



Redakcja: Grzegorz Gil (dyrektor IEŚ), Anton Saifullayeu
(zastępca dyrektora IEŚ), Agnieszka Zajdel (sekretarz redakcji),
Spasimir Domaradzki, Bartłomiej Krzysztan, Damian Szacawa,
Agata Tatarenko

Nr 1708 (213/2026) | 30.09.2026

ISSN 2657-6996
© IEŚ

Jakub Olchowski

Rosyjska presja na Europę. Między sabotażem a dezinformacją

Rosyjskie działania wobec Europy coraz wyraźniej wykraczają poza pojedyncze akty sabotażu, cyberataki czy operacje dezinformacyjne. Ich znaczenie wynika z łączenia różnych instrumentów w ramach szerszej strategii osłabiania Zachodu i ograniczania jego wsparcia dla Ukrainy. Działania państw europejskich pozostają jednak w dużej mierze reaktywne – inicjatywa jest po stronie Rosji. Skuteczna przeciwwaga wymaga więc nie tylko wzmacniania odporności, lecz także zmiany sposobu definiowania samego zagrożenia.

Intensyfikacja działań Federacji Rosyjskiej wobec Europy. Od lata 2025 r. obserwowana jest intensyfikacja działań Rosji wobec państw europejskich. Obejmuje ona szerokie spektrum aktywności – od aktów sabotażu i ataków na infrastrukturę krytyczną, przez działania wymierzone w europejski przemysł obronny, po cyberataki i naruszanie przestrzeni powietrznej państw NATO ([„Komentarze IEŚ”, nr 1703](#)). Podmioty powiązane z Rosją podejmują próby sabotażu infrastruktury krytycznej, w tym polskiej infrastruktury kolejowej, a także prowadzą kampanię podpaleń obiektów związanych z przemysłem obronnym, produkujących wyposażenie zarówno dla europejskich armii, jak i dla Ukrainy. Europejskie służby wywiadowcze i media informują również o próbach zamachów na przedstawicieli kierownictwa europejskich firm zbrojeniowych. Równolegle rosyjskie podmioty regularnie przeprowadzają cyberataki na cele rządowe i cywilne. Do tego dochodzą incydenty związane z wtargnięciami dronów i rakiet oraz naruszeniami przestrzeni powietrznej m.in. Polski, Niemiec, Danii, Rumunii, Mołdawii, Litwy, Łotwy i Estonii, a także działania w rejonie Arktyki (Norwegii).

Skala i charakter tych działań powodują, że służby wywiadowcze wielu państw, w tym Stanów Zjednoczonych, wskazują na wysokie prawdopodobieństwo ich dalszej eskalacji. Wedle tych ocen w nadchodzących miesiącach Rosja najprawdopodobniej zwiększy częstotliwość działań hybrydowych wymierzonych w państwa Zachodu, a ich konsekwencje mogą być poważniejsze niż dotychczas. Szczególne znaczenie mogą mieć działania zmierzające do ograniczenia wsparcia dla Ukrainy jeszcze przed jego dostarczeniem, m.in. poprzez sabotaż przedsięwzięć zbrojeniowych oraz transportów kolejowych przewożących uzbrojenie. Możliwe są również cyberataki mające na celu zakłócenie kluczowych funkcji państwa.

Ostrzeżenia dotyczą jednak nie tylko dalszego rozwoju działań hybrydowych. Mimo że otwartą agresję Rosji uważa się za bardzo mało prawdopodobną, nie wyklucza się jednak, że Rosja może się zdecydować na ograniczony atak militarny, z użyciem lądowych sił zbrojnych, przeciwko jednemu lub kilku państwom NATO z nią graniczącym. Rosja rozbudowuje także infrastrukturę wojskową i tworzy nowe jednostki w pobliżu północnej i wschodniej flanki NATO, zwiększając tym samym swoje możliwości wywierania presji, prowadzenia działań hybrydowych, a w dłuższej perspektywie także operacji konwencjonalnych¹.

