dr Adam KRZYŻANOWSKI
Akademia Finansów i Biznesu Vistula, Warszawa,
Stowarzyszenie Badań nad Źródłami i Funkcjami Prawa FONTES
adamkrzy19@gmail.com
ORCID: 0009-0006-2977-8926

BEZPIECZEŃSTWO POWSZECHNE ORAZ NOWE WYZWANIA DLA OCHRONY LUDNOŚCI WOBEC ZŁOŻONYCH ZAGROŻEŃ XXI WIEKU: MIĘDZY REALNYM A WIRTUALNYM POLEM WALKI

PUBLIC SECURITY AND NEW CHALLENGES FOR POPULATION PROTECTION IN THE FACE OF COMPLEX THREATS OF THE 21ST CENTURY: BETWEEN THE REAL AND VIRTUAL BATTLEFIELD

Streszczenie

W artykule dokonano analizy transformacji bezpieczeństwa powszechnego i ochrony ludności w warunkach złożonych zagrożeń XXI wieku, w których granice między pokojem, kryzysem i wojną ulegają zatarciu, a pole oddziaływania obejmuje równolegle sferę realną i wirtualną. Punktem wyjścia jest teza, że skuteczność współczesnego systemu ochrony ludności zależy od stopnia integracji ochrony infrastruktury kluczowej dla funkcjonowania państwa, zdolności do przeciwdziałania zagrożeniom hybrydowym i cybernetycznym oraz poziomu odporności społecznej. Zastosowano podejście analityczno-problemowe oparte na analizie aktów normatywnych i dokumentów strategicznych, uzupełnione studium przypadków: kryzysu na granicy polsko-białoruskiej (2021–2023), kampanii „Ghostwriter" (UNC1151) oraz incydentów i sabotażu wobec infrastruktury transportowej i energetycznej. Szczególną uwagę poświęcono rozwiązaniom wprowadzonym Ustawą z 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej jako odpowiedzi systemowej na presję poniżej progu wojny. Wyniki analizy wskazują na konieczność spójnego łączenia zarządzania kryzysowego, cyberbezpieczeństwa, komunikacji kryzysowej oraz współdziałania cywilno-wojskowego, a także na znaczenie praktycznego wdrażania nowych instrumentów planistycznych, organizacyjnych i szkoleniowych dla budowy odporności państwa i społeczeństwa.

Słowa kluczowe: bezpieczeństwo powszechne; ochrona ludności; zagrożenia hybrydowe; cyberbezpieczeństwo; odporność społeczna (resilience); infrastruktura krytyczna; działania poniżej progu wojny; komunikacja kryzysowa

Abstract

The article examines the transformation of comprehensive (public) security and civil protection under complex 21st-century threats, where the traditional boundaries between peace, crisis, and war are increasingly blurred and hostile influence operates simultaneously in physical and digital domains.

It advances the thesis that the effectiveness of modern civil protection depends primarily on: (1) the integration of protection for critical infrastructure essential to state functionality, (2) state capacity to counter hybrid and cyber threats, and (3) a high level of societal resilience. The study adopts an analytical-problem approach based on the review of legal acts and strategic documents, complemented by case studies of: the Poland–Belarus border crisis (2021–2023), the "Ghostwriter" (UNC1151) hack-and-leak/disinformation campaign, and incidents and sabotage targeting transport and energy infrastructure. Particular emphasis is placed on the Act of 5 December 2024 on Civil Protection and Civil Defence as a systemic response to sub-threshold pressure. The analysis indicates that effective adaptation requires coherent integration of crisis management, cybersecurity, crisis communication, and civil-military cooperation, alongside the practical implementation of new planning, organizational, and training instruments. Overall, the article argues that strengthening state and societal resilience is indispensable for civil protection in an era of hybrid conflict spanning real and virtual battlefields.

Keywords: comprehensive security; civil protection; hybrid threats; cybersecurity; societal resilience; critical infrastructure; sub-threshold activities; crisis communication

Wstęp

W pierwszych dekadach XXI wieku środowisko bezpieczeństwa uległo zasadniczej transformacji, zarówno pod względem charakteru zagrożeń, jak i sposobów ich oddziaływania na państwo oraz społeczeństwo. Tradycyjne rozumienie bezpieczeństwa, oparte głównie na zagrożeniach militarnych o charakterze symetrycznym, zostało uzupełnione, a w wielu aspektach zastąpione przez zagrożenia o charakterze złożonym, hybrydowym i sieciowym, funkcjonujące jednocześnie w przestrzeni realnej i wirtualnej. Szczególnego znaczenia nabierają dziś cyberataki, operacje informacyjne, presja migracyjna, działania poniżej progu wojny oraz oddziaływania wymierzone w infrastrukturę krytyczną i spójność społeczną państw.

W tych warunkach istotnej redefinicji wymaga pojęcie bezpieczeństwa powszechnego oraz system ochrony ludności, który nie może być już postrzegany wyłącznie jako domena reagowania na klęski żywiołowe i awarie techniczne. Współczesna ochrona ludności musi obejmować również przygotowanie społeczeństwa i instytucji państwowych na skutki konfliktów hybrydowych, cybernetycznych oraz długotrwałej presji poniżej progu wojny. Szczególne znaczenie ma w tym kontekście bezpieczeństwo infrastruktury krytycznej, odporność informacyjna społeczeństwa oraz zdolność do sprawnego współdziałania podmiotów cywilnych i wojskowych.

Nowe ramy funkcjonowania systemu ochrony ludności w Polsce wyznacza Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej[1] (dalej zwana: „Ustawa OLiOC"), która w sposób kompleksowy porządkuje zadania państwa w zakre-

1 Dz.U. 2024, poz. 1907.

sie przygotowania na zagrożenia czasu pokoju, kryzysu i wojny. Regulacja ta stanowi nie tylko odpowiedź na doświadczenia ostatnich lat, w tym pandemii, kryzysów energetycznych i presji migracyjnej, lecz także na eskalację zagrożeń wynikających z agresywnej polityki Federacji Rosyjskiej oraz dynamicznego rozwoju cyberprzestrzeni jako nowego pola oddziaływania konfliktowego.

Teza artykułu zakłada, że: *skuteczność współczesnego systemu bezpieczeństwa powszechnego i ochrony ludności w warunkach złożonych zagrożeń XXI wieku zależy przede wszystkim od stopnia integracji ochrony infrastruktury krytycznej, zdolności państwa do przeciwdziałania zagrożeniom hybrydowym i cybernetycznym, wspieranych przez wysoki poziom odporności społecznej*.

Celem artykułu jest analiza współczesnych wyzwań dla ochrony ludności w Polsce w kontekście zagrożeń hybrydowych i cybernetycznych, działań prowadzonych poniżej progu wojny, a także ocena znaczenia infrastruktury krytycznej i możliwości budowania odporności społecznej. Szczególny nacisk położono na ocenę rozwiązań wprowadzonych Ustawą OLiOC oraz ich potencjalną rolę w budowaniu odporności państwa i społeczeństwa.

W pracy sformułowano następujące pytania badawcze:

5. W jaki sposób współczesne zagrożenia hybrydowe i cybernetyczne redefiniują pojęcie bezpieczeństwa powszechnego i ochrony ludności?
6. Jaką rolę w systemie bezpieczeństwa powszechnego odgrywa infrastruktura krytyczna w warunkach konfliktu poniżej progu wojny?
7. Jakie uwarunkowania instytucjonalne i społeczne decydują o poziomie odporności społecznej na współczesne zagrożenia bezpieczeństwa?
8. W jakim stopniu rozwiązania przyjęte w ustawie z dnia 5 grudnia 2024 r. wzmacniają zdolności państwa do ochrony ludności przed zagrożeniami złożonymi?

Artykuł ma charakter analityczno-problemowy i opiera się na analizie aktów normatywnych, dokumentów strategicznych, literatury przedmiotu oraz wnioskach płynących z obserwacji współczesnych konfliktów i kryzysów bezpieczeństwa.

1. Bezpieczeństwo powszechne w XXI wieku: między realnym a wirtualnym polem walki

Współczesne środowisko bezpieczeństwa charakteryzuje się rosnącą dynamiką, wielowymiarowością oraz wysokim poziomem nieprzewidywalności. Zanik klasycznego podziału na stan pokoju, kryzysu i wojny, postępująca hybrydyzacja zagrożeń oraz przenikanie się sfery realnej i wirtualnej powodują, że bezpieczeństwo

powszechne nabiera nowego, znacznie bardziej złożonego znaczenia. Współzależności polityczne, militarne, gospodarcze, społeczne i technologiczne, funkcjonujące jednocześnie w wymiarze lokalnym, regionalnym i globalnym, generują efekt kaskadowy, w którym nawet pozornie odległe zdarzenia mogą wywoływać bezpośrednie skutki dla bezpieczeństwa państwa i jego obywateli.

Zmieniające się uwarunkowania bezpieczeństwa wywierają zasadniczy wpływ na kierunki transformacji systemów odpowiedzialnych za ochronę ludności. Dotyczy to zarówno struktur administracji publicznej, sił zbrojnych, służb ratowniczych i porządkowych, jak również podmiotów odpowiedzialnych za infrastrukturę krytyczną oraz bezpieczeństwo informacyjne i cyberbezpieczeństwo. Kluczową rolę w tym procesie odgrywa obecnie zdolność państwa do przeciwdziałania zagrożeniom o charakterze złożonym, tj. takim, które łączą elementy militarne i niemilitarne, fizyczne i cyfrowe, wewnętrzne i zewnętrzne.

W tym kontekście szczególnego znaczenia nabiera problematyka bezpieczeństwa powszechnego, rozumianego jako stan oraz proces zapewniania ochrony życia, zdrowia, mienia i środowiska naturalnego wszystkim obywatelom, niezależnie od charakteru zagrożenia. Bezpieczeństwo to nie jest już wyłącznie domeną wyspecjalizowanych służb, lecz staje się obszarem współodpowiedzialności wszystkich elementów systemu państwowego oraz społeczeństwa jako całości. Rosnąca rola przestrzeni informacyjnej i cybernetycznej sprawia ponadto, że granice klasycznego „pola walki" ulegają zatarciu, a działania destabilizujące mogą być prowadzone bez użycia tradycyjnych środków przemocy zbrojnej.

Jednym z najbardziej doniosłych wyzwań XXI wieku jest przenikanie się realnego i wirtualnego wymiaru zagrożeń. Cyberataki na infrastrukturę krytyczną, dezinformacja, operacje wpływu czy zakłócanie łączności mogą sparaliżować funkcjonowanie państwa w stopniu porównywalnym z klasycznymi działaniami zbrojnymi. Ustawa z 2024 r. uwzględnia ten fakt, wskazując konieczność ochrony systemów teleinformatycznych wykorzystywanych do ostrzegania, alarmowania, zarządzania kryzysowego i koordynacji działań ratowniczych.

W tym ujęciu bezpieczeństwo powszechne nie ogranicza się już do ochrony przed zagrożeniami naturalnymi czy technicznymi, lecz obejmuje również sferę informacyjną i cyfrową. Obywatel staje się uczestnikiem systemu bezpieczeństwa nie tylko jako potencjalna ofiara zdarzeń nadzwyczajnych, ale także jako podmiot narażony na oddziaływanie informacyjne, którego zachowania mogą wzmacniać lub osłabiać odporność państwa. Stąd też ustawodawca akcentuje rolę edukacji dla bezpieczeństwa, szkoleń z zakresu samoobrony powszechnej oraz budowania odporności społecznej (resilience).

2. Znaczenie strategii bezpieczeństwa narodowego i uwarunkowań międzynarodowych

Transformacja krajowego systemu ochrony ludności i bezpieczeństwa powszechnego pozostaje ściśle powiązana z założeniami zawartymi w strategicznych dokumentach państwa, w tym w Strategii Bezpieczeństwa Narodowego RP. Dokument ten wyznacza główne interesy narodowe oraz cele strategiczne w sferze bezpieczeństwa, odwołując się zarówno do wartości konstytucyjnych, jak i do międzynarodowych zobowiązań Polski.

