tym samym roku uchwalił Patriot Act[2]. Definiowała ona infrastrukturę krytyczną m.in. jako system i aktywa-fizyczne i wirtualne, których zniszczenie może mieć wpływ na obniżenie bezpieczeństwa narodowego, w tym ekonomicznego i publicznego[3].

Kilka lat później (po zamachach w Madrycie w 2004 r.) Unia Europejska zaczęła pracować nad europejskim programem ochrony infrastruktury krytycznej (EPOIK) oraz utworzeniem sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (SOZIK) Zaowocowało to opracowaniem zbioru zasad, procedur i narzędzi, które zostały wykorzystane w procesie tworzenia EPOIK[4]. W listopadzie 2005 r. Komisja przyjęła tzw. zieloną księgę w sprawie europejskiego programu ochrony infrastruktury krytycznej (EPOIK), w której opisano opcje polityczne, jakie Komisja mogłaby zastosować przy opracowywaniu EPOIK i SOZIK.

W Komunikacie z 2006 r. Komisja Europejska wskazała, że europejskie infrastruktury krytyczne to infrastruktury o największym znaczeniu dla Wspólnoty. Ich zakłócenie lub zniszczenie miałoby negatywny wpływ na co najmniej dwa państwa członkowskie lub na jedno państwo członkowskie, gdy infrastruktura krytyczna jest zlokalizowana w innym państwie członkowskim. Chodzi między innymi o skutki transgraniczne wynikające ze współzależności między powiązanymi ze sobąróżnymi sektorami infrastruktury.

Procedury rozpoznawania i wyznaczania europejskich infrastruktur krytycznych oraz wspólne zasady oceny potrzeb w zakresie zwiększenia ochrony takich infrastruktur zostały określone w dyrektywie 2008/114/WE[5]. Okazała się ona jednak niewystarczająca wobec coraz to nowych zagrożeń, dlatego też rozpoczęto prace nad nowymi regulacjami kompleksowo definiującymi zakres infrastruktury technicznej. Nowa dyrektywa CER (2022/2557), która weszła w życie 17 stycznia br.[6], definiuje usługi kluczowe (jako mające decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska – art. 2 pkt dyrektywy CER) oraz infrastrukturę krytyczną jako niezbędną do świadczenia usług kluczowych (jako składnik; obiekt, sprzęt, sieć lub system lub część składnika, obiektu, sprzętu, sieci,lub systemu; niezbędne do świadczenia usługi kluczowej – art. 2 pkt 4 dyrektywy CER). W załączniku do Dyrektywy wskazano sektory, w których, po wejściu w życie przepisów, wyznaczane będą podmioty krytyczne.

2 Por. M. Banasik, J. Bagińska „Krytyczne uwagi dotyczące bezpieczeństwa infrastruktury krytycznej", Rocznik Bezpieczeństwa Międzynarodowego 2019 vol. 13, nr 2, s. 72-73.

3 US Patriot Act. (2001, 26 października). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (US a Patriot Act) Act of 2001. Public Law No 107-56 (107th Congress), por. tamże, s. 73.

4 Komunikat Komisji w sprawie europejskiego programu ochrony infrastruktury krytycznej /* COM/2006/0786 końcowy, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52006DC0786&from=EN [dostęp: 23.02.2023 r.].

5 Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32008L0114 [dostęp: 23.02.2023 r.].

6 Dyrektywa Parlamentu Europejskiej i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Ray 2008/114/WE, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2557 [dostęp: 23.02.2023 r.,], dalej „dyrektywa CER".

Są to sektory:

- Energetyka (energia elektryczna, centralne ogrzewanie i chłodzenie, ropa, gaz, wodór);
- Transport (powietrzny, kolejowy, wodny, lądowy);
- Bankowość;
- Infrastruktura rynków finansowych;
- Zdrowie;
- Woda pitna;
- Ścieki;
- Infrastruktura cyfrowa;
- Administracja publiczna;
- Przestrzeń kosmiczna;
- Wytwarzanie, przetwarzanie i dystrybucja żywności.

Nowe regulacje prawne nakładają na państwa członkowskie obowiązki w zakresie opracowania analizy ryzyka, która uwzględnia sektorowe oceny ryzyka przeprowadzone na podstawie innych aktów prawnych UE oraz zależności pomiędzy sektorami krajowymi i międzynarodowymi. To fundament do przyjęcia strategii, której celem będzie wzmocnienie odporności podmiotów krytycznych. Wdrożenie dyrektywy CER jest przewidziane na okres 3 lat, dlatego już teraz Rada UE wydała rekomendacje w zakresie skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej[7]. W zaleceniu Rady wskazano, że państwa członkowskie powinny, zgodnie z prawem unijnym i krajowym, wykorzystywać wszystkie dostępne narzędzia, aby poczynić postępy i przyczynić się do wzmocnienia odporności fizycznej i cyberodporności.

W tym zakresie infrastrukturę krytyczną należy rozumieć jako obejmującą odpowiednią infrastrukturę krytyczną wskazaną przez państwo członkowskie na szczeblu krajowym lub wyznaczoną jako europejska infrastruktura krytyczna na mocy dyrektywy 2008/114/WE. Podmioty krytyczne należy wskazać w myśl dyrektywy CER, lub, w stosownych przypadkach, objęte dyrektywą NIS 2[8].

7 Zalecenie Rady Europejskiej z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej (2023/C 20/01), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32023H0120(01) [dostęp: 23.02.2023 r.], dalej jako „Zalecenie Rady".

8 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) [dostęp: 23.02.2023 r.].

Pojęcie odporności należy rozumieć jako odnoszące się do zdolności infrastruktury krytycznej do zapobiegania zdarzeniom, które w istotny sposób zakłócają lub mogą zakłócić świadczenie kluczowych na rynku wewnętrznym usług, tj. usług, które są konieczne dla utrzymania niezbędnych funkcji społecznych i gospodarczych, bezpieczeństwa publicznego, zdrowia ludności lub środowiska, a także do zdolności tej infrastruktury do ochrony przed takimi zdarzeniami, reagowania na nie, przeciwstawiania się im, łagodzenia lub amortyzowania ich skutków, przystosowywania się do nich lub przywracania poprzedniego stanu[9].

Mając na uwadze istniejące zagrożenia, związane z trwającą wojną w Ukrainie oraz zdarzenia, jakie już wystąpiły (zniszczenie NORD Stream I i II, cyberataki na infrastrukturę krytyczną oraz ataki sabotażowe na systemy sterowania ruchem pociągów w Niemczech), Rada Europejska zdecydowała się na wprowadzenie pilnych rozwiązań przejściowych[10]. Główny nacisk w obecnych działaniach kładzie się na podwyższoną gotowość państw członkowskich w zakresie ochrony infrastruktury cyfrowej, w szczególności powiązanej z infrastrukturą energetyczną oraz transportową, a także zapewnienie bezpieczeństwa tych dwóch sektorów.

1.2 POJĘCIE INFRASTRUKTURY KRYTYCZNEJ W POLSKIM PRAWIE

W polskim piśmiennictwie pojęcie infrastruktury krytycznej zaczęło być intensywniej dyskutowane w XX wieku, a uregulowane prawnie zostało już w 2007 r. Infrastruktura krytyczna pełni kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. W wyniku zdarzeń spowodowanych siłami natury lub będących konsekwencją działań człowieka, infrastruktura krytyczna może być zniszczona, uszkodzona, a jej działanie może ulec zakłóceniu, przez co zagrożone może być życie i mienie obywateli. Równocześnie tego typu wydarzenia negatywnie wpływają na rozwój gospodarczy państwa. Stąd też ochrona infrastruktury krytycznej jest jednym z priorytetów stojących przed państwem polskim. Istota zadań związanych z infrastrukturą krytyczną sprowadza się nie tylko do zapewnienia jej ochrony przed zagrożeniami, ale również do tego, aby ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat dla obywateli i gospodarki.

Ochrona infrastruktury krytycznej to wszelkie działania zmierzające do zapewnienia przez władze funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków. To także zdolnośćdo szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków czy innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Zgodnie z Ustawą o zarządzaniu kryzysowym, infrastrukturę krytyczną definiuje się (art. 3 pkt 2 ustawy) jako systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:

a) zaopatrzenia w energię, surowce energetyczne i paliwa;

b) łączności;

c) sieci teleinformatycznych;

9 Por. pkt 7 Zalecenia Rady.

10 Por. https://www.gov.pl/web/rcb/dyrektywa-cer—dyrektywa-o-odpornosci-podmiotow-krytycznych [dostęp: 23.02.2023 r.].

d) finansowe;

e) zaopatrzenia w żywność;

f) zaopatrzenia w wodę;

g) ochrony zdrowia;

h) transportowe;

i) ratownicze;

j) zapewniające ciągłość działania administracji publicznej;

k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Jest to działalność w dużym zakresie spełniająca definicję monopolu naturalnego w zakresie użyteczności publicznej, czyli podstawowych zadań publicznych, do których wykonywania zobowiązana jest administracja rządowa lub samorządowa.

Model zarządzania infrastrukturą krytyczną opiera się na przygotowywanym co dwa lata Krajowym Planie Zarządzania Kryzysowego (KPZK) oraz na raportach zagrożeń bezpieczeństwa narodowego (RZBN). Obowiązek sporządzania raportów mają ministerstwa, urzędy centralne oraz wojewodowie. W procesie tym opcjonalnie mogą uczestniczyć powiaty oraz gminy. Koordynatorem prac jest Rządowe Centrum Bezpieczeństwa (RCB), które na podstawie raportów opracowuje KPZK. Dokumenty te dają podstawę do opracowania wojewódzkich, powiatowych i gminnych planów zarzadzania kryzysowego a także Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK[11]), który określa zadania i obowiązki w zakresie ochrony infrastruktury krytycznej. Ochrona infrastruktury krytycznej opiera się na współpracy administracji publicznej z operatorami, czyli właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń i usług infrastruktury krytycznej (są to zarówno podmioty publiczne jak i prywatne).

