FUNDACJA IM. KAZIMIERZA PUŁASKIEGO

Agenci chaosu: ukryta kampania przeciwko Zachodowi

Wojna kognitywna i ofensywne operacje rosyjskich oraz białoruskich służb specjalnych

Wrzesień 2025

Maciej Filip Bukowski

Maciej Filip Bukowski

Agenci chaosu: ukryta kampania przeciwko Zachodowi

Wojna kognitywna i ofensywne operacje rosyjskich oraz białoruskich służb specjalnych

Fundacja im. Kazimierza Pułaskiego / Warszawa 2025

AUTOR Maciej Filip Bukowski

WYDAWCA Fundacja im. Kazimierza Pułaskiego
ul. Oleandrów 6, 00-629 Warszawa
www.pulaski.pl

PROJEKT GRAFICZNY Dobry Skład

Dofinansowano ze środków Centrum Dialogu
im. Juliusza Mieroszewskiego

Centrum Mieroszewskiego

Spis treści

Streszczenie wykonawcze / 5

1 OD „ZIELONYCH LUDZIKÓW" DO WOJNY UMYSŁÓW: ROZWÓJ ZAGROŻEŃ HYBYDOWYCH KU WOJNIE KOGNITYWNEJ / 7

2 WOJNA KOGNITYWNA I WSCHODNI KANON ZAKŁÓCEŃ / 9

Kluczowi myśliciele / 10

Kluczowe cele strategiczne / 12

Kluczowe taktyki wywiadowcze / 13

Kluczowe koncepcje operacyjne / 15

3 RAMY KONCEPCYJNE DZIAŁAŃ PROWADZONYCH PRZEZ ROSYJSKIE I BIAŁORUSKIE SŁUŻBY SPECJALNE / 16

Poziom 1: Infiltracja kognitywna / 17

Poziom 2: Tokenizacja wykonawców / 18

Poziom 3: Intensyfikacja skalowalnych zakłóceń / 19

4 TYPOLOGIA OPERACJI: OD PODPALEŃ PO FAŁSZYWE NARRACJE / 20

Sabotaż i Dywersja / 20

Outsourcing szpiegostwa / 23

Operacje kognitywne i dezinformacja / 25

Instrumentalizacja diaspor / 27

Nowe możliwości dzięki postępom technologicznym oprogramowania / 30

Nowe możliwości dzięki postępom technologicznym w sprzęcie komputerowym / 32

Czas: pięć faz w cyklach narracyjnych i operacyjnych / 34

5 MARTWE PUNKTY, BŁĘDY ADAPTACYJNE I JAK JE NAPRAWIĆ / 35

Deficyt poznawczy: brak zintegrowanego rozumienia zagrożeń / 36

Luka systemowa: fragmentacja kontrwywiadu, cyberbezpieczeństwa i polityki wewnętrznej / 37

Deficyt interoperacyjności: silosy danych między służbami państw członkowskich / 38

Próżnia regulacyjna: brak skutecznych instrumentów prawnych do przeciwdziałania obcym wpływom / 39

Odwrócenie ról: legalne działania hybrydowe przeciwko Rosji i Białorusi / 40

Polska: ograniczenia krajowe i potrzeba instytucjonalnej zmiany paradygmatu / 42

6 ZAKOŃCZENIE / 44

Recenzja 1 oraz komentarz: dr Anna Grabowska-Siwiec / 45

Recenzja 2: Grzegorz Małecki / 48

Streszczenie wykonawcze

W 2025 roku przestrzeń transatlantycka znajduje się pod trwałym atakiem nie w formie otwartej wojny, lecz poprzez rozproszoną, skoordynowaną ofensywną kampanię kognitywną i zakulisowych działań destabilizacyjnych. Rosyjskie i białoruskie służby wywiadowcze wdrożyły hybrydową strategię łączącą dywersję, sabotaż, działania o charakterze terrorystycznym, manipulację psychologiczną oraz infiltrację narracyjną w długofalowy plan osłabiania odporności Zachodu. Jej celem jest rozbicie zaufania, rozkruszenie spójności oraz erozja zdolności wspólnego rozumienia rzeczywistości – zarówno wewnątrz państw NATO, jak i w obrębie samego sojuszu. Nie jest to kampania mająca na celu zajęcie terytorium, lecz taka, której zadaniem jest osłabianie poznawczych mechanizmów obronnych społeczeństw, oraz rozbicie społeczeństw i tworzenie antagonistycznych grup destabilizujących państwa od wewnątrz.