Członkostwo Rzeczypospolitej Polskiej w Sojuszu Północnoatlantyckim oraz w Unii Europejskiej determinuje nie tylko kierunki rozwoju zdolności obronnych, lecz także standardy ochrony ludności. Mechanizmy współpracy cywilno-wojskowej, wspólne ćwiczenia w zakresie zarządzania kryzysowego, a także unijne programy ochrony ludności i pomocy humanitarnej wzmacniają krajową odporność systemową. Ustawa OLiOC tworzy podstawy prawne umożliwiające pełniejsze włączenie krajowych struktur ochrony ludności w europejskie i transatlantyckie systemy reagowania kryzysowego.

Jednym z kluczowych wyznaczników środowiska bezpieczeństwa XXI wieku jest upowszechnienie się zagrożeń hybrydowych, które cechuje celowe łączenie środków militarnych i niemilitarnych, jawnych i niejawnych, militarnych i cywilnych, prowadzonych zarówno w przestrzeni fizycznej, jak i informacyjnej oraz cybernetycznej. Istotą oddziaływań hybrydowych jest rozmycie granicy pomiędzy wojną a pokojem oraz utrudnienie jednoznacznej identyfikacji agresora, co w konsekwencji komplikuje proces uruchamiania klasycznych mechanizmów obronnych państwa.

Zagrożenia hybrydowe obejmują m.in. działania dezinformacyjne, presję ekonomiczną, instrumentalizację migracji, cyberataki, sabotaż infrastruktury krytycznej, prowokacje graniczne, działania wywiadowcze i dywersyjne, a także wykorzystywanie napięć społecznych i politycznych do destabilizacji państw. W odróżnieniu od klasycznych konfliktów zbrojnych nie zmierzają one w pierwszej kolejności do fizycznego zniszczenia potencjału militarnego przeciwnika, lecz do stopniowej erozji jego stabilności wewnętrznej, spójności społecznej oraz zaufania obywateli do instytucji państwa.

W tym kontekście bezpieczeństwo powszechne staje się jednym z głównych celów oddziaływań hybrydowych, gdyż dezorganizacja życia społecznego, zakłócenie dostaw energii, wody, żywności czy paraliż systemów łączności bezpośrednio wpływają na poczucie bezpieczeństwa obywateli oraz odporność państwa jako całości.

3. Cyberprzestrzeń jako nowe pole oddziaływania na bezpieczeństwo powszechne

Cyberprzestrzeń stała się obecnie jednym z podstawowych wymiarów rywalizacji strategicznej i konfliktów poniżej progu wojny. Ataki na systemy teleinformatyczne administracji publicznej, sektora finansowego, energetycznego, transportowego czy ochrony zdrowia mogą prowadzić do skutków porównywalnych z użyciem konwencjonalnych środków rażenia. Szczególnie wrażliwa jest infrastruktura krytyczna, której zakłócenie funkcjonowania bezpośrednio przekłada się na bezpieczeństwo powszechne ludności.

W realiach współczesnych cyberzagrożeń granice pomiędzy przestępczością, działalnością wywiadowczą a działaniami o charakterze quasi-militarnym ulegają zatarciu. Operacje w cyberprzestrzeni mogą być prowadzone w sposób długotrwały, rozproszony i trudny do jednoznacznego przypisania konkretnemu państwu, co dodatkowo ogranicza możliwości skutecznej reakcji prawnej i politycznej.

Ustawa OLiOC wzmacnia znaczenie cyberprzestrzeni jako obszaru wymagającego szczególnej ochrony, wskazując na konieczność zapewnienia ciągłości działania systemów ostrzegania, alarmowania i kierowania działaniami ratowniczymi również w warunkach zakłóceń teleinformatycznych. Tym samym cyberbezpieczeństwo zostało wprost powiązane z systemem ochrony ludności, a nie – jak dotąd – wyłącznie z bezpieczeństwem informacyjnym administracji czy sektora IT.

4. Działania Federacji Rosyjskiej oraz Republiki Białorusi poniżej progu wojny wobec Polski i regionu Europy Środkowo-Wschodniej jako wyzwanie dla bezpieczeństwa powszechnego i ochrony ludności

Działania poniżej progu wojny (sub-threshold activities) stały się jednym z głównych narzędzi realizacji polityki bezpieczeństwa Federacji Rosyjskiej, a w ostatnich latach również Republiki Białorusi, której samodzielność strategiczna uległa istotnemu ograniczeniu. Ich istotą jest prowadzenie długotrwałej, wielowymiarowej presji na państwa regionu – w tym Polskę – bez formalnego wypowiedzenia konfliktu zbrojnego i bez przekroczenia progu, który automatycznie uruchomiłby mechanizmy zbiorowej obrony NATO.

Instrumentarium tych działań obejmuje m.in.: operacje informacyjno-psychologiczne, cyberataki, presję migracyjną, działania sabotażowe wobec infrastruktury krytycznej, demonstracje wojskowe, a także prowokacje na granicach lądowych i w przestrzeni powietrznej. Celem jest systematyczna erozja odporności państw,

osłabienie spójności społecznej oraz podważanie zaufania obywateli do instytucji publicznych, a więc uderzenie w samo jądro bezpieczeństwa powszechnego.

W takim ujęciu Polska – jako państwo frontowe NATO i UE, położone pomiędzy obwodem kaliningradzkim a Białorusią – staje się jednym z głównych obszarów testowania i projekcji rosyjsko-białoruskich form wojny hybrydowej.

Analiza współczesnych zagrożeń dla bezpieczeństwa powszechnego wymaga odejścia od klasycznego, wyłącznie militarnego rozumienia konfliktu i uwzględnienia działań prowadzonych poniżej progu wojny, które w sposób bezpośredni i pośredni oddziałują na funkcjonowanie państwa oraz bezpieczeństwo ludności cywilnej. Zjawiska te – określane zbiorczo mianem działań hybrydowych – charakteryzują się łączeniem instrumentów politycznych, informacyjnych, cybernetycznych, ekonomicznych i militarnych, przy jednoczesnym celowym zacieraniu granicy między stanem pokoju a konfliktem zbrojnym. W efekcie pole oddziaływania współczesnych zagrożeń obejmuje nie tylko instytucje państwowe i siły zbrojne, lecz również społeczeństwo, infrastrukturę krytyczną oraz systemy informacyjne, od których zależy codzienne funkcjonowanie ludności.

Z perspektywy ochrony ludności szczególnie istotne jest to, że działania hybrydowe często nie powodują natychmiastowych, spektakularnych strat, lecz stopniowo erodują zdolność państwa do reagowania kryzysowego, podważają zaufanie obywateli do instytucji publicznych oraz generują długotrwałe napięcia społeczne. Tym samym stawiają one nowe wyzwania przed systemami bezpieczeństwa powszechnego, które muszą być przygotowane na równoczesne reagowanie na zagrożenia o charakterze fizycznym, informacyjnym i cyfrowym, zarówno w wymiarze lokalnym, jak i ogólnokrajowym.

W celu zobrazowania skali i złożoności tych wyzwań w niniejszym artykule zastosowano metodę studium przypadku. Pozwala ona na pogłębioną analizę konkretnych zdarzeń i procesów, które w ostatnich latach istotnie wpłynęły na funkcjonowanie polskiego systemu bezpieczeństwa oraz ochrony ludności. Przedstawione przykłady nie mają charakteru wyczerpującego, lecz zostały dobrane w taki sposób, aby ukazać różne wymiary współczesnych zagrożeń hybrydowych – od presji migracyjnej i operacji informacyjnych, przez cyberataki, po sabotaż infrastruktury krytycznej oraz demonstracje siły militarnej sprzężone z dezinformacją.

Każde z zaprezentowanych studiów przypadku stanowi ilustrację przenikania się realnego i wirtualnego pola walki, na którym ludność cywilna staje się zarówno pośrednim, jak i bezpośrednim adresatem oddziaływań wrogich działań. Ich analiza umożliwia sformułowanie wniosków dotyczących konieczności integracji systemów zarządzania kryzysowego, ochrony ludności, cyberbezpieczeństwa i ochrony infrastruktury krytycznej, a także znaczenia spójnej komunikacji kryzysowej w warun-

kach narastającej presji informacyjnej. W tym sensie studia przypadków stanowią empiryczne tło dla dalszych rozważań nad kierunkami adaptacji bezpieczeństwa powszechnego do realiów zagrożeń XXI wieku.

A. Studium przypadku I: kryzys na granicy polsko-białoruskiej 2021–2023 jako narzędzie wojny hybrydowej

Kryzys migracyjny na granicy polsko-białoruskiej, zapoczątkowany w 2021 r., jest klasycznym przykładem wykorzystania migracji jako instrumentu presji politycznej i wojny hybrydowej wobec państw UE i NATO. Badania analityczne wskazują, że migranci byli celowo sprowadzani przez białoruskie władze – m.in. poprzez ułatwienia wizowe i zorganizowany transport – w celu sztucznego wytworzenia presji na granicy z Litwą, Łotwą i przede wszystkim Polską.

Operacja ta miała charakter skoordynowany i wielofazowy: najpierw wymierzona była w Litwę i Łotwę, a następnie – od lata 2021 r. – skoncentrowała się na odcinku polskim, doprowadzając do konieczności wprowadzenia stanu wyjątkowego na części terytorium RP oraz radykalnego wzmocnienia ochrony granicy.

Z perspektywy bezpieczeństwa powszechnego i ochrony ludności kryzys ten miał kilka wymiarów:

1. Wymiar operacyjny – długotrwałe zaangażowanie Straży Granicznej, wojska, policji i służb ratowniczych na stosunkowo wąskim pasie przygranicznym, przy konieczności równoczesnego zabezpieczenia porządku publicznego, udzielania pomocy humanitarnej oraz przeciwdziałania próbom nielegalnego przekraczania granicy.
2. Wymiar społeczny – rosnące napięcia w społecznościach lokalnych, obciążonych obecnością służb, mediów, organizacji pozarządowych i migrantów, a także polaryzacja opinii publicznej w kraju.
3. Wymiar informacyjny – prowadzenie przez stronę białorusko-rosyjską intensywnej kampanii propagandowej przedstawiającej Polskę i UE jako odpowiedzialne za rzekomy „kryzys humanitarny", przy równoczesnym wykorzystywaniu dramatycznego położenia migrantów jako narzędzia presji medialnej.

Analizy międzynarodowe wskazują wprost, że kryzys ten należy interpretować jako element wojny hybrydowej przeciwko UE i NATO, w której ludzie zostali cynicznie potraktowani jako „narzędzie" wywierania nacisku na politykę graniczną i sankcyjną.

Z punktu widzenia polskiego systemu ochrony ludności doświadczenia kryzysu granicznego ujawniły potrzebę:

- lepszej integracji mechanizmów zarządzania kryzysowego, ochrony granic i ochrony ludności,

- przygotowania społeczności przygranicznych na długotrwałą obecność służb i możliwe incydenty,
- spójnej komunikacji kryzysowej, ograniczającej skuteczność wrogich narracji oraz polaryzacji społecznej.

Wnioski te znalazły odzwierciedlenie m.in. w pracach nad nową Ustawą OLiOC, która zakłada wzmocnienie współdziałania pomiędzy administracją rządową, samorządową oraz Siłami Zbrojnymi RP w sytuacjach długotrwałych kryzysów o charakterze hybrydowym.