Organy administracji publicznej i inne podmioty odpowiedzialne za dany system infrastruktury krytycznej prezentuje poniższa tabela.

11 Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity (uchwała nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej z uwzględnieniem Uchwały nr 116/2020 Rady Ministrów z dnia 13 sierpnia 2020 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej), https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 27.02.2023 r.].

TAB. 1. ORGANY ADMINISTRACJI PUBLICZNEJ I INNE PODMIOTY ODPOWIEDZIALNE ZA DANY SYSTEM INFRASTRUKTURY KRYTYCZNEJ

SYSTEM INFRASTRUKTURY KRYTYCZNEJ	PRZYKŁADOWE: INFRASTRUKTURA/OBIEKTY/ USŁUGI	PODMIOTY ZARZĄDZAJĄCE	ORGAN ADMINISTRACJI ODPOWIEDZIALNY ZA SYSTEM INFRASTRUKTURY KRYTYCZNEJ
zaopatrzenie w energię, surowce energetyczne i paliwa	sieci elektryczne i energetyczne	spółki energetyczne; spółki paliwowe	minister właściwy ds. aktywów państwowych; minister właściwy ds. energii; minister właściwy ds. gospodarki złożami kopalin
łączność	sieci telekomunikacyjne	operatorzy sieciowi; jednostki samorządu terytorialnego	minister właściwy ds. informatyzacji; minister właściwy ds. łączności
sieci teleinformatyczne	Internet i łącza szerokopasmowe, w tym aplikacje i programy instytucji publicznych	operatorzy teleinformatyczni; jednostki samorządu terytorialnego	minister właściwy ds. informatyzacji
systemy finansowe	systemy teleinformatyczne; obiekty banków i instytucji finansowych	banki, instytucje finansowe; operatorzy teleinformatyczni	minister właściwy ds. budżetu; minister właściwy ds. finansów publicznych; minister właściwy ds. instytucji finansowych
zaopatrzenie w żywność	systemy produkcji i pozyskiwania surowców żywnościowych; przetwórstwo; transport; przechowywanie; systemy bezpieczeństwa żywności	jednostki samorządu terytorialnego; spółki, w tym z udziałem Skarbu Państwa; przedsiębiorcy prywatni; urzędy administracji rządowej	minister właściwy ds. rolnictwa; minister właściwy ds. rynków rolnych; minister właściwy ds. zdrowia
zaopatrzenie w wodę	infrastruktura wodno-kanalizacyjna (w tym sieci wodno-kanalizacyjne; stacje uzdatniania wody, przepompownie)	spółki wodno-kanalizacyjne; jednostki samorządu terytorialnego; przedsiębiorcy prywatni	minister właściwy ds. gospodarki wodnej
ochrona zdrowia	szpitale; przychodnie	Narodowy Fundusz Zdrowia; przedsiębiorcy prywatni	minister właściwy ds. zdrowia
transport	infrastruktura drogowa, kolejowa, lotnicza, wodna	m.in. Generalna Dyrekcja Dróg Krajowych i Autostrad; jednostki samorządu terytorialnego	minister właściwy ds. transportu; minister właściwy ds. gospodarki morskiej
systemy ratownicze	Krajowy System Ratowniczo-Gaśniczy; Państwowe Ratownictwo Medyczne; System Powiadamiania Ratunkowego; ratownictwo górskie, morskie, górnicze, wodne; Krajowy System Wykrywania Skażeń i Alarmowania	administracja rządowa i terenowa	minister właściwy ds. Wewnętrznych; minister właściwy ds. obrony narodowej
zapewnianie ciągłości działania administracji publicznej	systemy teleinformatyczne; obiekty administracji publicznej	podmioty administracji publicznej; jednostki samorządu terytorialnego; jednostki pomocnicze	minister właściwy ds. informatyzacji
produkcja; składowanie; przechowywanie i stosowanie substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	m.in. rurociągi substancji niebezpiecznych; źródła promieniowania jonizującego; obiekty jądrowe	spółki energetyczne; instytucje państwowe; agencje	minister właściwy ds. klimatu i środowiska

Źródło: opracowanie własne na podstawie wykazu ministrów odpowiedzialnych za poszczególne systemy infrastruktury krytycznej, zawartego w NPOIK

W ramach systemu ochrony infrastruktury krytycznej zadania wykonują również wojewodowie z pomocą podległych im służb, straży i inspekcji, którzy. współpracują m.in. z samorządem terytorialnym w realizacji zadań z zakresu zarządzania kryzysowego i planowania cywilnego, wynikających z kompetencji samorządu województwa oraz z operatorami infrastruktury krytycznej.

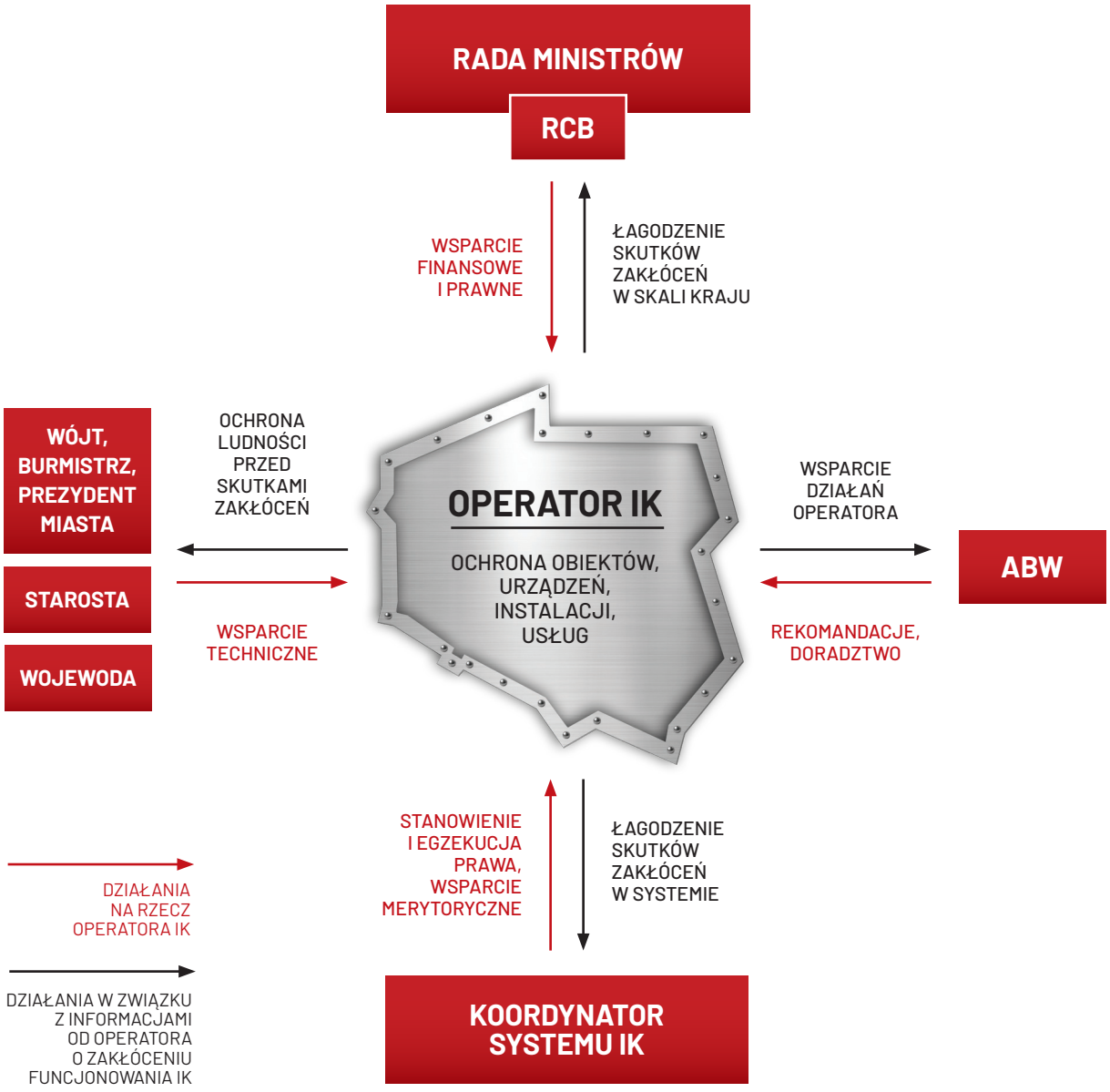
Jeśli chodzi o starostów, wójtów, burmistrzów i prezydentów miast, ich rolą jest przede wszystkim organizacja wykonania zadań z zakresu ochrony infrastruktury krytycznej, w tym:

- ujęcie zadań z zakresu ochrony infrastruktury krytycznej zlokalizowanej w obszarze właściwości w planach zarządzania kryzysowego;
- określanie procedur reagowania na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej w obszarze właściwości organu;
- ochrona ludności przed skutkami zakłócenia funkcjonowania infrastruktury krytycznej z wykorzystaniem zasobów własnych oraz operatora;
- wsparcie operatorów technicznymi i ludzkimi zasobami pozostającymi w dyspozycji własnej oraz podległych lub nadzorowanych służb, inspekcji i straży;
- współpraca i wsparcie operatorów w zakresie jej ochrony i współdziałanie w przypadku wystąpienia sytuacji kryzysowej w obszarze właściwości organu[12].

12 Por. NPOIK, s. 23, 24-25.

Poniższy wykres prezentuje relacje pomiędzy głównymi podmiotami w systemie ochrony infrastruktury krytycznej w Polsce.

RYS. 1. **RELACJE POMIĘDZY GŁÓWNYMI PODMIOTAMI W SYSTEMIE OCHRONY INFRASTRUKTURY KRYTYCZNEJ W POLSCE.**



Źródło danych: Narodowy Program Ochrony Infrastruktury Krytycznej, s. 26.

