Rok sabotażu: czego uczą nas ataki na infrastrukturę Polski w latach 2023 – 2025 – i dlaczego potrzebujemy strategii odporności, a nie gaszenia pożarów.

Ostatnie dwa lata przyniosły Polsce falę incydentów sabotażowych i dywersyjnych, jakiej nie widzieliśmy od dekad. Zdarzenia, które jeszcze kilka lat temu wydawały się odległe – próby wysadzania torów kolejowych, ataki dronowe i ich zestrzeliwanie przez Wojsko Polskie i siły NATO, cybernetyczne ingerencje w systemy uzdatniania wody, manipulacje w oczyszczalniach ścieków czy próby zakłócania pracy terminala LNG – stały się elementem nowej normalności. Niezależnie od tego, iż każde z tych wydarzeń analizujemy osobno, to dopiero spojrzenie całościowe pozwala zrozumieć, że Polska znajduje się dziś na froncie rozproszonej, nisko-kosztowej, bez formalnego wypowiedzenia, prowadzonej z zamazywaniem sprawstwa wojny hybrydowej, której celem jest nie spektakularny atak, ale systemowa erozja odporności państwa.

Warto więc zebrać te incydenty w jedną mapę, nazwać wspólne elementy i odpowiedzieć uczciwie na pytanie: **czy działamy proaktywnie – czy jedynie reagujemy?**

Sabotaż fizyczny: kolej, drony, podpalenia, uszkodzenia infrastruktury na Morzu Bałtyckim.

Listopad 2025 przyniósł dwie próby uszkodzenia linii kolejowej nr 7 Warszawa–Lublin. Najpierw wysadzono fragment torów w rejonie miejscowości Mika, dzień później uszkodzono szynę w okolicach Gołębia, co zmusiło pociąg z kilkuset pasażerami do gwałtownego hamowania. **Władze mówią o działaniach zorganizowanych, powiązanych z rosyjską aktywnością dywersyjną.**

Kilka miesięcy wcześniej, 9–10 września, mieliśmy do czynienia z jednym z najbardziej symbolicznych ataków hybrydowych ostatnich lat. **Dwadzieścia jeden dronów rosyjskich naruszyło polską przestrzeń powietrzną**, przelatując nad kilkunastoma miejscowościami w kilku województwach. Część została zestrzelona, część spadła na terenach zamieszkałych. To był test – techniczny i psychologiczny – który pokazał, jak wyglądają przyszłe konflikty poniżej progu NATO-wskiego artykułu 5.

Wreszcie, maj 2024. Pożar ogromnego kompleksu Marywilska 44 w Warszawie, który przez pierwsze miesiące klasyfikowano jako „wypadek”. Dopiero wiosną 2025 rząd oficjalnie potwierdził wskazując, że było to najprawomocniej **podpalenie na zlecenie rosyjskich służb specjalnych** – przykład operacji o charakterze ekonomiczno-psychologicznym, mającej uderzyć w lokalny ekosystem biznesowy i

wywołać poczucie chaosu.

Ostatnie 2-3 lata obfitowały również w ataki na infrastrukturę na Morzu Bałtyckim. **Ataki dotyczyły głównie elementów takich jak linie telekomunikacyjne, kable energetyczne czy innego rodzaju elementy kluczowe dla infrastruktury krytycznej.** Szerzej opisałem te działania w artykule dla Instytutu Sobieskiego z 20 czerwca 2025 roku [1].

Cyberataki na infrastrukturę: woda, ścieki, baseny, kolej, energetyka

Rok 2025 to także eskalacja cyberdywersji na systemy OT [2] (Operational Technology). Prorosyjscy „haktywiści" i grupy powiązane z Federacją Rosyjską zyskały dostęp do paneli sterowania stacji uzdatniania wody i oczyszczalni ścieków w Małdytach, Tolkmicku, Sierakowie, Witkowie, Kuźnicy, Szczytnie czy Jabłonnie – manipulując poziomami zbiorników, pompami, alarmami. W tym samym czasie przejęto sterowanie oczyszczalnią ścieków w Witkowie i Chodaczowie, a w kilku innych miejscach ingerowano w parametry basenów – podnosząc temperaturę do 50°C, ustawiając pH na wartości skrajnie niebezpieczne.