Wnioski z kryzysu 2021–2023 a konstrukcja współdziałania w Ustawie OLiOC

Kryzys na granicy polsko-białoruskiej (2021–2023) ujawnił, że w sytuacji długotrwałej presji hybrydowej (instrumentalizacja migracji, działania informacyjne, incydenty z użyciem przemocy, destabilizacja społeczna) „ochrona ludności" przestaje być wyłącznie domeną klasycznego reagowania ratowniczego. Staje się węzłem współdziałania: administracji rządowej (w tym wojewody), samorządu terytorialnego (gmina–powiat–województwo), służb (SG/Policja/PSP), podmiotów społecznych i – w określonych konfiguracjach – Sił Zbrojnych RP.

Nowa Ustawa OLiOC porządkuje tę logikę wprost: tworzy system organów/podmiotów/zasobów ochrony ludności, a jednocześnie wskazuje, że realizacja zadań w sytuacjach kryzysowych odbywa się „na podstawie ustawy o zarządzaniu kryzysowym" (czyli spina OLiOC z reżimem zarządzania kryzysowego). Wnioski z kryzysu granicznego (integracja mechanizmów, przygotowanie społeczności, spójna komunikacja) dają się przełożyć na konkretne mechanizmy prawne w Ustawie OLiOC i ustawach ustrojowo-kompetencyjnych.

Ustawa OLiOC rozstrzyga kwestię „kto jest organem ochrony ludności" i kto odpowiada na danym szczeblu:

- Wójt/burmistrz/prezydent miasta, starosta, wojewoda i minister właściwy ds. wewnętrznych to terytorialne organy ochrony ludności.
- Minister właściwy ds. wewnętrznych koordynuje realizację zadań w skali państwa, a wójt/starosta/wojewoda odpowiadają na swoich obszarach.

Należy zauważyć, iż w zdarzeniach długotrwałych (miesiące/lata), w których „rdzeń" jest na wąskim pasie granicy, a skutki (logistyka, napięcia społeczne, dezinformacja, ochrona infrastruktury, wsparcie medyczne i socjalne) rozlewają się terytorialnie, nie wystarcza dowodzenie „przez służby". Potrzebna jest administracyjna oś odpowiedzialności – od wójta przez starostę do wojewody – z koordynacją na poziomie MSWiA.

To koresponduje z ustawami samorządowymi, które już wcześniej sytuowały bezpieczeństwo/porządek publiczny w zadaniach JST:

- Gmina – zadania własne, m.in. porządek publiczny i bezpieczeństwo obywateli oraz ochrona przeciwpożarowa i przeciwpowodziowa. (art. 7 ustawy o samorządzie gminnym).
- Powiat – zadania ponadgminne, w tym obszary związane z bezpieczeństwem/porządkiem publicznym (art. 4 ustawy o samorządzie powiatowym).
- Województwo samorządowe – zadania wojewódzkie, wprost wskazujące m.in. „bezpieczeństwo publiczne i ochronę ludności" (art. 14 ustawy o samorządzie województwa).

Ustawa OLiOC działa tu jak „nadbudowa specjalistyczna": nie zmienia, że JST mają zadania bezpieczeństwa, ale dookreśla role i narzędzia właściwe ochronie ludności jako systemowi.

Jedną z kluczowych odpowiedzi Ustawy OLiOC na kryzysy hybrydowe jest legalizacja mechanizmu porozumień o wykonywaniu zadań oraz porozumień/umów o współdziałaniu między szczeblami.

- Ustawa OLiOC wskazuje, że podmiotami ochrony ludności mogą być także podmioty, z którymi organ zawarł porozumienie o wykonywaniu zadań (odwołanie do art. 19 OLiOC).
- Ustawa wymaga, aby w porozumieniu określić m.in. zakres zadań, warunki finansowania, sposób współpracy oraz możliwość użycia zasobów w sytuacjach zagrożeń (dostępność i dyspozycyjność personelu).
- Wprost przewidziano też, że wójt i starosta zawierają porozumienia/umowy o współdziałaniu w zakresie realizacji zadań ochrony ludności lub obrony cywilnej.

W kryzysie granicznym istotnym problemem była „ciągłość zdolności" (rotacje, przeciążenie, wielość aktorów, niekiedy sprzeczne oczekiwania społeczne). Mechanizm porozumień pozwala:

1. sformalizować rolę NGO, podmiotów medycznych, operatorów logistycznych, a nawet wybranych przedsiębiorców w łańcuchu ochrony ludności,
2. ustalić „kto, co i za ile" robi w długim horyzoncie (a nie tylko doraźnie),
3. przenieść część współdziałania z poziomu „ad hoc" na poziom planowy, audytowalny i finansowalny.

W sensie ustrojowym porozumienia nie konkurują z ustawami samorządowymi, tylko korzystają z klasycznej formuły współdziałania JST i administracji (porozumienia/umowy), ale zasilają je treścią specyficzną dla ochrony ludności (zasoby, dyspozycyjność, gotowość, finansowanie).

Ustawa OLiOC wyciąga ewakuację z „ogólnych deklaracji" i ubiera ją w procedurę wieloszczeblową:

- Wojewoda opracowuje wojewódzki plan ewakuacji ludności na podstawie wkładów przygotowanych przez wójtów i starostów.
- Wojewódzki plan ewakuacji jest załącznikiem funkcjonalnym do wojewódzkiego planu zarządzania kryzysowego, a wkłady gmin/powiatów są załącznikami funkcjonalnymi do planów zarządzania kryzysowego gminy i powiatu.

Należy podkreślić, iż jeśli kryzys graniczny nie jest „klasyczną ewakuacją" jak powódź, to w realiach hybrydowych pojawiają się przemieszczenia ludności i konieczność zabezpieczenia:

- lokalnych społeczności (np. czasowe ograniczenia dostępu, incydenty, napięcia, zagrożenia infrastruktury),
- osób wymagających szczególnej opieki,
- systemów przyjęcia/relokacji.

Ustawa OLiOC tworzy tu ważny efekt: jedno planowanie (ochrona ludności) jest zszyte z drugim planowaniem (zarządzanie kryzysowe). To ogranicza ryzyko „równoległych planów" w różnych instytucjach, co w kryzysach długotrwałych prowadzi do rozjazdu odpowiedzialności.

W kryzysie granicznym obciążenia społeczne były równie istotne jak operacyjne: ciągła obecność służb, ograniczenia w poruszaniu się, spory aksjologiczne, napięcia między „bezpieczeństwem" i „humanitaryzmem", presja medialna.

Ustawa OLiOC odpowiada na to poprzez:

- definicję społecznej odporności i obowiązek działań edukacyjno-informacyjnych (w tym instruowanie, przygotowanie do ewakuacji, pierwszej pomocy, budowanie odporności).
- umocowanie systemu ochrony ludności jako zorientowanego nie tylko na „reagowanie", ale też przygotowanie organów i ludności (zadania obejmujące szkolenia, ćwiczenia, ciągłość działania administracji).

Należy wskazać, iż w pasie przygranicznym potrzeba „odporności społecznej" dotyczy m.in.:

- zdolności mieszkańców do funkcjonowania przy długich utrudnieniach (logistyka, dojazdy, praca, turystyka, lokalny biznes),
- redukcji podatności na dezinformację i polaryzację,
- przygotowania procedur lokalnych (miejsca doraźnego schronienia, wsparcie socjalne, kanały informacji).

W tym miejscu bardzo ważne jest powiązanie z ustawami samorządowymi: skoro bezpieczeństwo i porządek publiczny są w zadaniach własnych gminy i zadaniach powiatu, to OLiOC dostarcza specjalistycznych instrumentów (plany ewakuacji, porozumienia, zasoby, szkolenia) do ich praktycznej realizacji.

W wymiarze informacyjnym kryzys graniczny był areną konkurujących narracji: odpowiedzialność za cierpienie migrantów, legalność działań państwa, rola UE, obraz służb, itp. Ustawa OLiOC nie ogranicza się tu do hasła „komunikacja", ale buduje komponent infrastrukturalny.

W Ustawie OLiOC ujęto System Bezpiecznej Łączności Państwowej (SBŁP), z którego mogą korzystać organy/urzędy/jednostki organizacyjne oraz także Siły Zbrojne RP w zakresie niezbędnym do realizacji zadań bezpieczeństwa państwa, ratownictwa, ochrony ludności i zarządzania kryzysowego.

W kryzysach hybrydowych „komunikacja kryzysowa" to nie tylko konferencje prasowe. To przede wszystkim:

- odporna łączność międzyinstytucjonalna,
- spójność przepływu ostrzeżeń i komunikatów,
- ograniczenie podatności na zakłócenia/ataki w cyberprzestrzeni i wojnie informacyjnej.

Ustawa OLiOC wprowadza Rządowy Zespół Ochrony Ludności jako ciało opiniodawczo-doradcze przy Radzie Ministrów w sprawach ochrony ludności i obrony cywilnej. W kryzysie granicznym (długotrwałym i wieloobszarowym) problemem bywa rozproszenie komunikatów i decyzji w wielu resortach i szczeblach. Instrument w postaci Zespołu wzmacnia horyzontalną koordynację (w tym spójność polityczną i komunikacyjną).

W kryzysach granicznych wojewoda jest kluczowy z dwóch powodów: reprezentuje Radę Ministrów w województwie i jednocześnie koordynuje administrację zespoloną (w tym służby).

Ustawa o wojewodzie i administracji rządowej w województwie przewiduje, że wojewoda:

- zapewnia współdziałanie organów administracji rządowej i samorządowej w województwie i kieruje ich działalnością w zakresie zapobiegania i zwalczania zagrożeń (życia, zdrowia, mienia, środowiska, bezpieczeństwa państwa i porządku publicznego, klęsk żywiołowych itd.) (art. 22).

Ustawa OLiOC „daje treść ochrony ludności", a ustawa wojewodowa „daje ster" w terenie do integrowania rządu i samorządu. W kryzysie hybrydowym to jest krytyczne: jeśli wojewoda nie pełni roli integratora, powstaje luka między:

- działaniami SG/Policji/PSP,
- działaniami JST (pomoc, logistyka lokalna, zarządzanie społecznymi skutkami),
- działaniami administracji rządowej (strategie, finansowanie, łączność, komunikaty centralne).

Ustawa o działach administracji rządowej porządkuje, kto w rządzie odpowiada za jakie „piony":

- W obszarze spraw wewnętrznych (dział) minister właściwy ds. wewnętrznych sprawuje nadzór nad kluczowymi służbami (m.in. Policja, SG, PSP) (art. 29 – dział „sprawy wewnętrzne").
- W obszarze obrony narodowej dział obejmuje sprawy obrony państwa i Sił Zbrojnych RP (art. 19).

Kryzys graniczny jako narzędzie wojny hybrydowej wymaga „mostu" między działem spraw wewnętrznych i działem obrony narodowej – bo to sytuacja, która nie jest jeszcze wojną, ale ma cel strategiczny i bywa wspierana instrumentami państwa-agresora (informacja, presja migracyjna, incydenty, testowanie granic reakcji). Ustawa OLiOC – szczególnie przez mechanizmy koordynacyjne i interoperacyjne – wzmacnia tę przestrzeń współdziałania.

Ustawa o zarządzaniu kryzysowym dopuszcza uczestnictwo oddziałów Sił Zbrojnych w realizacji zadań zarządzania kryzysowego – w zależności od przygotowania specjalistycznego – i wylicza typowe zadania (monitoring zagrożeń, ocena skutków, działania poszukiwawczo-ratownicze, ewakuacja) (art. 25). W tym ujęciu wojsko jest „zasobem wsparcia" dla organów cywilnych, uruchamianym wtedy, gdy inne siły i środki są niewystarczające lub wymagane jest specjalistyczne wsparcie. To pasuje do długotrwałej presji: wsparcie logistyczne, inżynieryjne, rozpoznawcze, medyczne, transportowe, zabezpieczenie ciągłości działań.