1.3 POJĘCIE INFRASTRUKTURY BEZPIECZEŃSTWA I OBRONNOŚCI

Infrastrukturę bezpieczeństwa i obronności można definiować poprzez odniesienie jej do zamówień w dziedzinie obronności i bezpieczeństwa, określonych w art. 7 pkt 36 Ustawy Prawo zamówień publicznych. Zgodnie z tym przepisem, do zamówień w dziedzinie obronności i bezpieczeństwa, zaliczają się zamówienia, których przedmiotem są:

- dostawy sprzętu wojskowego, w tym wszelkich jego części, komponentów, podzespołów lub oprogramowania;
- dostawy, usługi i roboty budowlane bezpośrednio związane ze sprzętem wojskowym w którejkolwiek z faz jego cyklu życia;
- usługi przeznaczone wyłącznie do celów wojskowych;
- roboty budowlane przeznaczone wyłącznie do celów wojskowych.
- dostawy newralgicznego sprzętu, w tym wszelkich jego części, komponentów, podzespołów lub oprogramowania;
- dostawy, usługi i roboty budowlane bezpośrednio związane z newralgicznym sprzętem w którejkolwiek z faz jego cyklu życia;
- newralgiczne usługi;
- newralgiczne roboty budowlane.

Newralgiczny sprzęt, newralgiczne usługi i newralgiczne roboty budowlane definiowane są (zgodnie z art. 7 pkt 11-13 Ustawy Prawo zamówień publicznych) jako odpowiednio, sprzęt, usługi i roboty budowlane przeznaczone do celów bezpieczeństwa, które:

- wiążą się z korzystaniem z informacji niejawnych lub informacji podlegających ochronie ze względów bezpieczeństwa;
- wymagają wykorzystania informacji niejawnych lub informacji podlegających ochronie ze względów bezpieczeństwa

lub

- zawierają informacje niejawne, lub informacje podlegające ochronie ze względów bezpieczeństwa.

Przez sprzęt wojskowy (zgodnie z art. 7 pkt 22 Ustawy Prawo zamówień publicznych) należy rozumieć wyposażenie specjalnie zaprojektowane lub zaadaptowane do potrzeb wojskowych i przeznaczone do użycia jako broń, amunicja lub materiały wojenne.

Tego rodzaju zakupy i projekty infrastrukturalne ze względu na zapewnienie bezpieczeństwa interesu państwa, nie są przedmiotem niniejszego raportu.

1.4 POJĘCIE INFRASTRUKTURY TYPU *DUAL-USE*

W niniejszym raporcie to pojęcie będzie odnosiło się do trwałej infrastruktury, która zapewnia bezpieczeństwo osób i mienia. W sposób naturalny zatem pojęcie to odnosi się do również do infrastruktury krytycznej, jednak dla celów niniejszego opracowania obejmuje przede wszystkim zakres infrastruktury, który nie jest w niej ujęty. Chodzi przede wszystkim o schrony oraz szeroko pojętą infrastrukturę, która może pełnić funkcję zapewnienia bezpieczeństwa podczas wojny, przy uwzględnieniu odpowiedniego sposobu jej zaprojektowania a także budowy i zarządzania tak, aby spełniała podwójną funkcję. Do tego rodzaju infrastruktury można zaliczyć m.in.: obiekty użyteczności publicznej, obiekty sportowe (hale sportowo-widowiskowe oraz stadiony), czy parkingi. Istotne jest jednak takie zaprojektowaniei wybudowanie obiektów, aby w razie zagrożenia co najmniej w części, mogły służyć miejscowej ludności jako schronienie, pełnić funkcje ratownicze (szpitalne) czy magazynowe.

Podkreślenia wymaga, że zagadnienie infrastruktury typu *dual-use* w rozumieniu trwałej infrastruktury mogącej spełniać równocześnie funkcje cywilne i wojenne, nie jest uregulowane prawnie. Gdzieniegdzie w ustawach pojawiają się regulacje dotyczące schronów (jak np. w rozporządzeniu Ministra Infrastruktury z dnia 24 czerwca 2022 r. w sprawie przepisów techniczno-budowlanych dotyczących dróg publicznych), jednak pojęcie schronu nie jest zdefiniowane prawnie. Obecnie jedynym aktem urzędowym, który określa wymagania techniczne dla schronów i ukryć są „Warunki techniczne, jakim powinny odpowiadać budowle ochronne" stanowiące załącznik nr 1 do wytycznych Szefa Obrony Cywilnej Kraju z 4 grudnia 2018 r. w sprawie zasad postępowania z zasobami budownictwa ochronnego. Nie ma on mocy wiążącej, a stanowi jedynie wskazówki w jaki sposób ewidencjonować budowle i budynki ochronne. Zalicza do nich m.in. garaże wielostanowiskowe (parkingi), piwnice budynków czy podziemne stacje metra.

Jak widać z konfliktu zbrojnego, który od 24 grudnia 2022 r. toczy się za wschodnią granicą Polski, oprócz działań wojennych, z wielkim natężeniem prowadzone są przez agresora ataki na ludność cywilną. Efektem tego jest niszczenie z premedytacją (poprzez ostrzały rakietowe i bombardowania) infrastruktury miejskiej w miastach, które jednocześnie zapewniają ludności podstawowe potrzeby i umożliwiają przeżycie – jedzenie i wodę, energię, łączność, schronienie.

Z tej sytuacji należy wyciągnąć poważne i mające dalekosiężny wpływ na planowanie projektów infrastrukturalnych, wnioski w zakresie konieczności uwzględnienia funkcjonowania infrastruktury zarówno w czasie pokoju, jak i możliwości wykorzystania jej w razie wojny. Koncepcja *dual-use* wydaje się odpowiedzią na to wyzwanie, ponieważ nakazuje ona spojrzeć na otaczającą nas rzeczywistość w sposób bardziej złożony, poprzez ocenę możliwości wykorzystania określonego obiektu w celach tak cywilnych, jak i wojskowych[13]. Należy przy tym zastrzec, że niniejszy raport wpisuje się dopiero w początek dyskusji na temat podwójnych celów przeznaczania infrastruktury, przy czym Autorzy mają nadzieję, że temat ten, ze względu na swoją wagę, będzie rozwijany i znajdzie swoje praktyczne zastosowanie.

W bezpośrednim tłumaczeniu *dual-use* oznacza „podwójne zastosowanie" i jest używane w różnych kontekstach znaczeniowych. Dopiero od niedawna przywołuje się pojęcie *dual-use* do planowania inwestycji, co – uwzględniając interes publiczny i podstawy realizowania zadań publicznych przez administrację w sposób efektywny, gospodarny, racjonalny i skuteczny – jest jak najbardziej uzasadnione. Ten rodzaj podejścia do długoletniego planowania inwestycyjnego powinien zostać wdrożony na stałe jako prawny obowiązek

13 Por. J.H. Szlachetko „Podejście *dual-use* w planowaniu przestrzennym jako strategia na wypadek konfliktu zbrojnego", Samorząd Terytorialny, 2022 r., nr 10, s. 37.

uregulowany ustawowo i stać się obowiązkowym kryterium dla podmiotów administracyjnych w zakresie przygotowania przedsięwzięć inwestycyjnych.

Koncepcja *dual-use* odnosi się również do stanu prawnego obiektów, które miałyby mieć podwójne przeznaczenie cywilno-wojenne. W tym podejściu autorów nie chodzi bowiem wyłącznie o inwestycje publiczne, jak te, o których mowa w art. 2 pkt 5 Ustawy o planowaniu i zagospodarowaniu przestrzennym, w tym np. obiekty użyteczności publicznej, obiekty sportowe, dworce, stacje metra, drogi[14], ale również o infrastrukturę prywatną (biurowce, galerie handlowe), a także publiczno-prywatną, która łączy obiekty o przeznaczeniu publicznym wraz z obiektami komercyjnymi i pozostaje w zarządzaniu publiczno-prywatnym (np. infrastruktura powstała w formule PPP: instalacja przetwarzania odpadów w Olsztynie, czy w Poznaniu, zrewitalizowane obiekty dworca PKP oraz budynki przydworcowe w Sopocie, wielopoziomowy parking w Warszawie, czy rozbudowa linii tramwajowej w Krakowie).

Warto przy tym zaznaczyć, że nie chodzi o zmianę funkcji danego obiektu w przypadku zaistnienia takiej konieczności, jak miało to miejsce np. w przypadku obiektów sportowych podczas pandemii covid-19 i przeznaczenia ich doraźnie na szpitale polowe dla ludności. Istotne jest wdrożenie całościowego podejścia do planowania, projektowania i budowy infrastruktury, mającego na celu podwójne funkcje: do wykorzystania cywilnego i wojskowego. Np. w przypadku obiektu szkoły – budynek ten powinien mieć możliwość pełnienia funkcji schronu, ale również np. szpitala, czy magazynu (w zależności od strategii zarządzania kryzysowego). Zatem powinien mieć dodatkowe, o odpowiedniej konstrukcji, pomieszczenia mogące wytrzymać atak rakietowy lub bombowy, o odpowiednich instalacjach i wyposażeniu (środki opatrunkowe), a także o odpowiedniej wielkości powierzchni.

Takie całościowe podejście do inwestycji wiąże się z koniecznością wprowadzenia do systemu prawnego norm, dotyczących parametrów technicznych takich obiektów w zakresie oświetlenia, doprowadzenia instalacji, wysokości i szerokości pomieszczeń, wytrzymałości, itd.

Rodzaj funkcji uzupełniających z przeznaczeniem dla ludności cywilnej i wspomagająco dla wojska, jakie mogłaby posiadać infrastruktura o przeznaczeniu *dual-use*, prezentuje poniższa tabela.