Niniejszy raport pokazuje, że nie są to incydentalne akty szpiegostwa, sabotażu czy dywersji, lecz elementy spójnej architektury wojny kognitywnej. Rosja i Białoruś połączyły teorię kontroli refleksyjnej, inżynierię narracji oraz sieciową dezinformację w doktrynę wymierzoną w fundamenty mentalne i emocjonalne społeczeństw Zachodu. Poniższa analiza koncentruje się na Europie, ze szczególnym uwzględnieniem Polski, państw bałtyckich oraz wybranych krajów Europy Zachodniej, gdzie operacje te najpełniej ilustrują skalę i logikę wojny prowadzonej poniżej progu artykułu 5 Traktatu NATO, lecz niosącej egzystencjalne konsekwencje.

Raport identyfikuje trzy wzajemnie uzupełniające się poziomy tej kampanii:

1. **Infiltracja kognitywna** – przenikanie do dyskursu publicznego i ekosystemów cyfrowych narracji o dużym ładunku psychologicznym i memetycznym, które podważają zaufanie do instytucji, zacierają granicę między prawdą a fikcją oraz wywołują pobudzenie, a następnie zmęczenie emocjonalne.
2. **Tokenizacja wykonawcza** – zdecentralizowana rekrutacja nieświadomych lub jednorazowych wykonawców do przeprowadzania aktów sabotażu fizycznego, takich jak podpalenia magazynów czy rozpoznanie dronowe. Zapewnia to wiarygodną zaprzeczalność przy jednoczesnej możliwości skalowania działań poprzez tzw. agenturę proxy [1] [2].
3. **Zakłócenia poprzez mikrooperacje** – rozproszone, lecz kumulatywne działania o niskiej intensywności są synchronizowane z wojną informacyjną tak, aby potęgować chaos, wywoływać paraliż oraz przeciążać zachodnie systemy reagowania kryzysowego.

Raport dowodzi, że Zachód musi odejść od czysto reaktywnej postawy. Defensywna logika wywiadowcza jest niewystarczająca wobec przeciwnika, który uderza w percepcję, emocje i sam proces podejmowania decyzji. Niezbędne jest wypracowanie wyważonej postawy ofensywnej, traktującej bezpieczeństwo poznawcze jako kluczowy element obrony narodowej i sojuszniczej.