W sytuacjach, gdy siły Straży Granicznej są niewystarczające lub stopień zagrożenia to uzasadnia, ustawa o Straży Granicznej przewiduje możliwość użycia oddziałów i pododdziałów Sił Zbrojnych do pomocy SG (art. 11b). To jest reżim „bardziej bezpośredni" dla kryzysów na granicy, bo łączy ochronę granicy z wojskowym wsparciem, ale nadal w logice legalnej i dowodzenia (wojsko pozostaje w systemie dowodzenia SZRP – co jest kluczowe dla odpowiedzialności, zasad użycia środków przymusu i rozdzielenia kompetencji).

B. Studium przypadku II: kampania „Ghostwriter" i cyberataki na polską administrację

Drugim kluczowym obszarem działań poniżej progu wojny są cyberoperacje oraz towarzyszące im kampanie informacyjne. W przypadku Polski szczególnie istotnym przykładem jest działalność grupy UNC1151, powiązanej z białoruskimi (i szerzej: rosyjskimi) strukturami państwowymi, prowadzonej w ramach tzw. kampanii „Ghostwriter".

Według analityków cyberbezpieczeństwa kampania ta łączyła:

- włamania do skrzynek pocztowych i systemów teleinformatycznych przedstawicieli władz państwowych,
- publikację selektywnie dobranych i zmanipulowanych treści („hack-and-leak"),

- działania dezinformacyjne w mediach tradycyjnych i społecznościowych,
- tworzenie fałszywych artykułów i oświadczeń przypisywanych polskim instytucjom.

Celem operacji nie było wyłącznie pozyskanie informacji, lecz przede wszystkim:

- kompromitacja przedstawicieli władz,
- podważenie wiarygodności instytucji państwowych,
- wytworzenie wrażenia trwałej słabości i chaosu w systemie bezpieczeństwa państwa,
- pogłębianie polaryzacji politycznej i społecznej.

Tego typu działania – choć pozornie „miękkie" – uderzają bezpośrednio w bezpieczeństwo powszechne. W sytuacji kryzysu lub konfliktu obywatele mogą bowiem mieć trudności z odróżnieniem wiarygodnych komunikatów władz od zmanipulowanych przekazów inspirowanych z zewnątrz. Z punktu widzenia ochrony ludności oznacza to ryzyko:

- ignorowania przez część społeczeństwa rzeczywistych ostrzeżeń i zaleceń,
- reagowania na fałszywe alarmy,
- blokowania działań ewakuacyjnych, logistycznych czy porządkowych.

W odpowiedzi polskie służby specjalne podjęły działania informacyjne wobec sojuszników z NATO, wskazując, że kampania „Ghostwriter" ma charakter skoordynowanej operacji wymierzonej w stabilność państw Europy Środkowo-Wschodniej.

Doświadczenia te znalazły odzwierciedlenie w krajowych działaniach regulacyjnych i organizacyjnych, m.in. w:

- wzmacnianiu krajowego systemu cyberbezpieczeństwa,
- rozwijaniu zdolności analitycznych w obszarze walki informacyjnej,
- włączaniu w system ochrony ludności kwestii ochrony systemów teleinformatycznych, w tym tych wykorzystywanych do ostrzegania i alarmowania ludności (co koresponduje z nową Ustawą OLiOC).

Analiza kampanii „Ghostwriter", prowadzonej przez grupę UNC1151, unaocznia fundamentalną zmianę charakteru zagrożeń oddziałujących na bezpieczeństwo powszechne w XXI wieku. Przypadek ten potwierdza, że współczesne cyberoperacje oraz skoordynowane działania dezinformacyjne nie stanowią jedynie domeny konfliktów zbrojnych sensu stricto, lecz są trwałym elementem funkcjonowania państw w warunkach rywalizacji poniżej progu wojny. W konsekwencji wymagają one adekwatnej odpowiedzi regulacyjnej, organizacyjnej oraz doktrynalnej, obejmującej także system ochrony ludności.

Jednym z kluczowych wniosków płynących z doświadczeń związanych z kampanią „Ghostwriter" jest konieczność traktowania cyberbezpieczeństwa nie wyłącznie jako zagadnienia technicznego lub sektorowego, lecz jako integralnego elementu

bezpieczeństwa powszechnego. Skala i charakter cyberataków wymierzonych w instytucje państwowe oraz osoby pełniące funkcje publiczne dowiodły, że naruszenia systemów teleinformatycznych mogą prowadzić do efektów porównywalnych z oddziaływaniem klasycznych środków destabilizacji państwa.

W odpowiedzi na te zagrożenia Polska podjęła działania zmierzające do wzmocnienia krajowego systemu cyberbezpieczeństwa, zarówno w wymiarze instytucjonalnym, jak i normatywnym. Obejmowały one m.in. rozwój zdolności reagowania na incydenty cybernetyczne, zwiększenie roli wyspecjalizowanych zespołów reagowania (CSIRT), a także intensyfikację współpracy między administracją publiczną, sektorem prywatnym oraz strukturami międzynarodowymi, w tym w ramach NATO.

Istotnym elementem tych działań stało się również uznanie infrastruktury teleinformatycznej administracji publicznej za część infrastruktury krytycznej, której ochrona ma bezpośrednie przełożenie na zdolność państwa do realizacji podstawowych funkcji wobec obywateli, w tym informowania, ostrzegania i koordynowania działań w sytuacjach kryzysowych.

Kampania „Ghostwriter" unaoczniła, że cyberataki rzadko funkcjonują w oderwaniu od szerszego kontekstu informacyjnego. Wręcz przeciwnie – stanowią one często jedynie wstęp do operacji wpływu, których zasadniczym celem jest kształtowanie percepcji społecznej, podważanie zaufania do instytucji państwowych oraz pogłębianie istniejących podziałów politycznych i społecznych.

W związku z tym jednym z kluczowych wniosków systemowych stała się potrzeba rozwijania wyspecjalizowanych zdolności analitycznych w obszarze walki informacyjnej. Obejmują one zarówno monitoring przestrzeni informacyjnej, analizę narracji dezinformacyjnych, jak i identyfikację mechanizmów ich dystrybucji oraz oddziaływania na różne grupy społeczne.

Z perspektywy ochrony ludności szczególnie istotne jest rozpoznawanie sytuacji, w których działania dezinformacyjne mogą zakłócać procesy decyzyjne obywateli w warunkach kryzysowych. Dezinformacja może bowiem prowadzić do:

- podważania zasadności działań władz publicznych,
- negowania zagrożeń lub ich wyolbrzymiania,
- utrudniania realizacji procedur ewakuacyjnych i ratowniczych,
- obniżania poziomu podporządkowania się zaleceniom służb odpowiedzialnych za bezpieczeństwo.

Rozwijanie zdolności analitycznych w tym obszarze stało się zatem nie tylko elementem bezpieczeństwa informacyjnego państwa, lecz również narzędziem wzmacniania odporności społecznej (resilience), która stanowi jeden z fundamentów nowoczesnych systemów ochrony ludności.

Szczególnie istotnym wnioskiem wynikającym z analizy kampanii „Ghostwriter" jest potrzeba objęcia ochroną cybernetyczną systemów wykorzystywanych bezpośrednio do ostrzegania i alarmowania ludności. Systemy te – obejmujące m.in. platformy komunikacji kryzysowej, systemy powiadamiania SMS, aplikacje mobilne czy infrastrukturę teleinformatyczną centrów zarządzania kryzysowego – stały się potencjalnym celem oddziaływań hybrydowych.

Zakłócenie ich funkcjonowania, przejęcie kontroli nad przekazem lub podszywanie się pod oficjalne komunikaty władz mogłoby prowadzić do poważnych konsekwencji dla bezpieczeństwa obywateli. Doświadczenia z kampanii „Ghostwriter" potwierdzają, że przeciwnik może dążyć nie tyle do całkowitego sparaliżowania systemu, ile do wytworzenia niepewności co do wiarygodności emitowanych komunikatów.

W tym kontekście istotne znaczenie mają rozwiązania przyjęte w nowej Ustawie OLiOC, która w sposób wyraźny poszerza rozumienie ochrony ludności o komponent cyfrowy i informacyjny. Ustawa ta tworzy ramy do:

- integracji zagadnień cyberbezpieczeństwa z systemem zarządzania kryzysowego,
- uwzględniania odporności systemów teleinformatycznych w planowaniu ochrony ludności,
- budowania zdolności do funkcjonowania systemów ostrzegania w warunkach zakłóceń cybernetycznych i informacyjnych.

Podsumowując, studium przypadku kampanii „Ghostwriter" potwierdza, że współczesne zagrożenia dla bezpieczeństwa powszechnego mają charakter wielowymiarowy i hybrydowy. Ich skutki oddziałują nie tylko na instytucje państwowe, lecz bezpośrednio na społeczeństwo, jego zdolność do racjonalnego reagowania oraz poziom zaufania do państwa.

Wnioski płynące z tego przypadku znalazły odzwierciedlenie w krajowych działaniach regulacyjnych i organizacyjnych, które stopniowo przesuwają akcent z reaktywnego zarządzania kryzysowego na budowanie systemowej odporności. Integracja cyberbezpieczeństwa, walki informacyjnej oraz ochrony infrastruktury teleinformatycznej z systemem ochrony ludności stanowi istotny krok w kierunku dostosowania państwa do realiów bezpieczeństwa XXI wieku – funkcjonującego jednocześnie w przestrzeni fizycznej, informacyjnej i cyfrowej.

C. Studium przypadku III: sabotaż i incydenty wobec infrastruktury krytycznej

Trzecim wymiarem działań poniżej progu wojny są incydenty wymierzone bezpośrednio w infrastrukturę krytyczną, w tym szczególnie w sektor transportu i energetyki. Przykładem, który odbił się szerokim echem, był incydent na polskiej sieci

kolejowej w 2023 r., kiedy nieznani sprawcy wykorzystali prosty sygnał radiowy typu „radio-stop" do zatrzymania kilkudziesięciu pociągów w północno-zachodniej Polsce. Kolejnym przykładem z ww. zakresu są wydarzenia w listopadzie 2025 r., gdzie miał miejsce poważny atak dywersyjny na polską infrastrukturę kolejową, w tym na linię Warszawa–Lublin, gdzie doszło do eksplozji uszkadzającej tory, co było elementem wojny hybrydowej i sabotażu mającego na celu zakłócenie transportu militarnego do Ukrainy. W związku z incydentem zatrzymano obywatela Ukrainy podejrzanego o pomoc w działaniach na zlecenie rosyjskich służb, co wywołało szeroką debatę i dezinformację w mediach, szczególnie na platformach społecznościowych.

Analizy wskazują, że atak ten mógł zostać przeprowadzony przy użyciu relatywnie prostego i taniego sprzętu, lecz jego skutki operacyjne były poważne: zakłócono ruch kolejowy, zwiększono ryzyko incydentów bezpieczeństwa, a także zademonstrowano podatność systemu na działania sabotażowe. W szerszym kontekście europejskim incydent ten wpisuje się w katalog domniemanych rosyjskich operacji sabotażowych, prowadzonych wobec infrastruktury państw NATO – w tym kabli energetycznych i telekomunikacyjnych, rurociągów oraz systemów transportowych.

W ostatnich latach pojawiły się również obawy związane z bezpieczeństwem infrastruktury elektroenergetycznej w Polsce, w tym linii przesyłowych i stacji transformatorowych, w świetle możliwych ataków dronowych oraz sabotażu. W odpowiedzi na narastające ryzyko w 2025 r. zacieśniono współpracę pomiędzy operatorem krajowej sieci przesyłowej a Siłami Zbrojnymi RP, obejmującą m.in. wymianę informacji, wspólne szkolenia oraz działania na rzecz ochrony obiektów kluczowych.