TAB. 2. **RODZAJ FUNKCJI UZUPEŁNIAJĄCYCH Z PRZEZNACZENIEM DLA LUDNOŚCI CYWILNEJ I WSPOMAGAJĄCO DLA WOJSKA, JAKIE MOGŁABY POSIADAĆ INFRASTRUKTURA O PRZEZNACZENIU *DUAL-USE***

FUNKCJA UZUPEŁNIAJĄCA	RODZAJ INFRASTRUKTURY
schron	budynki użyteczności publicznej; parkingi podziemne; biurowce; hotele; szkoły; domy opieki; galerie handlowe; przejścia podziemne; dworce; stacje metra
magazyn	budynki użyteczności publicznej; szkoły; domy opieki; parkingi podziemne
alternatywne drogi transportowe	drogi ekspresowe; autostrady; lotnicze pasy startowe
szpital	obiekty szpitalne; uzupełniająco szkoły; hotele i/lub inne obiekty kubaturowe

Źródło: opracowanie własne.

14 Por. J.H. Szlachetko, op. cit., s. 38 i n.

Obecnie o „podwójnej funkcji" obiektów jest mowa w dokumencie pt. „Warunki techniczne, jakim powinny odpowiadać budowle ochronne" stanowiący załącznik nr 1 do wytycznych Szefa Obrony Cywilnej Kraju z 4 grudnia 2018 r. w sprawie zasad postępowania z zasobami budownictwa ochronnego. W §71 wprowadzono zalecenie, aby budowle ochronne, z wyłączeniem obiektów specjalnego przeznaczenia (np. stanowisk kierowania, magazynów sprzętu ochrony cywilnej), użytkować jako obiekty pozostające w ciągłym użyciu w podwójnej funkcji: np. przejścia podziemne, komórki lokatorskie, sale zebrań, magazyny, szatnie, świetlice, obiekty kulturalne, sportowe, handlowe, szkoleniowe i inne. W niniejszym raporcie autorzy zwracają uwagę, aby planowane inwestycje z góry uwzględniały zadania ochronne dla ludności, w tym pełniły funkcje uzupełniające na wypadek wojny.

W związku z powyższym, zasadniczym wyzwaniem jest systemowe podejście do tej kwestii, opierające się na trzech filarach decyzyjnych:

1. przyjęcie podejścia *dual-use* w zakresie planowanej oraz projektowanej i budowanej infrastruktury;

2. określenie możliwości finansowych jednostek samorządu terytorialnego na realizację tego typu przedsięwzięć, biorąc pod uwagę sytuację gospodarczo-ekonomiczną oraz ograniczone możliwości wydatkowania środków publicznych, a także możliwość skorzystania z formuły partnerstwa publiczno-prywatnego;

3. opracowanie strategii działania w sytuacji zagrożenia wojennego, uwzględniającej zaprojektowanie i budowę obiektów użyteczności publicznej z uwzględnieniem funkcji przydatnych na wypadek wojny.

Autorzy prezentowanego raportu skupią się przede wszystkim na dwóch pierwszych punktach.

2. PARTNERSTWO PUBLICZNO-PRYWATNE

2.1 CHARAKTERYSTYKA PARTNERSTWA PUBLICZNO-PRYWATNEGO

Partnerstwo publiczno-prywatne stanowi formułę realizacji inwestycji (gminnych, powiatowych, wojewódzkich, rządowych) przez podmiot publiczny (np. jednostkę samorządu terytorialnego, rząd) przy udziale partnera prywatnego (najczęściej spółki celowej, rzadziej konsorcjum spółek). Współpraca ta charakteryzuje się włączeniem prywatnego partnera w realizację wieloetapowego przedsięwzięcia na zasadzie podziału zadań i ryzyk: za określone zadanie i ryzyka z nim związane odpowiada ta strona kontraktu, w której obszarze leżą kompetencje do wykonania określonych zadań oraz zarządzania ryzykami. Partner prywatny odpowiada zatem np. za zaprojektowanie, budowę i zarządzanie infrastrukturą, albo za budowę i utrzymanie obiektu. Na świecie znane są akronimy opisujące podstawowe etapy, w które zaangażowany jest partner prywatny, np.: BOT (*build-operate-transfer*), DBOFM *(design-build-operate-finance-maintenance).*

Wynagrodzenie partnera prywatnego jest płatne po zakończeniu etapu budowy i związane jest z dostarczaniem zakontraktowanych usług, tzn. jeśli usługi nie są dostarczane na umówionym poziomie, wówczas wynagrodzenie nie jest wypłacane albo obniżane zgodnie z postanowieniami umowy. Zgodnie z Ustawą o PPP, wynagrodzenie partnera prywatnego zależy od wykorzystania lub dostępności infrastruktury, za której utrzymanie, zarządzanie, czy eksploatację odpowiada partner prywatny. Oznacza to, że w przypadku infrastruktury, za pomocą której może być generowany dochód, partner prywatny może prowadzić działalność, z której środki pozwolą mu na częściowy zwrot zaangażowanego kapitału. Są takie projekty, jak np. wielopoziomowy parking przy Placu Powstańców Warszawy w Warszawie, które powstają w formule koncesji na roboty budowlane bez jakiegokolwiek zaangażowania finansowego ze strony podmiotu publicznego. Prognozy finansowe i oferta partnera prywatnego potwierdziły, że projekt będzie mógł być finansowany z opłat za parkowanie, które będzie pobierał partner prywatny, jednak parking przez okres trwania projektu będzie własnością miasta stołecznego Warszawy.

Innego rodzaju projektami są przedsięwzięcia, które ze swojej natury nie generują przychodów (jak np. drogi, za które nie są pobierane opłaty, budowa i zarządzanie obiektami kubaturowymi, zakup i utrzymanie sprzętu albo innego rodzaju infrastruktury), albo mogą uzyskać je jedynie w niewielkim stopniu (np. obiekty użyteczności publicznej z lokalami towarzyszącymi na wynajem). Do tej grupy inwestycji należą również przedsięwzięcia łączone, których infrastruktura powstała w ramach jednego przedsięwzięcia i posiada w części charakter publiczny, a w części komercyjny. W zakresie tych projektów inwestycyjnych podmiot publiczny jest włączony w zapewnienie, co najmniej w części, wynagrodzenia partnerowi publicznemu.

W ramach PPP prowadzone są również inwestycje poprzez spółki prawa handlowego z udziałem podmiotów publicznych, instytucji finansujących oraz partnerów prywatnych.

Umowa z partnerem prywatnym zawierana jest po przeprowadzeniu kilkuetapowego postępowania przygotowawczego oraz po zakończeniu postępowania na wybór partnera prywatnego. W ramach przygotowań do projektu przez podmiot publiczny, konieczne jest opracowanie oceny efektywności (art. 3a Ustawy o PPP) potwierdzającej, że formuła PPP stanowi najbardziej efektywny wariant realizacji danego przedsięwzięcia oraz przeprowadzenie wstępnych konsultacji rynkowych (art. 83 Ustawy Prawo zamówień publicznych), pozwalających na pozwalających na wstępne rozmowy z zainteresowanymi prywatnymi firmami co do zakresu, możliwości technologicznych i technicznych, sfinansowania i innych aspektów planowanego

przedsięwzięcia. W przypadku podjęcia decyzji o kontynuowaniu projektu w formule PPP, następny etap stanowi opracowanie projektów dokumentacji (w tym umowy o PPP) oraz przygotowanie postępowania dotyczącego wyboru partnera prywatnego. Jest ono prowadzone na podstawie art. 4 ustawy o PPP, najczęściej w trybie dialogu konkurencyjnego zgodnie z Ustawą Prawo zamówień publicznych. W przypadku wyboru partnera prywatnego do współpracy w zakresie infrastruktury bezpieczeństwa i obronności należy uwzględnić przepisy Ustawy Prawo zamówień publicznych odnoszące się do tego rodzaju zamówień.

Z infrastrukturą obronności i bezpieczeństwa związane są ograniczenia stosowania przepisów Ustawy Prawo zamówień publicznych, o których mowa w art. 13 Ustawy Prawo zamówień publicznych. Dotyczy to m.in. zamówień, którym nadano klauzulę niejawności, jeśli wymaga tego istotny interes bezpieczeństwa państwa, czy podlegających szczególnym procedurom. Z tego też względu tego rodzaju zamówienia, samodzielnie podlegające wyłączeniu spod przepisów Ustawy Prawo zamówień publicznych, w dalszej części raportu nie będą brane pod uwagę.

Do wyboru wykonawcy stosuje się tryb przetargu nieograniczonego, negocjacji z ogłoszeniem, negocjacji bez ogłoszenia albo dialogu konkurencyjnego. W wyjątkowych przypadkach można zastosować tryb zamówienia z wolnej ręki[15].

2.2 MOŻLIWOŚCI REALIZACJI I FINANSOWANIA INFRASTRUKTURY BEZPIECZEŃSTWA W FORMULE PPP

Dla realizacji projektów PPP, szczególnie jeśli chodzi o tak newralgiczną infrastrukturę, jaką jest infrastruktura bezpieczeństwa, istotne jest wsparcie tej formuły przez podmioty administracji rządowej, w tym Radę Ministrów oraz stabilne otoczenie prawne, zapewniające jasne i przejrzyste zasady wdrażania tego rodzaju przedsięwzięć, a także wytyczne w zakresie standardów stosowanych przy ich przygotowaniu i realizacji.