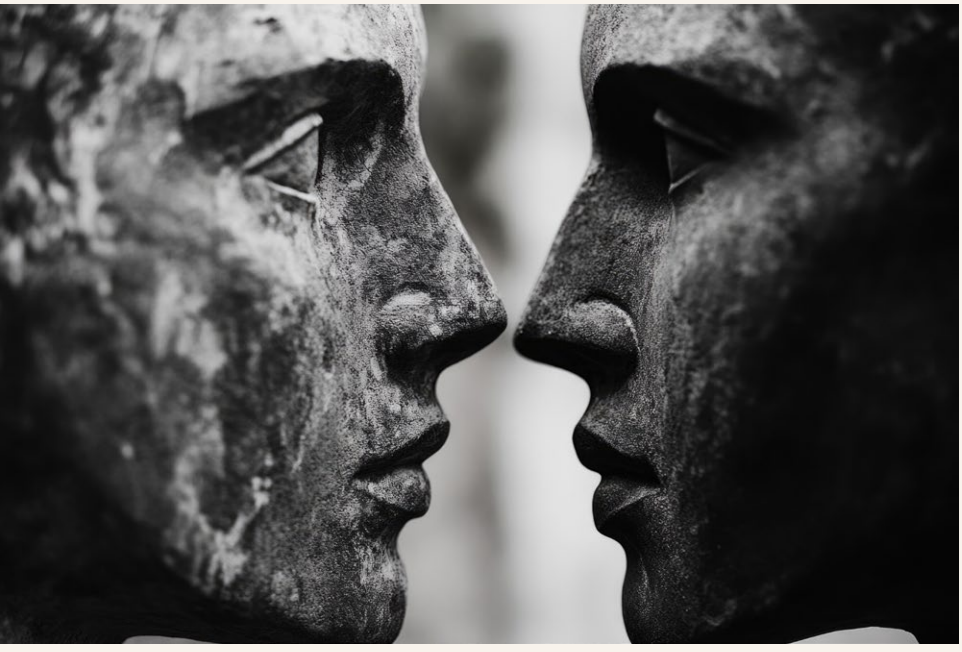
Najważniejsze rekomendacje obejmują:

- Utworzenie systemu wczesnego ostrzegania kognitywnego, łączącego dane z otwartych źródeł, narzędzia oparte na sztucznej inteligencji, analizę narracji i monitorowanie trendów emocjonalnych;
- Aktywizację aktywów kontrwywiadowczych w diasporach poprzez mobilizację rosyjskich i białoruskich środowisk emigracyjnych jako węzłów oporu – zarówno operacyjnych, jak i symbolicznych;
- Stworzenie europejskiego rejestru podmiotów wpływu zagranicznego i manipulacji percepcyjnej, wzorowanego na FARA, ale dostosowanego do specyfiki zagrożeń hybrydowych;
- Stosowanie ukierunkowanych kontr-narracji i kontrolowanych kampanii zakłóceń z wykorzystaniem inwersji symbolicznej, taktyk memetycznych i elastycznej komunikacji;
- Instytucjonalizację symulacji wojny kognitywnej w ramach planowania kryzysowego NATO i UE, aby odzwierciedlały one przekrojowy charakter współczesnych zagrożeń hybrydowych.

Ostatecznie skuteczność trwającej ofensywy hybrydowej zależy nie od siły kampanii toczonej przez Rosję i Białoruś, lecz od inercji Zachodu. Zwycięży ten, kto zrozumie, że polem bitwy nie jest terytorium, lecz zaufanie. Jasność postawy i spójność społeczna muszą być traktowane nie jako ideały, ale jako zasadnicze zasoby strategiczne, które należy chronić i wzmacniać.

1 Od „zielonych ludzików” do wojny umysłów: Rozwój zagrożeń hybydowych ku wojnie kognitywnej

Koncepcja wojny hybrydowej ewoluowała od modelu opartego na nieregularnych taktykach wojskowych i ograniczonej dezinformacji do wielowarstwowej strategii wymierzonej w poznawcze fundamenty społeczeństw demokratycznych. To, co zaczęło się od pojawienia się nieoznakowanych żołnierzy podczas aneksji Krymu i użycia oddziałów proxy w Donbasie, rozwinęło się w kampanię mającą na celu destabilizację percepcji społecznej, zakłócenie spójności emocjonalnej oraz korozję samego procesu, w którym społeczeństwa odróżniają prawdę od fałszu.



W początkowej formie wojna hybrydowa koncentrowała się na **niejednoznaczności fizycznej [3] [4] [5]**. Niezidentyfikowani aktorzy zajmowali infrastrukturę, manipulowali lokalnymi konfliktami politycznymi i poprzez mechanizm tzw. wiarygodnego zaprzeczenia zaciemniali odpowiedzialność państwa zlecającego [6]. Operacje te wykorzystywały zamieszanie w strefach prawno-wojskowych, które definiują reakcje poniżej progu otwartego konfliktu. Ich celem był wpływ materialny bez konieczności prowadzenia wojny konwencjonalnej. Kluczowy przykład stanowi szereg operacji poprzedzających nielegalne zajęcie Krymu przez Rosję [7] [8] [9].