Z perspektywy ochrony ludności incydenty infrastrukturalne – nawet jeśli nie powodują bezpośrednich ofiar – mają fundamentalne znaczenie:

- zakłócenie dostaw energii, wody czy transportu może szybko przełożyć się na problemy w zaopatrzeniu ludności, funkcjonowaniu szpitali i służb ratowniczych,
- powtarzalność takich incydentów prowadzi do narastania poczucia niepewności i braku kontroli,
- długotrwałe zakłócenia infrastrukturalne mogą stać się katalizatorem niepokojów społecznych.

Nowa ustawa o ochronie ludności i obronie cywilnej wprost łączy ochronę ludności z ochroną infrastruktury krytycznej, zobowiązując organy administracji publicznej do planowania działań na wypadek awarii i sabotażu, a także do współdziałania z operatorami infrastruktury oraz siłami zbrojnymi.

Wejście w życie Ustawy OLiOC stanowi jakościową zmianę w podejściu państwa do bezpieczeństwa powszechnego. Nowe regulacje normatywne w sposób systemowy łączą zagadnienia ochrony ludności z zapewnieniem ciągłości funkcjo-

nowania infrastruktury kluczowej dla podstawowych potrzeb społeczeństwa oraz zdolności obronnych państwa. Choć ustawa nie posługuje się literalnie pojęciem „infrastruktura krytyczna" w rozumieniu wcześniejszych regulacji sektorowych, to jej przepisy tworzą spójne ramy prawne dla planowania, przygotowania i reagowania na awarie, zakłócenia oraz działania sabotażowe wymierzone w kluczowe systemy infrastrukturalne.

Zgodnie z art. 1 pkt 3 ustawy, jednym z podstawowych elementów regulacji są zasady planowania ochrony ludności i obrony cywilnej. Planowanie to obejmuje nie tylko reagowanie na skutki zagrożeń, lecz również przygotowanie struktur państwowych i samorządowych na sytuacje, w których dochodzi do poważnych zakłóceń w funkcjonowaniu systemów zaopatrzenia, transportu czy łączności. Tym samym ustawodawca przesuwa punkt ciężkości z reaktywnego modelu zarządzania kryzysowego na model proaktywny, oparty na analizie ryzyka i odporności systemów.

Kluczowe znaczenie w tym kontekście ma art. 8 ustawy, który wprowadza pojęcie infrastruktury niezbędnej do realizacji zadań ochrony ludności i obrony cywilnej. Do tej kategorii zaliczono m.in. systemy energetyczne, transportowe, teleinformatyczne, zaopatrzenia w wodę i paliwa oraz magazynowania rezerw. Tak szerokie ujęcie odpowiada współczesnym zagrożeniom hybrydowym, w których oddziaływanie na infrastrukturę stanowi środek pośredni destabilizacji bezpieczeństwa ludności bez konieczności prowadzenia otwartych działań zbrojnych.

Nowa ustawa nakłada na organy administracji publicznej wyraźne obowiązki w zakresie koordynacji i współdziałania z innymi podmiotami odpowiedzialnymi za bezpieczeństwo infrastrukturalne. Zgodnie z art. 16 ust. 1 pkt 6–8 minister właściwy do spraw wewnętrznych zapewnia wymianę informacji niezbędnych do realizacji zadań ochrony ludności oraz współdziała z innymi organami ochrony ludności, w tym w ramach współpracy międzynarodowej i zobowiązań sojuszniczych. Przepis ten tworzy formalną podstawę do integracji działań administracji cywilnej z podmiotami odpowiedzialnymi za bezpieczeństwo energetyczne, transportowe i telekomunikacyjne.

Istotnym uzupełnieniem powyższego są przepisy art. 19 i 20 ustawy, które umożliwiają zawieranie porozumień pomiędzy organami ochrony ludności a innymi podmiotami realizującymi zadania na rzecz bezpieczeństwa. W praktyce oznacza to możliwość formalizacji współpracy z operatorami infrastruktury krytycznej, zarówno publicznymi, jak i prywatnymi, a także z Siłami Zbrojnymi RP w zakresie ochrony obiektów kluczowych. Rozwiązanie to odpowiada współczesnemu modelowi bezpieczeństwa, w którym odpowiedzialność za odporność infrastrukturalną jest rozproszona i wymaga koordynacji międzysektorowej.

Ustawodawca wyraźnie akcentuje znaczenie przygotowania praktycznego poprzez obowiązek organizowania ćwiczeń. Zgodnie z art. 53–54 ustawy organy ochrony ludności zobowiązane są do prowadzenia ćwiczeń z zakresu ochrony ludności i obrony cywilnej, obejmujących różnorodne scenariusze zagrożeń. W świetle współczesnych doświadczeń, w tym incydentów sabotażowych wobec infrastruktury transportowej i energetycznej, przepisy te należy interpretować jako obowiązek uwzględniania w ćwiczeniach scenariuszy awarii technicznych, ataków hybrydowych oraz zakłóceń o charakterze celowym.

Znaczenie ćwiczeń polega nie tylko na sprawdzeniu zdolności reagowania służb, lecz również na weryfikacji współpracy pomiędzy administracją publiczną, operatorami infrastruktury oraz wojskiem. W tym sensie ustawa tworzy ramy dla budowy realnej odporności systemowej, a nie jedynie formalnej gotowości planistycznej.

Szczególne znaczenie dla integracji ochrony ludności z ochroną infrastruktury krytycznej ma art. 156 ustawy, przewidujący opracowanie czteroletniego Programu Ochrony Ludności i Obrony Cywilnej. Program ten podlega uzgodnieniu m.in. z Ministrem Obrony Narodowej, co wprost wprowadza komponent wojskowy do planowania cywilnego. W kontekście zagrożeń hybrydowych oraz potencjalnych działań sabotażowych wobec infrastruktury, udział Sił Zbrojnych RP w planowaniu i przygotowaniu ma kluczowe znaczenie dla zapewnienia ciągłości funkcjonowania państwa w sytuacjach poniżej progu wojny.

Uzupełnieniem systemu są przepisy art. 61–63 ustawy, które ustanawiają mechanizmy nadzoru i kontroli nad realizacją zadań ochrony ludności i obrony cywilnej. Obejmują one zarówno działania organów administracji, jak i podmiotów współdziałających na podstawie zawartych porozumień. W praktyce oznacza to możliwość oceny stopnia przygotowania infrastruktury i procedur reagowania na zakłócenia, co ma fundamentalne znaczenie w kontekście prewencji i ograniczania skutków sabotażu.

Analiza przepisów ustawy o ochronie ludności i obronie cywilnej prowadzi do wniosku, że ustawodawca dokonał istotnego przesunięcia paradygmatu bezpieczeństwa powszechnego. Ochrona ludności została trwale powiązana z odpornością infrastrukturalną państwa, a administracja publiczna została zobowiązana do planowania, współdziałania i ćwiczenia scenariuszy awaryjnych oraz sabotażowych. W kontekście złożonych zagrożeń XXI wieku – w tym działań hybrydowych i operacji poniżej progu wojny – regulacje te tworzą podstawy do budowy systemu ochrony ludności zdolnego do funkcjonowania w warunkach długotrwałych zakłóceń infrastrukturalnych.

5. Intensyfikacja działań hybrydowych po 2022 r. – drony, manewry wojskowe, kampanie dezinformacyjne

Po pełnoskalowej agresji Rosji na Ukrainę w 2022 r. obserwuje się dalszą eskalację działań poniżej progu wojny wobec Polski i regionu. Należą do nich m.in.:

- incydenty naruszeń lub bliskich naruszeń przestrzeni powietrznej przez rosyjskie drony, które skłoniły NATO do wzmocnienia misji nadzoru nad wschodnią flanką,
- powtarzające się ćwiczenia wojskowe typu „Zapad", organizowane na terytorium Białorusi i zachodniej Rosji, o scenariuszach jawnie zakładających konflikt z państwami NATO,
- intensywne kampanie dezinformacyjne sprzęgnięte z działaniami militarnymi, jak w przypadku skoordynowanych operacji dronowych i zmasowanego zalewu mediów społecznościowych fałszywymi narracjami dotyczącymi rzekomej roli Ukrainy czy NATO w incydentach wojskowych na terytorium Polski.

Te działania – choć wciąż formalnie „poniżej progu wojny" – mają realny wpływ na bezpieczeństwo powszechne, wymuszając:

- podwyższenie gotowości systemów alarmowania i obrony powietrznej,
- częstsze angażowanie sił zbrojnych do ochrony infrastruktury i granic,
- ciągłą komunikację kryzysową z obywatelami,
- rozwój zdolności do identyfikacji i neutralizacji kampanii dezinformacyjnych.

Złożone działania hybrydowe obserwowane po 2022 r., obejmujące incydenty z użyciem bezzałogowych statków powietrznych, demonstracyjne manewry wojskowe oraz skoordynowane kampanie dezinformacyjne, ujawniły ograniczenia dotychczasowego modelu reagowania kryzysowego. W odpowiedzi na te wyzwania ustawodawca w ustawie o ochronie ludności i obronie cywilnej wprowadził rozwiązania, które integrują ochronę ludności z ochroną infrastruktury kluczowej dla funkcjonowania państwa, a także formalizują współdziałanie administracji publicznej, operatorów infrastruktury oraz Sił Zbrojnych RP.

Zasadniczą zmianę wprowadza art. 1 pkt 3 ustawy, który wskazuje, że jednym z podstawowych elementów regulacji są zasady planowania ochrony ludności i obrony cywilnej. Planowanie to obejmuje nie tylko sytuacje klęsk żywiołowych, lecz również zdarzenia wynikające z celowych działań o charakterze wrogim, w tym sabotażu, dywersji oraz działań poniżej progu wojny.

Rozwinięciem tego podejścia jest art. 8, w którym ustawodawca definiuje infrastrukturę niezbędną do realizacji zadań ochrony ludności i obrony cywilnej. Do tej kategorii zaliczono m.in.:

- systemy energetyczne i paliwowe,

- transport i logistykę,
- łączność i systemy teleinformatyczne,
- zaopatrzenie w wodę,
- magazynowanie i dystrybucję zasobów niezbędnych do przetrwania ludności.

Takie ujęcie wprost odpowiada zagrożeniom hybrydowym, w których atak na infrastrukturę staje się narzędziem wywierania presji strategicznej i destabilizacji bezpieczeństwa powszechnego bez formalnego rozpoczęcia konfliktu zbrojnego.

Nowa ustawa jednoznacznie wzmacnia obowiązek współdziałania międzyinstytucjonalnego, co ma kluczowe znaczenie w warunkach działań hybrydowych. Zgodnie z art. 16 ust. 1 pkt 6–8, minister właściwy do spraw wewnętrznych:

- zapewnia wymianę informacji niezbędnych do realizacji zadań ochrony ludności,
- koordynuje działania w ramach współpracy międzynarodowej i zobowiązań sojuszniczych,
- współdziała z innymi organami ochrony ludności.

Przepis ten stanowi normatywną podstawę do integracji działań administracji cywilnej z systemami bezpieczeństwa infrastrukturalnego, w tym z operatorami sieci energetycznych, transportowych i telekomunikacyjnych, które w realiach wojny hybrydowej stają się pierwszorzędnym celem oddziaływania.

Szczególnie istotne znaczenie w kontekście ochrony infrastruktury krytycznej mają art. 19 i 20 ustawy, które przewidują możliwość zawierania porozumień pomiędzy organami ochrony ludności a innymi podmiotami realizującymi zadania na rzecz bezpieczeństwa. Mechanizm ten umożliwia:

- formalne włączenie operatorów infrastruktury do systemu ochrony ludności,
- określenie zasad współdziałania w sytuacjach awarii, sabotażu lub zagrożeń militarnych,
- skoordynowanie działań administracji publicznej z Siłami Zbrojnymi RP.