Jeśli chodzi o wsparcie rozwoju PPP w Polsce, obowiązująca Polityka PPP wyraża całościową politykę państwa w zakresie zaaprobowania partnerstwa publiczno-prywatnego jako narzędzia realizacji zadań w zakresie przedsięwzięć infrastrukturalnych tak na poziomie rządowym, jak i samorządowym. Dokument ten jest komplementarny ze Strategią na rzecz Odpowiedzialnego Rozwoju[16], która identyfikuje potrzebę włączenia w realizację zadań publicznych posiadanego przez sektor prywatny oraz kapitału prywatnego, doświadczenia w zarządzaniu i utrzymywaniu infrastruktury oraz przygotowaniu i realizacji projektów. Partnerstwo publiczno-prywatne, obok partnerstwa inwestycyjnego z samorządami, rozwoju rynku venture capital w Polsce oraz rozwoju zrównoważonego terytorialnie, ze szczególnym uwzględnieniem specjalnych stref ekonomicznych, zostało określone jako obszar priorytetowy dla Rządu jakokorzystanie z nowych instrumentów rozwoju[17].

Polityka PPP jest również wyrazem działania Rządu zapowiedzianym w Strategii na rzecz Odpowiedzianego Rozwoju, w celu wsparcia podmiotów publicznych przy wykorzystywaniu tej formuły przeprowadzania inwestycji.

Polityka PPP jest cały czas aktualizowana, odbywają się konsultacje z podmiotami publicznymi, partnerami prywatnymi oraz ekspertami w zakresie opracowania wytycznych odpowiadających na coraz to nowe

15 Art. 415 i n. Ustawy Prawo zamówień publicznych.

16 Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.), przyjęta uchwałą Rady Ministrów w dniu 14 lutego 2017 r., https://www.gov.pl/web/fundusze-regiony/informacje-o-strategii-na-rzecz-odpowiedzialnego-rozwoju (dostęp 28.02.23 r.).

17 Strategia na rzecz Odpowiedzialnego Rozwoju, op. cit., s. 2.

wyzwania. Odzwierciedleniem założeń opisanych w Polityce PPP są wytyczne opracowane przez MRiPR w zakresie kolejnych etapów przygotowania i realizacji projektów PPP[18].

Obecnie wypromowanie idei partnerstwa publiczno-prywatnego poprzez ukazanie praktycznych zalet współpracy między sektorem publicznym i prywatnym oraz identyfikacje i realizację wspólnych celów interesów sektora publicznego i prywatnego przewiduje również m.in. NPOIK. Podkreśla on m.in. wypromowanie idei partnerstwa publiczno-prywatnego za pomocą pokazania praktycznych zalet współpracy między sektorem publicznym i prywatnym oraz identyfikację i realizację wspólnych interesów sektora publicznego i prywatnego.

Jednym z elementów zarządzania kryzysowego związanego ochroną infrastruktury krytycznej jest współpraca administracji publicznej z biznesem. Według Rządowego Centrum Bezpieczeństwa to jeden z kluczowych elementów zapewniających sprawną i całościową ochronę infrastruktury krytycznej, szczególnie, że część infrastruktury krytycznej pozostaje w rękach prywatnych. Celem w tym kontekście jest wypracowanie przejrzystych zasad i procedur między administracją a właścicielami obiektów, instalacji lub urządzeń infrastruktury krytycznej.

Formułą współpracy sektora prywatnego z sektorem państwowym jest forum publiczno-prywatne, które zajmuje się kwestiami związanymi z ochroną infrastruktury krytycznej. W ramach prac Forum utworzono mechanizm ochrony infrastruktury krytycznej, którego celem jest m.in. wsparcie koordynacji działań w przypadku zniszczenia lub zakłócenia funkcjonowania infrastruktury, a także udzielanie przez podmioty administracji publicznej wsparcia merytorycznego (doradztwo, szkolenia) w zakresie fizycznej i informatycznej ochrony obiektów, jak również w zakresie funkcjonowania wewnętrznych mechanizmów ochrony infrastruktury krytycznej i zarządzania kryzysowego.

Warto zwrócić uwagę, że NPOIK w ramach *Standardów służących zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, wskazał rekomendacje w zakresie umów zawieranych z podmiotami zewnętrznymi, w tym m.in.:[19]

- wzięcie pod uwagę przy wyborze usługodawcy jego bieżącej sytuacji finansowo-ekonomicznej oraz zbadanie struktury właścicielskiej, łącznie z identyfikacją beneficjentów rzeczywistych;
- rozpoczęcie każdej relacji z nowym partnerem od zawarcia umowy o zachowanie poufności (umowa taka powinna gwarantować realne sankcje w przypadku jej naruszenia);
- precyzyjne opisanie przedmiotu umowy tak, aby zminimalizować ryzyko obszarów, które nie zostały przypisane wyraźnie do jednej ze stron;
- opisanie w umowie oczekiwanego zakresu współpracy usługodawcy, w tym osób trzecich działających na jego rzecz, współuczestniczących w świadczeniu usługi z operatorem infrastruktury krytycznej w sytuacji usuwania awarii (zakres ten powinien obejmować m.in.: udostępnianie określonej infrastruktury, personelu i gotowości tego personelu do działania);

18 https://www.ppp.gov.pl/wytyczne/ [dostęp: 9.03.2023 r.].

19 Załącznik nr 1 do NPOIK „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje", s. 113-115, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 4.03.2023 r.].

- zawarcie w umowie na dostawę lub obsługę serwisową oprogramowania, postanowień dotyczących procedury zarządzania zmianami w tym oprogramowaniu oraz sposobu ustalania wynagrodzenia usługodawcy z tego tytułu;

- określenie w umowie mechanizmów sankcyjnych, nadających operatorowi infrastruktury krytycznej uprawnień finansowych (np. potrącenia, kary umowne) lub rozwiązania umowy w przypadku naruszenia zobowiązań przez dostawcę;

- brak w umowie postanowień całkowicie wyłączających odpowiedzialność dostawcy lub ograniczających jego odpowiedzialność do kwot nieodpowiadających ryzyku związanemu z dostarczeniem produktu lub usługi niespełniających warunków zamówienia;

- opisanie w umowie sformalizowanej ścieżki eskalacji w rozwiązywaniu problemów powstałych na gruncie realizacji umowy, w tym procedury umożliwiającej podjęcie natychmiastowych działań w przypadku zagrożeń dla infrastruktury krytycznej wynikających z ataków na infrastrukturę informatyczną;

- zawarcie w umowie zasad zlecania podwykonawcom poszczególnych czynności wraz z wymogiem stosowania równorzędnych zabezpieczeń, wynikających z zawartej umowy głównej.

Konieczność rozważenia stosowania formuły PPP do realizacji projektów *dual-use* wydaje się obecnie oczywista. Z jednej strony zbrojna agresja Rosji przeciw Ukrainie ukazała, jak ważna jest zmiana podejścia do projektowania i realizacji infrastruktury publicznej oraz konieczności planowania nowej infrastruktury, czy modernizacji obecnej, z uwzględnieniem doświadczeń płynących z Ukrainy. Z drugiej strony, dynamiczna sytuacja i związane z nią obciążenia budżetów jednostek samorządu terytorialnego, wymuszają konieczność szybkiej zmiany podejścia – nastawienia na optymalizację wydatków oraz na osiągnięcie korzyści mierzonych niższymi wydatkami bieżącymi. Trudno sobie bowiem wyobrazić, że infrastrukturę typu parkingi podziemne, szkoły, będzie budowało państwo, nawet wówczas, gdy obiekty te będą miały podwójne zastosowanie.

Z punktu widzenia podmiotów publicznych, zważywszy, jaka jest budowa indywidualnego wskaźnika zadłużenia jednostek samorządu terytorialnego po nowelizacji ustawy o finansach publicznych, konieczność przedefiniowania formuły realizacji inwestycji staje się bardziej niż pilna, w szczególności, jeśli realizacja nowych inwestycji typu *dual-use* wiązałaby się z wyższymi kosztami. W innym przypadku zabraknąć może czasu na wprowadzenie zmian, przygotowanie projektów do wdrożenia w formule PPP i zachowanie realizacji projektów w ogóle.

W przypadku infrastruktury, będącej tematem niniejszego raportu, warto zwrócić uwagę na aspekty, które nabierają obecnie fundamentalnego znaczenia. Pierwszy jest znany jednostkom samorządu terytorialnego w Polsce, choć ciągle stosowany w niewystarczającym stopniu, czyli konieczność zoptymalizowania wydatków majątkowych, innego ich rozłożenia w czasie w powiązaniu ze zoptymalizowaniem wydatków bieżących, które będą z tych inwestycji w okresie ich eksploatacji wynikać. Drugi, to zwrócenie uwagi na koszty i jakość utrzymania projektów typu *dual-use* tak, aby zapewnić optymalny standard utrzymania i wykorzystania. Powyższe dwa aspekty przenikają się, bowiem partner prywatny może mieć wpływ na optymalizację wydatków, a dzięki jego kompetencjom możliwe będzie efektywne zarządzanie infrastrukturą, prowadzące do obniżenia wydatków bieżących.

W ramach omawianych przedsięwzięć mamy do czynienia z bardzo szerokim zakresem możliwych do wspólnej realizacji inwestycji: począwszy od projektów pełniących niezbędne funkcje miejskie, które mogą być

realizowane bez jakiegokolwiek wynagrodzenia ze strony podmiotu publicznego jak np. obiekty rewitalizowane czy parkingi (niektóre z nich, jak pokazał przykład warszawski, mogą być zrealizowane w takiej formule), aż po koncesje na usługi, projekty rewitalizacji miast (albo ich części) i wygenerowanie działalności komercyjnej, inwestycje synergiczne (połączenie funkcji publicznych oraz komercyjnych). Przy czym należy pamiętać, iż w obecnej sytuacji pozycja negocjacyjna strony publicznej będzie osłabiona z powodu ryzyka, związanego z komercjalizacją przestrzeni przez partnera prywatnego w najbliższym czasie.