Ataki dotknęły też sektor energetyczny. W październiku 2025 potwierdzono ingerencję w system sterowania stacją regazyfikacji LNG w Polsce. Prorosyjscy aktywiści opublikowali nagranie z panelu sterowania stacji LNG – gdzie widać na nim manipulacje parametrami technicznymi obiektu. Można dostrzec m.in. manipulowanie ciśnieniem: LNG w zbiorniku, azotu w butli czy też gazu przed układem redukcji. To najbardziej niebezpieczny incydent w obszarze kriogenicznym, jaki odnotowano od lat, choć szczegóły słusznie pozostają niejawne.

Uderzono również w systemy kolejowe. Na przełomie stycznia i lutego 2025 kampania ataków DDoS sparaliżowała sprzedaż biletów PKP Intercity, co w środku sezonu zakupowego było ciosem nie tylko operacyjnym, ale również reputacyjnym. Tego rodzaju działania to przede wszystkim narzędzia propagandowe. W odróżnieniu od ingerencji w automatykę przemysłową terminala LNG nie stanowią istotnego zagrożenia.

Patrząc na te wydarzenia osobno i wybiórczo, można odnieść wrażenie, że to przypadkowe, rozproszone epizody wynikające z nieuwagi, podatności systemów lub „zbiegu okoliczności". Niestety te incydenty tworzą **spójną matrycę celów i metod** [3], którą widzimy także w Finlandii, Estonii, na Łotwie, na Litwie, w Czechach i w Niemczech. Co warto podkreślić **Rosjanie robią trzy rzeczy**

jednocześnie:

1. **Podnoszą koszty funkcjonowania państwa.**

Każdy cyberatak wymusza inwestycje w OT, każdy dron – dodatkowe zakupy systemów przeciwdronowych i interceptorów, każdy sabotaż kolejowy – patrole, inspekcje, modernizacje, monitoring. Koszty rosną w sposób nieproporcjonalnie większy niż koszt samego ataku – który często jest minimalny.

2. **Przyspieszają erozję zaufania społecznego.**

Czy pociągi są bezpieczne? Czy woda w kranie jest czysta? Czy państwo panuje nad przestrzenią powietrzną? Tego rodzaju pytania, zaczynają krążyć w przestrzeni publicznej. A to właśnie **psychologiczna presja jest jednym z najskuteczniejszych narzędzi wojny hybrydowej**.

3. **Testują reakcję instytucji.**

Czas reakcji, komunikacja kryzysowa, koordynacja służb, zdolność do wskazania sprawcy oraz odpowiedzialnego za likwidację szkody – to elementy obserwowane przez przeciwnika w czasie rzeczywistym. Wnioski są jednoznaczne: **w latach 2024–2025 przeciwko Polsce prowadzono systematyczną kampanię sabotażowo-dywersyjną niskiej intensywności, poniżej progu otwartego konfliktu.**

Problem Polski: działamy reaktywnie, nie strategicznie.

Każdy z incydentów z ostatnich miesięcy – czy to próba wysadzenia torów, czy atak na infrastrukturę wodociągową – wywoływał falę komentarzy ekspertów i służb, które mówiły o „konieczności podjęcia działań”, „zwiększeniu czujności” lub „analizie ryzyka”. Po każdym takim ataku następują dyskusje i propozycje środków zaradczych, które jak widać są reaktywne i dalece niewystarczające. Mam wrażenie, że Polska niestety wciąż działa w logice: **„Dopóki się coś nie wydarzy, nie ruszamy systemowych zmian.”** To dokładnie odwrotność filozofii państw nordyckich, które zakładają, że incydent jest nie ostrzeżeniem, lecz potwierdzeniem trendu – i natychmiast wdrażają kolejne warstwy ochrony.