Rozwiązanie to odpowiada realiom współczesnych zagrożeń, w których wojsko coraz częściej angażowane jest w ochronę granic, przestrzeni powietrznej oraz infrastruktury kluczowej, nawet w sytuacjach formalnie pozostających poza stanem wojny.

W odpowiedzi na rosnącą liczbę incydentów hybrydowych ustawodawca położył nacisk na przygotowanie praktyczne. Art. 53–54 ustawy nakładają na organy ochrony ludności obowiązek organizowania ćwiczeń z zakresu ochrony ludności i obrony cywilnej. Ćwiczenia te powinny obejmować scenariusze:

- zakłóceń w funkcjonowaniu infrastruktury,
- awarii systemów energetycznych i teleinformatycznych,
- działań dywersyjnych i sabotażowych,

- incydentów z użyciem bezzałogowych statków powietrznych.

W tym sensie ćwiczenia stają się narzędziem budowania odporności państwa na zagrożenia hybrydowe, a nie jedynie elementem formalnej gotowości.

Kluczowym elementem integrującym ochronę ludności z ochroną infrastruktury w warunkach zagrożeń hybrydowych jest art. 156 ustawy, który przewiduje opracowanie Programu Ochrony Ludności i Obrony Cywilnej. Program ten:

- obejmuje okres czteroletni,
- podlega aktualizacji,
- jest uzgadniany z Ministrem Obrony Narodowej.

Wprowadzenie obligatoryjnego udziału resortu obrony narodowej w planowaniu cywilnym należy interpretować jako instytucjonalne uznanie roli Sił Zbrojnych RP w reagowaniu na zagrożenia poniżej progu wojny, w tym ochronę infrastruktury i wsparcie administracji publicznej.

System uzupełniają art. 61–63 ustawy, ustanawiające mechanizmy nadzoru i kontroli nad realizacją zadań ochrony ludności i obrony cywilnej. Obejmują one zarówno organy administracji publicznej, jak i podmioty współdziałające na podstawie zawartych porozumień. Rozwiązanie to ma kluczowe znaczenie w kontekście zapobiegania zaniedbaniom w przygotowaniu infrastruktury na sytuacje awaryjne i sabotażowe.

Analiza przepisów ustawy o ochronie ludności i obronie cywilnej wskazuje, że ustawodawca w sposób świadomy odpowiedział na eskalację działań hybrydowych po 2022 r. Ochrona ludności została normatywnie powiązana z ochroną infrastruktury kluczowej, a administracja publiczna została zobowiązana do planowania, współdziałania i ćwiczenia scenariuszy awarii oraz sabotażu. W efekcie ustawa tworzy podstawy prawne do funkcjonowania systemu ochrony ludności w warunkach długotrwałej presji hybrydowej, charakterystycznej dla współczesnego środowiska bezpieczeństwa.

6. Wnioski z perspektywy bezpieczeństwa powszechnego i ochrony ludności

Przedstawione studia przypadków – kryzys migracyjny na granicy polsko-białoruskiej, kampania „Ghostwriter" oraz incydenty wobec infrastruktury krytycznej – pokazują, że działania Federacji Rosyjskiej i Białorusi poniżej progu wojny:

- przenoszą konflikt z poziomu ściśle militarnego na poziom codziennego funkcjonowania społeczeństwa,
- wymuszają traktowanie ochrony ludności jako kluczowego narzędzia polityki bezpieczeństwa, a nie wyłącznie domeny służb ratowniczych,

- łączą realne i wirtualne pole walki – operacje w cyberprzestrzeni i przestrzeni informacyjnej wywołują skutki w świecie fizycznym (na granicy, w infrastrukturze, w zachowaniach ludzi), a incydenty fizyczne są wzmacniane kampaniami informacyjnymi.

W tym kontekście Ustawę z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej należy postrzegać jako odpowiedź systemową na doświadczenia ostatnich lat. Jej skuteczność będzie jednak zależała od:

- konsekwentnego wdrażania zapisów dotyczących współdziałania cywilno-wojskowego,
- integracji ochrony infrastruktury krytycznej z planowaniem ochrony ludności,
- rozwoju odporności społecznej na presję hybrydową,
- zdolności do szybkiego reagowania na skoordynowane działania w realnej i wirtualnej przestrzeni konfliktu.

Szczególnym źródłem zagrożeń hybrydowych dla bezpieczeństwa powszechnego Polski są działania podejmowane przez Federację Rosyjską w ramach strategii oddziaływań poniżej progu wojny. Od wielu lat obserwuje się intensyfikację aktywności rosyjskich służb specjalnych, operacji dezinformacyjnych, cyberataków oraz prób destabilizacji sytuacji społecznej i politycznej państw Europy Środkowo-Wschodniej, w tym Rzeczypospolitej Polskiej.

Działania te obejmują m.in.:

- długotrwałe kampanie dezinformacyjne w przestrzeni medialnej i w mediach społecznościowych,
- operacje wpływu ukierunkowane na antagonizowanie społeczeństwa,
- ataki cybernetyczne na instytucje publiczne oraz sektor infrastruktury krytycznej,
- próby ingerencji w procesy wyborcze,
- wykorzystywanie presji migracyjnej jako narzędzia destabilizacji sytuacji na granicach.

Cechą charakterystyczną tych działań jest ich permanentny charakter oraz stopniowanie intensywności w zależności od sytuacji międzynarodowej. Operacje poniżej progu wojny pozwalają na osiąganie celów strategicznych bez formalnego wypowiedzenia konfliktu zbrojnego i bez uruchamiania mechanizmów artykułu 5 Traktatu Północnoatlantyckiego. W tym sensie bezpieczeństwo powszechne staje się pierwszą linią oddziaływania agresora, a społeczeństwo – głównym obiektem presji psychologicznej i informacyjnej.

A. Wniosek nr 1: od incydentu do „kryzysu długiego trwania" w warunkach hybrydowych

Trzy przywołane studia przypadku (kryzys na granicy 2021–2023, kampania „Ghostwriter", incydenty i sabotaż wobec infrastruktury krytycznej) ukazują wspólną cechę współczesnych zagrożeń: nie mieszczą się one w klasycznych kategoriach „pokoju" i „wojny", lecz funkcjonują poniżej progu wojny, jednocześnie generując realne skutki dla bezpieczeństwa powszechnego. W praktyce oznacza to „kryzysy rozciągnięte w czasie", w których presja jest stała, wielowymiarowa (operacyjna, społeczna, informacyjna, infrastrukturalna), a próg eskalacji jest kontrolowany przez przeciwnika.

Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (dalej: Ustawa OLiOC) odpowiada na tę logikę, budując ramy koordynacji wieloszczeblowej i trwałej gotowości państwa do ochrony ludności, w tym przy aktywnym udziale samorządu terytorialnego i – w określonych obszarach – Sił Zbrojnych RP.

Równolegle ustawodawca dopina systemowo relacje kompetencyjne, wprowadzając i doprecyzowując powiązania z:

- ustawami samorządowymi (gminną i powiatową – oraz pośrednio wojewódzką),
- ustawą o wojewodzie i administracji rządowej w województwie (instrumenty koordynacji i poleceń),
- ustawą o zarządzaniu kryzysowym (plany, infrastruktura krytyczna, planowanie cywilne uwzględniające użycie/wykorzystanie SZ RP),
- ustawą o działach administracji rządowej (umiejscowienie ochrony ludności/OC w „sprawach wewnętrznych" i połączenie z zarządzaniem kryzysowym i migracjami),
- ustawą o obronie Ojczyzny (normatywne „mosty" zasobowe i organizacyjne, w tym świadczenia rzeczowe oraz komponenty zdolności – WOT i Wojska Obrony Cyberprzestrzeni).

B. Wniosek nr 2: kryzys graniczny jako test „współdziałania w pionie" – od samorządu do wojewody i poziomu rządowego

Kryzys na granicy polsko-białoruskiej pokazał, że w warunkach presji hybrydowej (w tym instrumentalizacji migracji) kluczowe staje się:

- szybkie uruchamianie zasobów (logistyka, medycyna, schronienie, transport),
- stabilne współdziałanie służb, administracji i samorządu na ograniczonym obszarze, ale przez długi czas,
- spójna komunikacja i zarządzanie napięciami społecznymi w społecznościach lokalnych.

Ustawa OLiOC wzmacnia w tym zakresie rolę organów samorządowych jako organów ochrony ludności na swoich poziomach oraz osadza je w systemie koordynacji wojewody i RM.

1. **Zadania wójta/burmistrza/prezydenta miasta – poziom „pierwszej odpowiedzi"**

Ustawa OLiOC wprost określa zadania wójta (burmistrza, prezydenta miasta), w tym kierowanie i koordynowanie realizacji zadań ochrony ludności i obrony cywilnej na obszarze gminy.

To jest kluczowe w kryzysach granicznych, bo „pierwsza odpowiedź" (logistyka pomocy, zabezpieczenie porządku, wsparcie działań służb i ratownictwa, organizacja zasobów, kontakt z mieszkańcami) bardzo często materializuje się właśnie w gminach.

Co ważne, ustawodawca dopina tę rolę także w ustawie samorządowej: wójt otrzymuje expressis verbis kompetencję wykonywania zadań organu ochrony ludności i OC określonych w OLiOC (art. 31aa ustawy o samorządzie gminnym).

Interpretacja w kontekście kryzysu granicznego: gmina nie jest wyłącznie „zapleczem socjalnym" incydentu – staje się formalnym węzłem systemu ochrony ludności, zdolnym do koordynacji zasobów i działań na rzecz przetrwania ludności (mieszkańców i osób przebywających czasowo), przy jednoczesnym współdziałaniu z podmiotami państwowymi.

2. **Zadania starosty – poziom integracji ponadgminnej**

Analogicznie, OLiOC definiuje zadania starosty jako organu ochrony ludności na poziomie powiatu. Jednocześnie ustawa o samorządzie powiatowym wprost ujmuje „ochronę ludności i obronę cywilną" w katalogu zadań ponadgminnych (art. 4 ust. 1 pkt 16).

Interpretacja: w kryzysach granicznych powiat jest poziomem, na którym:

- skala działań przekracza jedną gminę (np. presja migracyjna rozlewa się na kilka JST),
- rośnie potrzeba koordynacji zasobów (magazyny, transport, zabezpieczenie medyczne, infrastruktura zbiorowej ochrony),
- pojawia się potrzeba zarządzania konsekwencjami społecznymi (ruch, porządek publiczny) w układzie ponadgminnym.

Dodatkowo powiat posiada instrumenty stanowienia przepisów porządkowych dla ochrony bezpieczeństwa publicznego (art. 41 ustawy o samorządzie powiatowym). W praktyce kryzysów hybrydowych oznacza to możliwość szybkiego uregulowania zachowań zbiorowych w sytuacjach niecierpiących zwłoki (z zachowaniem ustawowych ograniczeń i nadzoru legalności).

3. **Wojewoda jako „integrator pionu" i narzędzie koordynacji administracji rządowej z samorządem**

Ustawa o wojewodzie przypisuje wojewodzie obowiązek zapewnienia współdziałania organów administracji rządowej i samorządowej w zakresie zapobiegania zagrożeniom życia, zdrowia, mienia, porządku publicznego i bezpieczeństwa państwa (art. 22 pkt 2), a po zmianach – także wykonywanie zadań organu OLiOC (art. 22 pkt 3a).

Najsilniejszym instrumentem „na czas kryzysu długiego trwania" są polecenia wojewody:

- wiążą organy administracji rządowej w województwie,
- a w sytuacjach nadzwyczajnych – także organy JST,
- przy czym ustawodawca doprecyzował, że sytuacjami nadzwyczajnymi są również sytuacje kryzysowe w rozumieniu ustawy o zarządzaniu kryzysowym (art. 25 ust. 1 i 1a).