W przypadku drugiego rodzaju przedsięwzięć możemy mówić o tych, które muszą być zrealizowane, a zapłatę za nakłady inwestycyjne można rozłożyć w czasie w formule opłaty za dostępność, po oddaniu tych inwestycji do użytku. PPP w tym przypadku może być alternatywą właśnie dzięki innemu ukształtowaniu struktury wydatków majątkowych, przy czym korzyść dla budżetu będzie dotyczyć przede wszystkim planowanych, a jeszcze nie rozpoczętych inwestycji. Z kolei w przypadku zupełnie nowych projektów, nie ujętych w prognozie finansowej, korzyści mogą pojawić się przy przedefiniowaniu istniejących projektów i włączeniu nowych do realizacji w tej formule. W tym kontekście możemy mówić nie tylko o inwestycjach samorządowych, ale także rządowych, projektach drogowych, projektach obejmujących budowę szkół, przedszkoli, dróg gminnych czy każdej innej planowanej i niezbędnej infrastruktury.

W przypadku projektów inwestycyjnych sektora samorządowego, które mogłyby mieć podwójne zastosowanie, a ich przeformułowanie w tym kierunku wiązałoby się z poniesieniem wyższych nakładów inwestycyjnych i wyższych kosztów bieżących, niż w przypadku wyłącznie podstawowego celu ich realizacji, możliwe jest rozważenie formuły PPP, gdzie jednostka samorządu terytorialnego uzyskuje wsparcie finansowe dla takich projektów ze strony Skarbu Państwa lub projekt jest wspólnie zamawiany przez jednostkę samorządu terytorialnego i Skarb Państwa. Dotyczy to w szczególności projektów opartych o opłatę za dostępność, jako modelu wynagradzania partnera prywatnego. Uwzględnienie strumienia środków z budżetu Państwa w przypadku realizacji infrastruktury samorządowej o przeznaczeniu *dual-use*, w związku z kondycją finansową samorządów oraz z uwzględnieniem długofalowych efektów formuły PPP w cyklu życia projektu – jakości utrzymania infrastruktury, mogłoby wpłynąć korzystnie na przyspieszenie realizacji lub modernizacji infrastruktury, która może mieć podwójne zastosowanie.

W zakresie inwestycji, które mają spełniać podwójną rolę – użytkowania w trakcie pokoju i na wypadek wojny – udział partnera prywatnego będzie coraz bardziej niezbędny ze względu na podstawową wartość dodaną, która będzie wynikała z partnerstwa: wniesienie *know-how*, zapewnienia nowych technologii, utrzymania i serwisu infrastruktury technicznej, wymagającej bieżącego dostępu do wysokokwalifikowanej kadry technicznej. Kluczowym wyzwaniem jest właściwe zdefiniowanie potrzeb, które mają być zapewnione w połączeniu ze świadomością konieczności optymalizacji wydatków bieżących, w przeciwnym razie pojawi się silne dążenie do stosowania formuły tradycyjnej i rozrostu struktur administracji lub spółek komunalnych.

Już dzisiaj widać zwiększone zainteresowanie firm prywatnych, poszukujących możliwości wejścia w przedsięwzięcia o potencjale długofalowej i stabilnej współpracy. Umożliwi to realizację projektów niezbędnych, z punktu widzenia zaspokojenia potrzeb mieszkańców poszczególnych szczebli samorządu, takich jak: obiekty kubaturowe, projekty rewitalizacyjne i budownictwo komunalne, które nie finansują się samodzielnie i opierają się na rozłożonym w czasie wynagrodzeniu płaconym przez podmiot publiczny (w formie opłaty za dostępność).

W obliczu ewentualnej recesji, możemy spodziewać się zwiększonego zainteresowania tego rodzaju przedsięwzięciami i stosunkowo większej elastyczności obydwu stron (publicznej i prywatnej) w trakcie prowadzonych negocjacji, o ile sektor publiczny jaki i przedsiębiorcy prywatni współpracujący z nim, zdadzą sobie sprawę, że PPP daje im możliwość działania.

2.3 SZANSE I ZAGROŻENIA ZWIĄZANE Z WYKORZYSTANIEM PPP DO BUDOWY I UTRZYMANIA INFRASTRUKTURY ZAPEWNIENIA BEZPIECZEŃSTWA

Mając na względzie doświadczenia w zakresie stosowanie formuły PPP przy różnego rodzaju przedsięwzięciach infrastrukturalnych w Polsce, w tym rekomendacje zawarte w NPOIK w zakresie współpracy z partnerami prywatnymi, a także raport NATO na temat doświadczeń w zakresie zastosowania formuły PPP w inwestycjach, związanych z wojskowością[20], należy przeanalizować szanse i zagrożenia wynikające z zastosowania tej koncepcji. W raporcie zarekomendowano każdorazowo przeprowadzenie analizy w zakresie możliwości wykorzystania formuły PPP i wskazano trzy główne czynniki kluczowe dla tego rodzaju współpracy:

- odpowiedni podział zadań i ryzyk;
- pomiar terminowości wykonywania zobowiązań przez każdą ze stron;
- ustalenie odszkodowań i kar w przypadku niewłaściwego wykonania zobowiązań.

Podkreślono również zwrócenie szczególnej uwagi zarówno na etap zawarcia, jak i zmiany umowy o PPP, w ramach której partner prywatny posiada istotne znaczenie albo doświadczenie związane z realizacją projektów w zakresie infrastruktury zapewnienia bezpieczeństwa[21].

Istotne są również wskaźniki efektywności, czyli tzw. KPI (*key performance indicators*), które określają skuteczność poszczególnych działań partnera prywatnego w trakcie obowiązywania umowy o partnerstwie publiczno-prywatnym. Mierniki te powinny być szczegółowo określone w kontrakcie a ich niedotrzymanie musi wiązać się z naliczeniem partnerowi prywatnemu punktów karnych albo kar umownych.

Szanse związane ze współpracą publiczno-prywatną:

- możliwość pozyskania finansowania dla projektu, którego nie można przeprowadzić z powodu braku środków w budżecie podmiotu publicznego;
- zapewnienie długoletniego zarządzania daną infrastrukturą, pozyskanie *know-how* w zakresie utrzymania tego rodzaju przedsięwzięć;
- podział odpowiedzialności za konkretne zadania i ryzyka a także zwiększona (w stosunku do całkowicie publicznego sposobu zrealizowania określonego przedsięwzięcia) szansa na osiągnięcie zakładanych rezultatów[22];
- PPP można rozważać w przedsięwzięciach, które są ustrukturowane w sposób jasny i mają zrozumiałe oraz racjonalne założenia organizacyjne i finansowe (są bankowalne);

20 NATO "Public Private Partnership in a NATO Context. Guidance on where Public Private Partnerships (PPP) have been successfully used by nations to provide or support military capabilities. Final Report of NATO SAS-112", 2019 r., https://www.sto.nato.int/publications/pages/results.aspx?k=ppp&s=Search%20All%20STO%20Reports [dostęp: 11.01.2023 r.].

21 Tamże s. 35.

22 Raport NATO, s.11.

- ryzyka w formule PPP należy przypisać stronie, której kompetencje pozwalają najlepiej zarządzać danym ryzykiem; natomiast należy wziąć pod uwagę, że niektóre rodzaje ryzyk (np. sukces operacyjny) nie mogą być przeniesione na partnera prywatnego.

Zagrożenia związane ze współpracą publiczno-prywatną:

- PPP nie zawsze jest rekomendowaną i najlepszą ścieżką do realizacji przedsięwzięcia; każdorazowo należy przeanalizować możliwość uzyskania efektywności i oszczędności (nie tylko finansowych) w zakresie PPP w stosunku do sytuacji, w której dany zakup byłby realizowany w formie tradycyjnej ze środków publicznych;

- przy projektach związanych w jakikolwiek sposób z realizacją infrastruktury zapewnienia bezpieczeństwa, należy uwzględnić ochronę interesu państwowego;

- im bardziej złożone projekty, tym trudniej jest podmiotowi publicznemu kontrolować jakość danej infrastruktury czy dostarczanych usług;

- w każdej sytuacji należy mieć na względzie to, że firmy prywatne będą zawsze dążyły do zmaksymalizowania swojego zysku, jeśli takie podejście jest do pogodzenia z oczekiwaniami publicznymi; przykładowo: w zakresie jak najszybszego terminu wykonania wówczas PPP można rozpatrywać jako sposób realizacji projektu; istnieje bowiem w sektorze publicznym tendencja do niedoszacowania czasu na dostarczenia danych rozwiązań, co na ogół powoduje istotny wzrost kosztów, nawet jeśli projekt jest realizowany bez udziału partnera prywatnego.

3. PROJEKTY PPP W ZAKRESIE INFRASTRUKTURY KRYTYCZNEJ ORAZ BEZPIECZEŃSTWA PLANOWANE I REALIZOWANE W POLSCE I NA ŚWIECIE

3.1 PROJEKT W POLSCE

W Polsce projekty PPP stanową niewielką część wszystkich realizowanych inwestycji infrastrukturalnych. Jak wynika z Raportu rynku PPP za lata 2009-2022, opublikowanego przez Ministerstwo Funduszy i Polityki Regionalnej (MFiPR), w 2022 roku zawarto jedynie 10 umów PPP o łącznej wartości ok. 270 ml zł, wśród których nie ma projektów w zakresie obronności. W opinii autorów wynika to przede wszystkim z długotrwałych procedur wyłaniania partnera prywatnego, przejęcia roli organizatora rynku przez MFiPR oraz niewystarczającego określenia i promocji zasad współpracy i realizacji projektów w formule partnerstwa publiczno-prywatnego.

Obecnie, w formule szeroko rozumianego PPP w zakresie infrastruktury zapewnienia bezpieczeństwa, planowany jest do realizacji obiekt ćwiczeniowo-szkoleniowy Wojsk Obrony Terytorialnej w Limanowej[23]. Przedsięwzięcie nie jest realizowane na podstawie Ustawy o PPP, jednak do jego przeprowadzenia wykorzystana jest spółka celowa, a finansowanie jest udzielone przez PFR.