Istota i cel działań. Rosyjskie działania wobec Europy należy postrzegać jako skoordynowane oddziaływanie prowadzone równolegle w wielu domenach – militarnej, informacyjnej, cybernetycznej, politycznej i społecznej. Określanie ich mianem „działań hybrydowych” jest użyteczne, ale wymaga ostrożności, ponieważ termin ten, nadużywany w ostatnich latach przez media i polityków, stał się bardzo szeroki i bywa stosowany do opisu niemal

¹ W tym kontekście Institute for the Study of War przygotował również scenariusz ograniczonej rosyjskiej operacji militarnej wobec Estonii: *What a Limited Russian Incursion Into Estonia Might Look Like: A Narva Scenario*, <https://understandingwar.org/research/defense-of-europe/what-a-limited-russian-incursion-into-estonia-might-look-like-a-narva-scenario/> [29.09.2026].



każdej aktywności znajdującej się „pomiędzy wojną a pokojem”. Istotą rosyjskiego podejścia nie jest jednak sam „hybrydowy” charakter poszczególnych działań, lecz umiejętne łączenie różnych instrumentów w sposób pozwalający osiągać efekty strategiczne przy ograniczaniu ryzyka otwartej konfrontacji oraz przy wykorzystaniu relatywnie niewielkich zasobów.

Taka logika jest głęboko zakorzeniona w rosyjskiej myśli i kulturze strategicznej. Granica między stanem wojny i stanem pokoju ma charakter płynny, a presja na przeciwnika może być wywierana także bez formalnego rozpoczęcia konfliktu². Dlatego działania kinetyczne są uzupełniane (lub poprzedzane) działaniami niekinetycznymi, m.in. informacyjnymi i cybernetycznymi. Ich znaczenie polega nie tylko na bezpośrednich skutkach, ale przede wszystkim na wpływaniu na percepcję zagrożeń, zachowania społeczne i decyzje polityczne państw zachodnich. Działania te są przy tym dostosowywane do specyfiki konkretnego państwa. W przypadku Polski jest to np. narracja przedstawiająca agresywne działania Rosji jako „ukraińskie prowokacje” mające na celu „wciągnięcie Polski do wojny”³.

Kampaniom propagandowym i dezinformacyjnym towarzyszą zatem cyberataki, akty sabotażu oraz działania wymierzone w infrastrukturę krytyczną – od energetyki i transportu po sieci teleinformatyczne, obiekty przemysłowe i zaplecze logistyczne. Poszczególne incydenty mogą mieć ograniczoną skalę, ale ich kumulacja może tworzyć wrażenie narastającego chaosu i utraty kontroli nad sytuacją.

Działania „poniżej progu wojny” pozwalają Rosji oddziaływać na społeczeństwa państw europejskich bez konieczności bezpośredniego atakowania ich terytorium. Ich celem jest wywoływanie strachu i poczucia zagrożenia, pogłębianie istniejących podziałów społecznych, wzmacnianie teorii spiskowych oraz podważanie zaufania do instytucji państwa i struktur międzynarodowych (przede wszystkim NATO i UE). Istotny jest komponent emocjonalny: w sytuacji kryzysowej emocje zwiększają podatność części odbiorców na manipulacje, które mogą generować kryzysy polityczne i społeczne.

W tym sensie celem rosyjskiego oddziaływania nie musi być samo wyrządzenie szkody. Równie ważne jest doprowadzenie do sytuacji, w której społeczeństwo zaczyna kwestionować zdolność własnego państwa do zapewnienia bezpieczeństwa, a presja społeczna ogranicza swobodę działania władz. Uderzenie w zaufanie do państwa może być więc równie istotne jak uderzenie w jego infrastrukturę – możliwe jest osiągnięcie efektu politycznego bez konieczności prowadzenia klasycznej operacji wojskowej.

Na poziomie strategicznym działania te wpisują się w dwa powiązane ze sobą cele. Po pierwsze, Rosja ma świadomość, że nie pokona militarnie Ukrainy, dopóki będzie ona wspierana przez Zachód – należy zatem doprowadzić do zahamowania zachodniej pomocy. Po drugie, chodzi o osłabienie samego Zachodu – jego spójności, odporności społecznej i zdolności do wspólnego reagowania. Obejmuje to m.in. działania zmierzające do pogłębiania podziałów w NATO i UE oraz wzmacniania radykalnych, populistycznych i skrajnie nacjonalistycznych środowisk.

Największe znaczenie ma zatem nie pojedynczy cyberatak, kampania dezinformacyjna czy akt sabotażu, lecz ich potencjalna kumulacja i wzajemne wzmacnianie się. Rosja może jednocześnie oddziaływać na infrastrukturę, przestrzeń informacyjną, nastroje społeczne i proces decyzyjny państw europejskich. Taka kombinacja instrumentów pozwala jej zwiększać koszty wspierania Ukrainy, testować odporność Zachodu i stopniowo podważać jego spójność bez konieczności podejmowania decyzji o otwartej wojnie z państwami NATO.