Interpretacja wprost pod kryzys graniczny: ten mechanizm rozwiązuje „problem rozproszenia decyzyjnego", typowy dla długotrwałych presji hybrydowych. Wojewoda może ujednolicać działanie instytucji na obszarze województwa w sposób szybki, bez czekania na wieloetapowe uzgodnienia, z zachowaniem ograniczeń (polecenia nie ingerują m.in. w istotę decyzji administracyjnych i czynności operacyjno-rozpoznawcze).

4. **Umiejscowienie systemu w rządzie: „dział sprawy wewnętrzne"**

Ustawa o działach administracji rządowej przypisuje do działu „sprawy wewnętrzne" m.in. ochronę granicy państwa i politykę migracyjną, zarządzanie kryzysowe oraz ochronę ludności i obronę cywilną (art. 29 ust. 1 pkt 2, 3 i 4). To istotne w kontekście kryzysu granicznego: ustawodawca lokuje kluczowe elementy odpowiedzi (granica–migracje–kryzys–ochrona ludności) w jednym dziale, co sprzyja spójności kompetencyjnej i budżetowej na poziomie rządowym.

C. Wniosek nr 3: „pole walki informacyjnej" jako element bezpieczeństwa powszechnego – od komunikacji kryzysowej do odporności łączności państwa

Kampania „Ghostwriter" pokazuje, że cyberoperacje i dezinformacja mogą uderzać bezpośrednio w bezpieczeństwo powszechne poprzez:

- erozję zaufania do instytucji,
- chaos poznawczy wśród obywateli,
- obniżenie wykonalności ewakuacji, alarmowania, działań porządkowych,
- wzrost podatności na „fałszywe narracje" w czasie napięć społecznych.

W odpowiedzi Ustawa OLiOC wzmacnia dwa filary: obowiązki komunikatowe oraz bezpieczną, odporną łączność.

Artykuł 73 Ustawy OLiOC wprowadza obowiązek niezwłocznego, nieodpłatnego przekazywania komunikatów na żądanie MSWiA lub wojewody, przekazane przez Rządowe Centrum Bezpieczeństwa – dla nadawców radiowo-telewizyjnych, operatorów sieci mobilnych (w tym kierowanie komunikatów do wszystkich lub określonych grup użytkowników), a także dla wydawców stron internetowych i redaktorów dzienników.

Interpretacja pod „Ghostwriter": to przepis antychaosowy. W środowisku, w którym przeciwnik próbuje podmieniać treści i dyskredytować komunikaty instytucji, ustawodawca wzmacnia formalny kanał „państwo´ obywatel", oparty o RCB, z możliwością uruchomienia na określonym obszarze i w określonym czasie. To nie likwiduje dezinformacji, ale zwiększa szansę, że komunikat autentyczny dotrze masowo i szybko.

W Ustawie OLiOC istotne są przepisy dotyczące Systemu Bezpiecznej Łączności Państwowej (dalej: „SBŁP"):

- organy ochrony ludności mogą wykorzystywać SBŁP do ogłaszania/odwoływania alarmów i przekazywania komunikatów ostrzegawczych (art. 77),
- SBŁP ma zapewniać odpowiedni poziom bezpieczeństwa usług (w tym – w miarę potrzeb – szyfrowaną komunikację) w celu realizacji zadań ochrony ludności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego (art. 78 ust. 1).
- ustawodawca przewiduje wsparcie techniczne dla operatora SBŁP udzielane przez wskazane przez MON jednostki wojskowe (art. 76 ust. 4 – w zakresie rozliczania wartości wsparcia).

Interpretacja: to bardzo praktyczny „łącznik" realnego i wirtualnego pola walki. Przy kampaniach typu hack-and-leak, a także przy próbach zakłóceń infrastruktury telekomunikacyjnej, państwo potrzebuje kanałów komunikacji odpornych na przechwycenie i sabotaż. Włączenie MON do wsparcia SBŁP oznacza, że zdolności wojskowe (techniczne, organizacyjne) mogą wzmacniać bezpieczeństwo komunikacji wykorzystywanej przez organy ochrony ludności.

Uzupełnieniem jest ustawa o obronie Ojczyzny, która wyodrębnia w SZ RP Wojska Obrony Cyberprzestrzeni jako komponent właściwy do działań w cyberprzestrzeni, w tym proaktywnej ochrony i aktywnej obrony zasobów kluczowych z punktu widzenia SZ RP (art. 15 ust. 4 pkt 2). W warunkach zagrożeń hybrydowych jest to potencjalne zaplecze zdolnościowe (systemowe – nie „policyjne"), które może wzmacniać odporność państwa na operacje w cyberprzestrzeni w obszarach powiązanych z bezpieczeństwem i obronnością.

D. Wniosek nr 4: sabotaż infrastruktury jako zagrożenie bezpieczeństwa powszechnego – od planowania cywilnego do zasobów „na 72 godziny" i mechanizmów wsparcia

Incydenty kolejowe (radio-stop, sabotaż infrastruktury) pokazują, że „tani atak" może generować „drogi skutek":

- paraliż transportu,
- zwiększone ryzyko wypadków i wtórnych zdarzeń,
- napięcia społeczne,
- zakłócenie zdolności przerzutu wojsk i logistyki państwa.

W tym obszarze kluczowe są: planowanie, zasoby, współdziałanie z operatorami oraz w razie potrzeby – wsparcie sił zbrojnych.

Ustawa o zarządzaniu kryzysowym definiuje infrastrukturę krytyczną i ochronę IK (art. 3), wskazując systemy m.in. transportowe, łączności i sieci teleinformatycznych oraz „zapewniające ciągłość działania administracji publicznej". Jednocześnie „planowanie cywilne" obejmuje także planowanie w zakresie wspierania SZ RP oraz planowanie wykorzystania SZ RP do realizacji zadań z zarządzania kryzysowego (art. 3 pkt 4 lit. b). Dalej, zadania planowania cywilnego obejmują przygotowanie planów zarządzania kryzysowego, utrzymywanie zasobów oraz rozwiązania na wypadek zniszczenia/zakłócenia IK (art. 4), a systemowo ustanowione są plany krajowe/wojewódzkie/powiatowe/gminne (art. 5).

Ten pakiet przepisów jest prawną podstawą do tego, by scenariusze dywersji (kolej, energetyka, telekomunikacja) nie były traktowane jako „wypadki", tylko jako planowane ryzyko bezpieczeństwa powszechnego. Jednocześnie ustawodawca od lat dopuszcza wprost planowanie użycia/wykorzystania SZ RP w zarządzaniu kryzysowym – OLiOC wzmacnia ten kierunek, nadając mu dodatkową warstwę (ochrona ludności/OC).

Ustawa OLiOC wprowadza definicję infrastruktury niezbędnej do realizacji zadań ochrony ludności i OC (art. 8), obejmującej m.in. zaopatrzenie w wodę i żywność, produkty lecznicze, energię, paliwo, łączność, usługi teleinformatyczne i transport. To jest bardzo istotne: ustawodawca ujmuje w jednym przepisie to, co sabotaż infrastrukturalny może „odciąć" i co bezpośrednio rzutuje na warunki przetrwania ludności.

Dodatkowo Ustawa OLiOC nakłada na wójta, starostę i wojewodę obowiązek zapewnienia zasobów ochrony ludności niezbędnych do wykonywania zadań przez co najmniej 3 dni trwania zagrożenia, w tym m.in. w zakresie wsparcia działań ratowniczych, powiadamiania/ostrzegania/alarmowania, łączności oraz funkcjonowania obiektów zbiorowej ochrony. Ww. uregulowania stanowią odpowiedź na dynamikę sabotażu i zakłóceń – pierwsze 48–72 godziny po ataku/serii incyden-

tów są kluczowe, bo wtedy zwykle występuje największa niepewność informacyjna i największe ryzyko wtórnych konsekwencji (panika, przerwy w dostawach, zatory transportowe, przeciążenie służb). Obowiązek „zasobów na 3 dni" jest normatywnym wymuszeniem minimalnej odporności.

W kryzysach infrastrukturalnych państwo potrzebuje szybkiego „wpięcia" podmiotów dysponujących realnymi zasobami (magazyny, sprzęt, transport, łączność, usługi). OLiOC przewiduje:

- możliwość wyznaczania jako podmiotów ochrony ludności podległych JST jednostek organizacyjnych i spółek z większościowym udziałem sektora finansów publicznych (art. 18),
- możliwość zawierania porozumień o wykonywaniu zadań ochrony ludności/OC m.in. z NGO (art. 19),
- możliwość uznawania podmiotów za podmioty ochrony ludności, jeżeli jest to uzasadnione koniecznością zapewnienia wykonania zadań (art. 20).

Ww. rozwiązanie stanowi przykład rozwiązania typowo „hybrydowego" – zwiększa adaptacyjność systemu. Przy sabotażu infrastruktury krytycznej potrzebne są często zasoby spoza klasycznych służb (operatorzy, spółki komunalne, firmy logistyczne, podmioty teleinformatyczne, organizacje zapewniające wsparcie humanitarne). OLiOC tworzy legalną ścieżkę szybkiego włączania takich podmiotów do systemu.

E. Wniosek nr 5: współdziałanie z Siłami Zbrojnymi RP – od „doraźnej pomocy" do trwałej architektury zdolności

W analizowanych przypadkach udział SZ RP ma trzy główne postacie:

1. wsparcie działań ochronnych i logistycznych (kryzys graniczny, ochrona obiektów, zabezpieczenie transportu),
2. wsparcie zdolnościowe w obszarze łączności i cyberodporności (w kontekście operacji informacyjnych i cyberataków),
3. zapewnienie zdolności do działania w sytuacjach, gdy zasoby cywilne są niewystarczające lub przeciążone.

OLiOC wskazuje Program Ochrony Ludności i Obrony Cywilnej jako podstawę finansowania zadań (art. 7) i umieszcza go w logice działania RM (zatwierdzanie, sprawozdawczość) (art. 6–7). Jednocześnie ustawa przewiduje mechanizmy budżetowe, w których MON wydziela środki przeznaczone na realizację zadań ochrony ludności i OC (w tym o charakterze obronnym), w programie fragment dotyczący etapu opracowywania budżetu i odniesienia do ustawy o obronie Ojczyzny.

W kryzysach hybrydowych problemem nie jest tylko „kto dowodzi", lecz „kto utrzymuje zdolności i za co". Włączenie MON do strumienia finansowania (na zadania

z pogranicza ochrony ludności i obronności) sprzyja temu, by zdolności potrzebne w czasie presji hybrydowej nie były budowane ad hoc.

Ustawa o obronie Ojczyzny przewiduje możliwość nakładania obowiązku świadczeń rzeczowych m.in. na cele zwalczania klęsk żywiołowych, likwidacji ich skutków oraz zarządzania kryzysowego (art. 628 ust. 1), a świadczenia te mogą być wykonywane m.in. na rzecz Sił Zbrojnych oraz innych jednostek realizujących zadania na potrzeby obrony państwa i zarządzania kryzysowego (art. 628 ust. 2).

Ww. uregulowania prawne to „twarda" podstawa mobilizacji zasobów w sytuacjach, w których łańcuchy dostaw i zasoby cywilne są zakłócone. W warunkach sabotażu infrastruktury albo presji granicznej może to mieć znaczenie dla transportu, zakwaterowania, sprzętu i infrastruktury pomocniczej.

Ustawa o obronie Ojczyzny wskazuje Wojska Obrony Terytorialnej jako rodzaj Sił Zbrojnych (art. 15 ust. 1 pkt 5). To jest ważne w kryzysach hybrydowych z perspektywy ochrony ludności, bo WOT stanowi potencjalny komponent zdolności „blisko terenu", użyteczny m.in. w:

- ochronie i dozorze obiektów,
- wsparciu logistycznym i ewakuacyjnym,
- wsparciu działań porządkowych w zakresie wynikającym z odrębnych podstaw prawnych i decyzji organów uprawnionych.