Przedmiot inwestycji stanowi kompleks wojskowy na potrzeby 114. Batalionu Lekkiej Piechoty w Limanowej w ramach pododdziału 11. Małopolskiej Brygady Obrony Terytorialnej im. gen. bryg. Leopolda Okulickiego ps. „Niedźwiadek". Strona wojskowa zakłada, że liczba żołnierzy stacjonujących w jednostce będzie wynosić do 440 osób, w tym 390 żołnierzy terytorialnej służby wojskowej oraz 50 żołnierzy zawodowych. Kompleks wojskowy obejmie m.in.: budynek koszarowo-biurowy o powierzchni 8600 m^2, garaż dla pojazdów wojskowych (1700 m^2 powierzchni użytkowej) oraz pełną infrastrukturę. Całość zlokalizowana będzie na powierzchni ok. 12 ha. Szacowany koszt inwestycji ma wynieść ok. 100 mln zł. Przekazanie obiektu Wojskom Obrony Terytorialnej planowane jest na koniec 2024 roku.

Realizacja inwestycji będzie odbywała się na podstawie umowy zawartej w grudniu 2022 r. pomiędzy Ministerstwem Obrony Narodowej, Polskim Funduszem Rozwoju, Miastem Limanowa oraz spółką celową LimWOT. Spółka LimWOT jest spółką gminną, w której 100% udziałów należy do Miasta Limanowa[24]. Podstawowym celem, dla którego Spółka została zawiązana, jest, w ramach współpracy z jednostkami organizacyjnymi Skarbu Państwa na podstawie zamówienia na roboty budowlane w zakresie budowy kompleksu wojskowego, budowa na terenie Miasta Limanowa infrastruktury przeznaczonej dla Sił Zbrojnych RP. Finansowanie projektu zapewnia PFR.

23 Informacje o projekcie pochodzą ze strony: https://pfrsa.pl/aktualnosci/pfr-i-miasto-limanowa-inwestuja-w-budowe-koszar-wojsk-obrony-terytorialnej.html [dostęp: 27.02.2023 r.].

24 Informacje pochodzą z KRS spółki, który jest dostępny na stronie: https://ekrs.ms.gov.pl/web/wyszukiwarka-krs/strona-glowna/ oraz ze strony limwot.miastolimanowa.pl [dostęp: 27.02.2023 r.].

3.2 PROJEKTY NA ŚWIECIE

W raporcie NATO z 2019 r. wspomnianym powyżej zaprezentowano niektóre z projektów PPP opisanych w raporcie.

TAB. 3. **NIEKTÓRE Z PROJEKTÓW PPP OPISANYCH W RAPORCIE NATO**

PROJEKT 1.	**SYSTEM INFORMATYCZNY BUNDESWEHRY**
NAZWA PROJEKTU /ORGANIZACJA/KRAJ	Projekt HERKULES / Bundeswehra (armia niemiecka).
RODZAJ PARTNERSTWA PUBLICZNO-PRYWATNEGO	PPP na szczeblu rządowym.
ZAKRES PROJEKTU	Modernizacja, standaryzacja, konsolidacja i centralizacja niewojskowej infrastruktury informatycznej Bundeswehry oraz jej utrzymanie przez 10 lat (2006 – 2016). Planowana wartość: 7,1 mld euro (z podatkami).
WYMAGANE EFEKTY PROJEKTU	Niedrogi, niezawodny, wydajny, elastyczny i bezpieczny system informatyczny.
SPOSÓB WYBORU OFERTY	Brak danych, negocjacje przed oddaniem kontraktu trwały pięć lat.
ZREALIZOWANE KORZYŚCI	Chociaż donoszono, że koszty Herkulesa wzrosły o 700 milionów euro powyżej budżetu, po uwzględnieniu inflacji było to o 7% mniej, niż pierwotnie planowano [2]. Kontrakt został ukończony pod koniec 2016 roku, a BWI GmbH, spółka utworzona w celu realizacji kontraktu, stała się w 100% własnością niemieckiego rządu federalnego. Umowa umożliwiła dokonanie niezbędnych inwestycji początkowych, co byłoby trudne w publicznym procesie budżetowania rocznego.
CIEKAWOSTKI	Chociaż BWI GmbH jest obecnie w 100% własnością rządu federalnego, dopiero w ciągu najbliższych kilku lat okaże się, czy będzie w stanie utrzymać zarówno poziom umiejętności, jak i wielkość zasobów, a co za tym idzie, jak łatwo będzie Bundeswehrze utrzymywać i rozwijać swoje systemy informatyczne w przyszłości.

PROJEKT 2.	**SYSTEM RUCHU LOTNICZEGO**
NAZWA PROJEKTU /ORGANIZACJA/KRAJ	Brytyjskie Partnerstwo Publiczno-Prywatne (PPP) dla National Air Traffic Services Ltd (NATS).
RODZAJ PARTNERSTWA PUBLICZNO-PRYWATNEGO	PPP na szczeblu rządowym.
ZAKRES PROJEKTU	Utrzymanie bezpieczeństwa i bezpieczeństwa narodowego przy jednoczesnym zastrzyku finansowym sektora prywatnego oraz poprawa umiejętności zarządzania projektami, tak, aby sprostać oczekiwanemu przyszłemu wzrostowi ruchu lotniczego. Planowana wartość: blisko 800 mln funtów.
WYMAGANE EFEKTY PROJEKTU	Bezpieczny system ruchu lotniczego, który z jednej strony wymaga inwestycji niezbędnych do dostosowania się do jego przyszłego wzrostu, a z drugiej i chroni interesy podatnika.
SPOSÓB WYBORU OFERTY	Siedem firm wyraziło wstępne zainteresowanie, z czego cztery z nich wycofały się, powołując się na obawy dotyczące regulacji cen NATS. Finalnie na stole zostały oferty dwóch głównych rywali: Nimbus i Airline Group. Rząd wybrał ofertę Airline Group, która zaakceptowała więcej warunków rządowych, chociaż była mniej solidna finansowo. Koszty procesu licytacji i selekcji dla oferentów wyniosły około 30 milionów funtów, a rządu około 44 milionów funtów. Koszty rządowe były o 17 milionów funtów wyższe niż szacowano, głównie dlatego, że proces trwał 33 miesiące, a nie oczekiwane 18 miesięcy. Warto zauważyć, że analizy rządowe przyjęły optymistyczne założenia, że ruch lotniczy będzie stale wzrastał w przyszłości, mimo że w ciągu ostatnich trzydziestu lat były trzy przypadki, gdy nie było to prawdą.
ZREALIZOWANE KORZYŚCI	Rząd otrzymał 758 milionów funtów od zwycięskich oferentów i obecnie posiada 49% odnoszącego sukcesy biznesu, jakim stał się NATS. Wydaje się, że wymagane poziomy bezpieczeństwa i bezpieczeństwa narodowego zostały utrzymane.
CIEKAWOSTKI	W maju 2001 r., trzy miesiące po podpisaniu umowy handlowej, Airline Group poinformowała rząd, że zmniejszenie ruchu lotniczego oznacza, że nie stać ich na uzgodnioną cenę, która została obniżona o 87 mln GBP do 758 mln GBP. Wydarzenia z dnia 11 września 2001 r. spowodowały następnie pogorszenie ruchu lotniczego, które zmniejszyło dochody NATS, a także dochody linii lotniczych wchodzących w skład grupy Airlines, co ograniczyło ich zdolność do inwestowania w NATS. Zdolność NATS do przyciągania inwestycji zewnętrznych była również ograniczona przez pytania o jego zdolność do obsługi zadłużenia generowanego przez strukturę PPP. Dlatego konieczne było refinansowanie NATS. W tym celu pozyskano130 milionów funtów dodatkowych inwestycji: 50% od rządu i 50% od BAA (British Airports Authority -operator 6 brytyjskich lotnisk) Ta inwestycja, w połączeniu ze złagodzeniem cen, które NATS mógł pobierać od linii lotniczych, pozwoliła na refinansowanie w wysokości 600 milionów funtów w sierpniu 2003 r. Zaaranżowanie tej transakcji było trudne i trwało 18 miesięcy. W swoim badaniu brytyjska Narodowa Izba Kontroli zauważyła, że szczególnie ważne jest przetestowanie solidności PPP, zwłaszcza w odniesieniu do ryzyka, w przypadku którego kierownictwo nie może kontrolować występowania ryzyka, a jedynie ograniczać jego wpływ.

PROJEKT 3.	SYSTEM OBSERWACJI ZIEMI KOSMICZNEJ
NAZWA PROJEKTU /ORGANIZACJA/KRAJ	Hiszpańskie Ministerstwo Obrony (MON) i prywatny operator kosmiczny (HISDESAT).
RODZAJ PARTNERSTWA PUBLICZNO-PRYWATNEGO	PPP na szczeblu rządowym.
ZAKRES PROJEKTU	Opracowanie, zakup, uruchomienie i obsługa Systemu Obserwacji Ziemi Kosmicznej (SEOS: Spanish Earth Observation System). Planowana wartość: 110 mln €.
WYMAGANE EFEKTY PROJEKTU	System musiał spełniać wymagania operacyjne hiszpańskiego CHOD (szef obrony) oraz niektóre ulepszenia w operacyjnych trybach użytkowania na przyszłość lub następną generację. Umowa przemysłowa z kontrahentami z Niemiec.
SPOSÓB WYBORU OFERTY	Hiszpańskie Ministerstwo Obrony określiło ogólne wymagania, które definiowały oczekiwane wyniki. Agencja Acquisition wybrała podejście do zawierania umów i partnerów, aby spełnić wymagania. Hiszpański CHOD brał udział w odbiorze końcowym, przed oddaniem do eksploatacji.
ZREALIZOWANE KORZYŚCI	SEOS jest częścią Narodowego Programu Obserwacji Ziemi w Kosmosie, który dostarczył nowej koncepcji obserwacji Ziemi w dowolnym czasie i przy każdej pogodzie. Hiszpański przemysł kosmiczny podjął się pełnej integracji satelity, a jego operator korzysta z możliwości globalnego rozpoznania kosmosu, oprócz prymarnych możliwości komunikacyjnych. Siły Zbrojne otrzymają w ciągu najbliższych kilku miesięcy nową zdolność w systemach EOS (Earth Observation System).
CIEKAWOSTKI	Wstępne planowanie było częścią szerszego Narodowego Programu Kosmicznego. Operator rządowy musiał podjąć różne elementy rozwoju, integracji, wystrzelenia, przetestowania i walidacji działań na orbicie w propozycji przemysłowej. Podczas procesu produkcyjnego pojawiły się nowe możliwości ulepszenia systemów (przed krytycznym przeglądem projektu), aby uwzględnić nowe tryby operacyjne. Hiszpańska agencja ds. zakupów Ministerstwa Obrony musiała zarządzać hipotetycznymi kosztami ogólnymi. Tego rodzaju system wymaga ciągłej aktualizacji, przez cały cykl życia. Wszystkie te kwestie zostały pomyślnie rozwiązane w ramach umowy PPP.