Zachód w defensywie. Państwa europejskie funkcjonują na podstawie procedur pokojowych. Dotyczy to zarówno przygotowania militarnego i trybu funkcjonowania sił zbrojnych, jak i odporności społecznej. Przez dekady zaniedbywano m.in. obronę cywilną i przygotowanie społeczeństw do funkcjonowania w warunkach kryzysu.

² Przykładem jest koncepcja „wojny buntowniczej” (*мятеж-война*) Jewgienija Messnera.

³ Nieprzypadkowo jedną z najczęstszych narracji stosowanych w rosyjskich działaniach kognitywnych jest oskarżanie krytyków Rosji o „podżeganie do wojny” – jest to kontynuacja retoryki z okresu zimnej wojny – wówczas „podżegaczem wojennym” także był „agresywny, imperialistyczny Zachód”.



Przewaga Rosji jest szczególnie widoczna w sferze niekinetycznej. Demokracje europejskie, oparte na wolności słowa i pluralizmie, tworzą otwartą przestrzeń informacyjną, którą Rosja wykorzystuje do prowadzenia operacji wpływu i pogłębiania istniejących podziałów. Problemem jest również tempo reakcji. Zanim instytucje zweryfikują informacje i przedstawią oficjalne stanowisko, przestrzeń informacyjna jest już wypełniona dezinformacją i teoriami spiskowymi. Państwo często reaguje więc na narrację, która zdążyła już ukształtować społeczne postrzeganie wydarzenia.

Dodatkowym wyzwaniem pozostaje atrybucja. Cyberataki, akty sabotażu czy operacje wpływu trudno jednoznacznie przypisać konkretnemu sprawcy, a proces weryfikacji wymaga czasu. Jednocześnie kwestie bezpieczeństwa są często wykorzystywane instrumentalnie w bieżącej rywalizacji politycznej, co utrudnia wypracowanie długofalowej i spójnej odpowiedzi.

W efekcie reakcja państw zachodnich niejednokrotnie sprowadza się jedynie do ostrzeżeń, deklaracji i działań podejmowanych już po wystąpieniu incydentu. Daje to dodatkową przewagę Rosji, która działa szybko, niejawnie i jednocześnie w wielu domenach.

Co robić? Konfrontacja z Rosją w cyberprzestrzeni i infosferze już trwa. Państwa zachodnie nie mogą traktować rosyjskich działań jako serii odizolowanych czy przypadkowych incydentów. Określenie „wojna hybrydowa” staje się eufemizmem, który może bagatelizować skalę i charakter problemu. Konieczne jest wspólne zdefiniowanie zagrożenia i uznanie, że skoordynowane działania kinetyczne i niekinetyczne stanowią element szerszej strategii Rosji wobec Europy, której cele wykraczają daleko poza Ukrainę.

Stąd potrzeba wspólnej, długofalowej strategii NATO i państw europejskich, opartej na analizie wzajemnych powiązań rosyjskich działań, a nie na reagowaniu na pojedyncze incydenty. Brak zdecydowanej reakcji może być przez Rosję odczytywany jako przyzwolenie na dalszą eskalację. W perspektywie może to oznaczać nasilanie operacji wpływu, mobilizowanie rosyjskich zasobów wywiadowczych i sieci współpracowników, a następnie kolejne działania sabotażowe i cyberataki wymierzone w infrastrukturę krytyczną – energetykę, banki, wodociągi czy systemy ciepłownicze.

Odpowiedź winna obejmować nie tylko ochronę infrastruktury, lecz także budowanie odporności społecznej. Kluczowe znaczenie mają edukacja i świadomość zagrożeń, ponieważ to społeczeństwo jest jednym z głównych celów rosyjskich działań dezinformacyjnych. Potrzebne są również stałe szkolenia instytucji publicznych, rozwój zdolności obrony cybernetycznej oraz konsekwentne stosowanie obowiązującego prawa. Istotnym elementem pozostaje także skuteczniejsza regulacja platform internetowych, zarówno na poziomie Unii Europejskiej, jak i państw członkowskich. Media społecznościowe stały się bowiem jednym z podstawowych narzędzi prowadzenia operacji wpływu.