Równolegle wskazanie Wojsk Obrony Cyberprzestrzeni (art. 15 ust. 4 pkt 2) jest istotne dla wymiaru „Ghostwriter" i ochrony łączności/teleinformatyki.

F. Wniosek nr 6: integracja samorządu z systemem ochrony ludności – od zadań własnych do roli „elementu systemu bezpieczeństwa powszechnego"

Ustawa o samorządzie gminnym określa, że zaspokajanie zbiorowych potrzeb wspólnoty jest zadaniem własnym gminy (art. 7), a wśród narzędzi wzmacniania porządku i bezpieczeństwa dopuszcza np. monitoring dla zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej (art. 9a). Po zmianach powiązanych z OLiOC gmina ma także jasno dopisaną rolę organu ochrony ludności (art. 31aa).

Ustawa o samorządzie powiatowym idzie analogicznie: w katalogu zadań ponadgminnych zawiera porządek publiczny i bezpieczeństwo obywateli (art. 4 ust. 1 pkt 15) oraz ochronę przeciwpowodziową/przeciwpożarową, zapobieganie nadzwyczajnym zagrożeniom, a także ochronę ludności i OC (art. 4 ust. 1 pkt 16).

W związku z uchwaleniem i wprowadzeniem w życie Ustawy OLiOC samorząd przestaje być traktowany wyłącznie jako „wykonawca zadań komunalnych" w kryzysie. Staje się elementem architektury państwowej odporności, ze zdefiniowanym

zakresem koordynacji, obowiązkami zasobowymi (w logice 72 godzin) i możliwością formalnego włączania podmiotów (art. 18–20 Ustawy OLiOC).

Zakończenie

Przeprowadzona analiza potwierdza, że bezpieczeństwo powszechne w realiach XXI wieku wymaga odejścia od wąskiego, „ratowniczego" ujmowania ochrony ludności jako reakcji na klęski żywiołowe i awarie techniczne. Współczesne środowisko bezpieczeństwa charakteryzuje się zacieraniem granic między pokojem, kryzysem i wojną oraz przenikaniem się oddziaływań fizycznych i cyfrowych. W tym układzie ochrona ludności staje się jednym z kluczowych elementów odporności państwa – zarówno w wymiarze instytucjonalnym, infrastrukturalnym, jak i społecznym – a złożone zagrożenia hybrydowe, cybernetyczne i informacyjne oddziałują bezpośrednio na codzienne funkcjonowanie społeczeństwa oraz zdolność państwa do wykonywania funkcji podstawowych.

W odniesieniu do pierwszego pytania badawczego („W jaki sposób współczesne zagrożenia hybrydowe i cybernetyczne redefiniują pojęcie bezpieczeństwa powszechnego i ochrony ludności?") ustalenia prowadzą do wniosku, że redefinicja ta ma charakter systemowy i paradygmatyczny. Bezpieczeństwo powszechne nie może być już rozumiane jako stan zapewniany głównie przez wyspecjalizowane służby w sytuacjach nadzwyczajnych, lecz jako ciągły proces utrzymywania zdolności państwa i społeczeństwa do funkcjonowania w warunkach trwałej presji. Hybrydyzacja zagrożeń oznacza, że działania w cyberprzestrzeni, operacje informacyjne i sabotaż infrastrukturalny stają się narzędziami oddziaływania porównywalnymi skutkami z tradycyjnymi środkami przemocy, choć często realizowanymi „poniżej progu wojny". Ochrona ludności w takim ujęciu obejmuje nie tylko ewakuację, ratownictwo i zabezpieczenie logistyczne, ale również ochronę łączności, zdolność do wiarygodnego ostrzegania i alarmowania, komunikację kryzysową, przeciwdziałanie dezinformacji oraz budowanie odporności poznawczej i organizacyjnej społeczeństwa.

W kontekście drugiego pytania badawczego („Jaką rolę w systemie bezpieczeństwa powszechnego odgrywa infrastruktura krytyczna w warunkach konfliktu poniżej progu wojny?") przedstawione studia przypadków wskazują jednoznacznie, że infrastruktura krytyczna (w tym transport, energetyka, łączność i systemy teleinformatyczne administracji) staje się pierwszoplanowym celem działań hybrydowych, ponieważ jej zakłócenie wywołuje efekt kaskadowy: ogranicza możliwości reagowania służb, dezorganizuje funkcjonowanie administracji i gospodarki oraz wpływa na postawy społeczne (niepewność, panika, spadek zaufania). Incydenty kolejowe,

sabotaż oraz potencjalne oddziaływania na system elektroenergetyczny dowodzą, że nawet „tani" atak może generować „drogi" skutek systemowy. Oznacza to, że ochrona ludności musi być projektowana w ścisłym powiązaniu z ciągłością działania infrastruktury niezbędnej do zaspokajania podstawowych potrzeb ludności, a planowanie ochrony ludności powinno obejmować scenariusze awarii celowych (dywersji, sabotażu) oraz długotrwałych zakłóceń.

Odpowiadając na trzecie pytanie badawcze („Jakie uwarunkowania instytucjonalne i społeczne decydują o poziomie odporności społecznej na współczesne zagrożenia bezpieczeństwa?"), analiza wskazuje na trzy grupy czynników: instytucjonalno-organizacyjne, informacyjno-komunikacyjne oraz społeczno-kulturowe. Po stronie instytucjonalnej kluczowe znaczenie ma spójna architektura współdziałania (administracja rządowa–samorząd–służby–operatorzy infrastruktury–podmioty społeczne), która w warunkach kryzysów długotrwałych redukuje rozproszenie decyzyjne i przeciążenie zasobów. Po stronie informacyjnej decydujące jest utrzymanie zdolności do szybkiego, wiarygodnego i masowego przekazu ostrzeżeń oraz komunikatów, co ogranicza skuteczność operacji dezinformacyjnych i podnosi wykonalność działań ochronnych (ewakuacji, dystrybucji zasobów, regulacji porządku publicznego). Po stronie społecznej odporność budują: poziom zaufania do instytucji, kompetencje obywateli w zakresie bezpieczeństwa (edukacja dla bezpieczeństwa, samoorganizacja, umiejętności pierwszej pomocy), a także zdolność wspólnot lokalnych do funkcjonowania w warunkach długotrwałych ograniczeń. Kampania „Ghostwriter" pokazuje natomiast, że osłabienie odporności społecznej może następować nie przez fizyczne straty, lecz przez erozję zaufania, polaryzację i chaos poznawczy, co bezpośrednio uderza w bezpieczeństwo powszechne.

W odniesieniu do czwartego pytania badawczego („W jakim stopniu rozwiązania przyjęte w ustawie z dnia 5 grudnia 2024 r. wzmacniają zdolności państwa do ochrony ludności przed zagrożeniami złożonymi?") należy stwierdzić, że Ustawa OLiOC stanowi jakościową zmianę normatywną, ponieważ:

- rozszerza rozumienie ochrony ludności o wymiar informacyjny i teleinformatyczny,
- wzmacnia planowanie wieloszczeblowe (w tym planowanie ewakuacji jako funkcjonalne załączniki do planów zarządzania kryzysowego),
- formalizuje współdziałanie poprzez instrumenty porozumień i możliwość włączania podmiotów spoza klasycznych służb,
- akcentuje przygotowanie praktyczne poprzez obowiązek ćwiczeń oraz
- tworzy ramy systemowe, w których ochrona ludności jest sprzęgnięta z obroną cywilną i komponentem cywilno-wojskowym.

Jednocześnie skuteczność tych rozwiązań będzie zależeć od wdrożenia: finansowania, interoperacyjności procedur, realnych ćwiczeń obejmujących scenariusze hybrydowe oraz zdolności do integracji działań na poziomie lokalnym i regionalnym.

Na tej podstawie możliwa jest weryfikacja postawionej we wstępie tezy. Zebrane argumenty i wyniki analizy studiów przypadków potwierdzają, że skuteczność współczesnego systemu bezpieczeństwa powszechnego i ochrony ludności w warunkach złożonych zagrożeń rzeczywiście zależy przede wszystkim od:

- integracji ochrony infrastruktury krytycznej / infrastruktury niezbędnej do realizacji zadań ochrony ludności,
- zdolności państwa do przeciwdziałania zagrożeniom hybrydowym i cybernetycznym (w tym ochrony łączności, ostrzegania i odporności informacyjnej), oraz
- wysokiego poziomu odporności społecznej, rozumianej jako gotowość obywateli i instytucji do funkcjonowania w warunkach presji poniżej progu wojny.

Kryzys na granicy polsko-białoruskiej pokazał, że o rezultatach decyduje zdolność do długotrwałego współdziałania i zarządzania skutkami społecznymi, a nie wyłącznie „siła" odpowiedzi operacyjnej. Kampania „Ghostwriter" unaoczniła, że cyberoperacje i dezinformacja są instrumentami bezpośrednio oddziałującymi na bezpieczeństwo powszechne poprzez osłabianie wiarygodności komunikatów państwa i wykonalności działań ochronnych. Z kolei incydenty infrastrukturalne potwierdziły, że podatność infrastruktury na zakłócenia staje się dźwignią destabilizacji społecznej i funkcjonalnej państwa.

W konsekwencji należy uznać, że Ustawa OLiOC tworzy potrzebne ramy dla adaptacji systemu ochrony ludności do realiów zagrożeń hybrydowych, lecz nie stanowi rozwiązania samowystarczalnego. O jej realnej wartości zadecyduje praktyczne wdrożenie, w szczególności:

- zintegrowane planowanie i ćwiczenia obejmujące scenariusze hybrydowe (cyber, dezinformacja, sabotaż infrastruktury),
- trwałe mechanizmy współdziałania z operatorami infrastruktury i podmiotami społecznymi,
- rozwój narzędzi komunikacji kryzysowej i bezpiecznej łączności oraz
- systemowe budowanie odporności społecznej poprzez edukację i przygotowanie wspólnot lokalnych.

W tym sensie bezpieczeństwo powszechne i ochrona ludności w XXI wieku powinny być traktowane jako rdzeń polityki bezpieczeństwa państwa, a nie jej komponent peryferyjny – zwłaszcza w regionie Europy Środkowo-Wschodniej, gdzie presja poniżej progu wojny jest elementem trwałego środowiska strategicznego.

Bibliografia

Literatura

Śliwa Z., *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej 2021*, „Wiedza Obronna", 2022.

Filipec O., *Multilevel Analysis of the 2021 Poland-Belarus Border Crisis*, „Central European Journal of Politics", 2022.

Żurawski S., *Unia Europejska wobec kryzysu migracyjnego na granicy z Białorusią*, „Desecuritate", 2025.

Polski Instytut Spraw Międzynarodowych, *Kryzys graniczny jako przykład działań hybrydowych*, PISM, Warszawa 2022.

European Parliamentary Research Service, *EU-Belarus relations: State of play*, Brussels 2021.

Square V., *Behind the hack-and-leak scandal in Poland*, 2022.

Minister Koordynator Służb Specjalnych, *Findings regarding hacker attacks*, gov.pl, 2021.

National Security Archive, *The Ghostwriter Campaign*, George Washington University, 2021.

Greenberg, *The Cheap Radio Hack That Disrupted Poland's Railway System*,„Wired", 27.08.2023.

Zamecnik P., *The Border Crisis as an Example of Hybrid Warfare*, PISM, 2022.

Le Monde, *Poland makes 'East Shield' core of its military power ambitions*, 2025.

Reuters, *Polish army to help power grid protect key infrastructure*, 2025.

AP News, *NATO flexes its muscles and bulks up defenses on its eastern flank to ward off Russia*, 2025.

Le Monde, *Poland hit by unprecedented disinformation attack following Russian drone incursion*, 2025.