PROJEKT 4.	HOTEL WOJSKOWY
NAZWA PROJEKTU /ORGANIZACJA/KRAJ	Łotewskie Ministerstwo Obrony i miejscowy hotelarz.
RODZAJ PARTNERSTWA PUBLICZNO-PRYWATNEGO	PPP na szczeblu rządowym.
ZAKRES PROJEKTU	Zapewnienie zakwaterowania w hotelu dla wizytującego personelu wojskowego i cywilnego łotewskich sił zbrojnych.
WYMAGANE EFEKTY PROJEKTU	Obniżone koszty zakwaterowania dla personelu wojskowego i urzędników służby cywilnej odwiedzających Rygę. Wzrost obrotów i zysków dla hotelarza.
SPOSÓB WYBORU OFERTY	Miejscowy hotelarz, który wcześniej służył w łotewskim wojsku, zauważył, że łotewskie Ministerstwo Obrony wydaje co roku znaczne kwoty na płacenie komercyjnych stawek za zakwaterowanie gości dyżurujących w lokalnych hotelach. Hotelarz zasugerował, aby Ministerstwo Obrony kupiło lokalny hotel i wymagało od gości korzystania z tego hotelu. Prowadziłby hotel, który byłby otwarty również dla gości spoza wojska, a zyski byłyby dzielone.
ZREALIZOWANE KORZYŚCI	Zmniejszone koszty dla łotewskiego Ministerstwa Obrony, zwiększone zyski dla hotelarza.

BIBLIOGRAFIA

M. Banasik, J. Bagińska *„Krytyczne uwagi dotyczące bezpieczeństwa infrastruktury krytycznej”*, Rocznik Bezpieczeństwa Międzynarodowego 2019 vol. 13, nr 2

Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32008L0114 [dostęp: 23.02.2023 r.]

Dyrektywa Parlamentu Europejskiej i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Ray 2008/114/WE, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2557 [dostęp: 23.02.2023 r.,], dalej „dyrektywa CER”

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) [dostęp: 23.02.2023 r.].

Komunikat Komisji w sprawie europejskiego programu ochrony infrastruktury krytycznej /* COM/2006/0786 końcowy, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52006DC0786&from=EN [dostęp: 23.02.2023 r.].

Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity (uchwała nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej z uwzględnieniem Uchwały nr 116/2020 Rady Ministrów z dnia 13 sierpnia 2020 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej), https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 27.02.2023 r.].

NATO “ Public Private Partnership in a NATO Context. Guidance on where Public Private Partnerships (PPP) have been successfully used by nations to provide or support military capabilities. Final Report of NATO SAS-112”, 2019 r., https://www.sto.nato.int/publications/pages/results.aspx?k=ppp&s=Search%20All%20STO%20Reports [dostęp: 11.01.2023 r.].

Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.), przyjęta uchwałą Rady Ministrów w dniu 14 lutego 2017 r., https://www.gov.pl/web/fundusze-regiony/informacje-o-strategii-na-rzecz-odpowiedzialnego-rozwoju (dostęp 28.02.23 r.).

J.H. Szlachetko *„Podejście dual-use w planowaniu przestrzennym jako strategia na wypadek konfliktu zbrojnego”*, Samorząd Terytorialny, 2022 r., nr 10

Uchwała Nr 116/2017 Rady Ministrów z dnia 26 lipca 2017 roku w sprawie przyjęcia dokumentu *„Polityka Rządu w zakresie rozwoju partnerstwa publiczno-prywatnego”*, aktualizowana

US Patriot Act. (2001, 26 października). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (US a Patriot Act) Act of 2001. Public Law No 107–56 (107th Congress)

Wytyczne dotyczące projektów partnerstwa publiczno-prywatnego https://www.ppp.gov.pl/wytyczne/ [dostęp: 9.03.2023 r.].

Zalecenie Rady Europejskiej z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej (2023/C 20/01), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32023H0120(01) [dostęp: 23.02.2023 r.], dalej jako „Zalecenie Rady”.

Załącznik nr 1 do NPOIK *„Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje”*, s. 113-115, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 4.03.2023 r.].

O AUTORACH

Agata Kozłowska

Prawniczka. Od 20 lat doradza przy projektach infrastrukturalnych w zakresie zamówień publicznych i PPP. Doradzała m.in. przy największych obecnie realizowanych projektach w Polsce, jak zaprojektowanie, budowa i utrzymanie instalacji przetwarzania odpadów w Olsztynie, a także przy projekcie koncesyjnym dotyczącym zaprojektowania, budowy i eksploatacji parkingu wielopoziomowego w Warszawie; rewitalizacji dworca PKP w Sopocie i przy projektach z zakresu modernizacji oświetlenia. Prowadzi szkolenia na temat PPP, koncesji i zamówień publicznych.

Autorka i współautorka książek na temat PPP i koncesji (w tym komentarzy do ustawy o PPP) oraz artykułów, analiz i raportów na ten temat. Brała udziałach w pracach nad projektami ustaw o PPP oraz o umowie koncesji na roboty budowlane lub usługi. Pełni rolę eksperta konsultującego założenia i aktualizacje Polityki Rządu w zakresie rozwoju partnerstwa publiczno-prywatnego. Członkini Ogólnopolskiego Stowarzyszenia Konsultantów Zamówień Publicznych.

Kacper Kozłowski

Ekonomista, menedżer. Posiada ekspertyzę w projektach inwestycyjnych. Koordynuje i prowadzi usługi doradcze na rzecz sektora publicznego i prywatnego ze szczególnym uwzględnieniem biznesowej i finansowej strony przedsięwzięć. Pracował przy projektach inwestycyjnych planowanych i realizowanych w formule PPP, m.in. w Warszawie, Krakowie, Łodzi, Poznaniu, Gdańsku, Szczecinie, Katowicach, Olsztynie, Sopocie i wielu innych oraz przy opracowaniu i wdrażaniu modeli zarządzania infrastrukturą komunalną.

Od ponad dwudziestu lat doradza przy projektach realizowanych w formule PPP. Prowadzi szkolenia na temat PPP, koncesji oraz finansowania, realizacji i zarządzania infrastrukturą.

Współautor artykułów i książek na zarządzania infrastrukturą, wdrażania PPP i koncesji oraz analiz i raportów na ten temat. Ekspert Polskiej Organizacji Branży Parkingowej oraz Instytutu Sobieskiego.

Absolwent Wydziału Zarządzania oraz Wydziału Dziennikarstwa i Nauk Politycznych na kierunku Polityka Społeczna Uniwersytetu Warszawskiego. Absolwent podyplomowych studiów z zakresu rynku nieruchomości oraz MBA.

Mając na względzie trwającą od ponad roku wojnę, będącą skutkiem napaści zbrojnej Rosji na Ukrainę, analizie poddano, z punktu widzenia form jej realizacji, zarówno infrastrukturę krytyczną, jak i obiekty, czy budynki, które mogą posłużyć wykorzystaniu na wypadek zagrożenia (obiekty infrastrukturalne o szerokim przeznaczeniu), a także infrastrukturę w zakresie obronności i bezpieczeństwa. Zapewnienie oraz eksploatacja (w tym utrzymanie, zarządzanie) tego typu infrastruktury wymaga niezwykle wysokich nakładów finansowych oraz wiedzy, które – w niektórych przedsięwzięciach – może zapewnić partner prywatny.

O zastosowaniu formuły partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa, w tym infrastrukturze krytycznej i obronności, dyskutuje się coraz częściej jednak ze względu na niewielką liczbę przeprowadzonych w tej formule projektów, coraz bardziej zaawansowany technicznie charakter tego rodzaju inwestycji, przy jednoczesnej konieczności zachowania tajemnicy państwowej oraz różnego rodzaju obawy, stosuje się ją rzadko. PPP pozwala jednak na osiągnięcie nowatorskich rozwiązań (szczególnie w zakresie technologicznym i informatycznym), a także rozłożenie finansowania przedsięwzięcia w długim okresie czasu.

Zdaniem autorów Raportu nadszedł czas na szczegółową analizę koncepcji PPP i zastanowienie się jak można ją wykorzystać dla realizacji i podjęcia działań w zakresie budowy i zarządzania szeroko rozumianą infrastrukturą, która mogłaby zostać wykorzystana w przypadku zagrożenia wojennego.

TWORZYMY IDEE DLA POLSKI

INSTYTUT SOBIESKIEGO

Instytut Sobieskiego
Lipowa 1a/20
00-316 Warszawa
tel.: 22 826 67 47

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

ISBN 978-83-966872-1-0

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO

NIW Narodowy Instytut Wolności

Sfinansowano ze środków Narodowego Instytutu Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego Rządowego Programu Rozwoju Organizacji Obywatelskich na lata 2018–2030 PROO

Rządowy Program Rozwoju Organizacji Obywatelskich na lata 2018–2030 PROO