Istotnym elementem jest również próba predykcji i określenia tego, co może wydarzyć się w latach 2026–2027 oraz przygotowania się na takie scenariusze. Najbliższe lata będą czasem rosnącej presji hybrydowej na państwa NATO – w tym

na Polskę. Rosja, mimo osłabienia gospodarczego, będzie kontynuować operacje poniżej progu wojny, ponieważ są tanie, trudne do przypisania i strategicznie skuteczne. Trendy z lat 2024–2025 nie tylko się utrzymają, ale wejdą w bardziej zaawansowaną fazę.

W latach 2026–2027 należy więc oczekiwać **kontynuacji znanych metod działania**, stosowanych **częściej, równolegle i w sposób bardziej skoordynowany**, obejmujących nowe sektory i większą liczbę obiektów niż dotychczas. To, co do tej pory było incydentem jednostkowym, może przekształcić się w **ciągłą presję hybrydową**, prowadzącą do stopniowej erozji odporności państwa. Ataki nie będą spektakularne – będą **powtarzalne, niskokosztowe i trudne do przypisania**, co czyni je szczególnie efektywnymi.

W tym kontekście najważniejszym staje się pytanie nie czy dojdzie do kolejnych incydentów, lecz: **czy będziemy gotowi, zanim one nastąpią?**

W Polsce w chwili obecnej warto pomyśleć o implementacji elementów i środków, w których państwo pozostaje permanentnie spóźnione o pół kroku. Są to w pierwszej kolejności:

1. **centrum dowodzenia dla infrastruktury krytycznej i publicznej**, które działałoby 24/7;
2. **jednolity protokół reagowania dla ICS/OT** – sektor wod-kan, energetyka, transport i administracja mają różne standardy, często niekompatybilne;
3. **realny system predykcji zagrożeń** – analityka big data, AI, analiza anomalii zaszytych w systemy CCTV, integracja sensorów fizycznych i cyber etc.

Propozycja strategii odporności 2025–2030

Jeżeli chcemy wyjść z logiki „gaszenia pożarów”, musimy zbudować **strategię odporności warstwowej** – obejmującą fizyczną infrastrukturę, cyberbezpieczeństwo, procedury, wojsko oraz odporność społeczną.

1. **Fizyczna ochrona infrastruktury**

- sensory światłowodowe na kluczowych magistralach gazowych i energetycznych,
- stałe strefy antydronowe (NFZ + geofencing) wokół terminali LNG i budowanego FSRU, Naftoportu, tłoczni, węzłów kolejowych etc.
- modernizacja ochrony perymetrycznej obiektów wysokiej wartości: ogrodzenia,

bariery, kontrola dostępu, stała obecność formacji mundurowych.

2. **Cyberbezpieczeństwo OT/ICS** [4]

- rozdzielenie sieci biurowych i sterujących,
- obowiązkowy roczny audyt ICS/OT dla wodociągów, ciepłowni, kolei i energetyki,
- zespoły szybkiego reagowania OT – działające jak „straż pożarna cyber".

3. **System informacji i dowodzenia**

- jedno krajowe centrum odpowiedzialne za monitoring wszystkich sektorów IK,
- obowiązek raportowania incydentów w czasie rzeczywistym,
- integracja danych z ABW, SG, Policji, NASK i operatorów infrastruktury.

4. **Odporność społeczna** (wymaga także szerszego włączenia biznesu w komunikację kryzysową — jak wskazywaliśmy w naszym raporcie[5] o budowaniu odporności we współpracy z przedsiębiorcami, firmy dzięki własnym kanałom komunikacji i relacjom lokalnym mogą pełnić rolę wektorów szybkiego przekazywania informacji w sytuacjach zagrożeń).

- jasna, szybka komunikacja kryzysowa,
- krajowy program „SAFE CITY" dla samorządów – obejmujący wod-kan, transport, energetykę etc.
- minimalne standardy cyberbezpieczeństwa dla wszystkich spółek komunalnych.

5. **Współpraca międzynarodowa**

- integracja Naftoportu, infrastruktury Baltic Pipe, terminala LNG w Świnoujściu i strefy FSRU Gdańsk z systemem NATO Undersea Infrastructure Protection,
- udział Polski w unijnej platformie ochrony infrastruktury krytycznej (EU-CIP),
- wspólne ćwiczenia i wymiana doświadczeń z krajami basenu Morza Bałtyckiego.

Potrzebujemy strategii, która wyprzedza ruchy przeciwnika

Dywersja, sabotaż i działania w „strefie cienia" poniżej progu wojny w latach 2024–2025 to nie jednorazowe ataki – to **mapa zagrożeń**, która pokazuje, jak przeciwnik wykorzystuje nasze słabości proceduralne, technologiczne i organizacyjne. Nie chodzi już o to, czy kolejny incydent się wydarzy. Pytanie brzmi:

kiedy, gdzie i z jaką intensywnością. Jeżeli w 2025 roku reagujemy tylko wtedy, gdy pojawia się nowy nagłówek „atak”, to w 2027–2030 będziemy spóźnieni o lata. Polska potrzebuje strategii odporności, która nie patrzy w lustro wsteczne, ale wyprzedza ruch przeciwnika o kilka kroków. Bo w **wojnie hybrydowej wygrywa nie ten, kto gasi pożary, lecz ten, kto zapobiega ich powstaniu**. Dlatego – jeśli jeszcze tego nie zrobiono – należy niezwłocznie powołać **międzyresortowy, interdyscyplinarny zespół** złożony z przedstawicieli służb specjalnych, Wojska Polskiego, operatorów infrastruktury krytycznej, podmiotów kluczowych dla bezpieczeństwa gospodarczego, administracji państwowej i samorządów. Zespół ten powinien otrzymać zadanie pilnego wypracowania założeń do nowej strategii odporności – aktualizowanej na bieżąco, obejmującej zarówno część jawną, jak i niejawne mechanizmy operacyjne.

Elementem równie istotnym, co sama Strategia Odporności, jest zagwarantowanie jej realnego wdrożenia. Dokument — nawet najlepszy — pozostanie jedynie papierowym opracowaniem, jeśli nie będzie mu towarzyszył mechanizm stałego, cyklicznego monitorowania postępów i jakości implementacji. Doświadczenia państw, które skutecznie budują odporność instytucjonalną, pokazują jednoznacznie: **przygotowanie strategii to zaledwie początek pracy.** Prawdziwym wyzwaniem jest jej konsekwentne wdrażanie w „żywych organizmach” instytucji publicznych, samorządów, operatorów infrastruktury i przedsiębiorstw. To proces wymagający dyscypliny, współpracy międzysektorowej, zdolności adaptacji i regularnego audytu skutków podejmowanych działań.

Na sam koniec mam nadzieję, że moje refleksje — choć konieczne — są spóźnione; że odpowiednie zespoły, procedury i plany działania już funkcjonują, choć z oczywistych względów nie mogą być publicznie znane. Jeśli tak jest, to dobrze — bo oznacza to, że Polska już dziś buduje odporność, której w świecie rosnącej presji hybrydowej nie da się tworzyć ad hoc. Jeśli jednak takich mechanizmów jeszcze nie ma, to najwyższy czas na ich pilne powołanie i wdrożenie.

---

[1] https://sobieski.org.pl/bezpieczenstwo-morza-baltyckiego/

[2] Zgodnie z analizami CSIRT/NASK i https://cyberdefence24.pl/cyberbezpieczenstwo/atak-prorosyjskiej-grupy-na-polska-stacje-regazyfikacji-lng

[3] https://www.polskieradio.pl/395/7784/Artykul/3597357,official-says-russian-sabotage-in-poland-a-form-of-terrorism

[4] ICS – Industrial Control Systems; OT – Operational Technology

[5] Instytut Sobieskiego, *Jak zbudować odporność państwa we współpracy z przedsiębiorcami*, 2025; https://sobieski.org.pl/wp-content/uploads/X-2025-Jak-Zbudowac-Odpornosc-Panstwa-We-Wspolpracy-Z-Przedsiebiorcami.pdf

---