Jednak z czasem, i wraz z rozwojem technologii, punkt ciężkości działań przeciwnika przesunął się ku **niejednoznaczności psychologicznej**. Dziś rosyjskie i białoruskie strategie hybrydowe dążą nie tylko do ukrycia sprawcy, lecz także do tego, aby sam atak był nierozróżnialny od wewnętrznych dysfunkcji państwa i społeczeństwa. To podejście uderza w percepcję, interpretację i emocje. Jego celem jest rozbicie wspólnej i spójnej rzeczywistości społecznej i zalanie jej sprzecznościami, fałszywymi wyborami oraz poczuciem zmęczenia. Ma ono wywoływać chaos i wyczerpanie, a nie wymuszać posłuszeństwo siłą.

W tej nowej fazie zagrożenia hybrydowe opierają się mniej na zajmowaniu budynków czy linii transportowych, a bardziej na okupowaniu przestrzeni informacyjnej i emocjonalnej. Stosowane są przemyślane narracje, destabilizujące

pogłoski, zmanipulowane obrazy oraz algorytmicznie wzmacniane fale emocji, które mają zaszczepić niepewność na każdym poziomie życia demokratycznego. Celem nie jest już tylko przewaga strategiczna, lecz **epistemiczny nieład**. Społeczeństwa, które nie potrafią uzgodnić, co jest rzeczywiste, nie są w stanie przed takimi działaniami skutecznie się bronić.

Ta transformacja ma głębokie konsekwencje. Oznacza, że służby wywiadowcze, operacje wpływu i technologie informacyjne stały się instrumentami ofensywy przeciwnika. Oznacza to również, że tradycyjne ramy odstraszania, oparte na widoczności i proporcjonalności, są niewystarczające wobec aktora działającego niejako niewidzialnie i w rozproszeniu. Wojna prowadzona dziś przeciwko Zachodowi przeniosła się z tradycyjnego pola bitwy do ludzkiego umysłu, a jej wygranie wymaga traktowania poznania nie jako dodatku, lecz jako głównego celu wrogich działań. Służby specjalne, które tradycyjnie działały w cieniu, dziś coraz częściej rezygnują z metody wiarygodnego zaprzeczania, a ich działania są praktycznie jawne.

2 Wojna kognitywna i wschodni kanon zakłóceń

Rosyjska oraz – *ex consequenti* – białoruska koncepcja wojny kognitywnej ma charakter instrumentalny, a nie teleologiczny. Jej ostatecznym celem pozostaje ekspansja geopolityczna oraz rewizja porządku międzynarodowego. Arsenał kognitywny nie jest celem samym w sobie, lecz środkiem do paraliżowania oporu, erozji spójności oraz kształtowania pola walki na długo przed eskalacją kinetyczną czy polityczną. Strategie wywiadowcze Rosji i Białorusi opierają się na dorobku teoretycznym, który pełni funkcję nie ideologii, lecz zestawu narzędzi. Kanon ten łączy postsowiecką myśl wojskową z postmodernistycznymi strategiami wojny percepcyjnej i kontroli narracji. Doktryny te traktują umysły jako teren walki, a emocje, zmęczenie i dezorientację jako broń. Poniżsi teoretycy tworzą intelektualne rusztowanie współczesnych operacji wpływu, zakulisowych ingerencji i zakłóceń psychologicznych.

Kluczowi myśliciele

Jewgienij Messner [10] [11] [12]

Carski oficer, a następnie teoretyk na emigracji, rozwinął koncepcję *мятежная война* („wojny buntowniczej"), ujmując współczesny konflikt jako rebelię toczącą się wewnątrz psychiki społeczeństw. Twierdził, że wojny nie będą toczyć się o terytorium ani dominację armii, lecz poprzez zanikanie cywilizacyjnej woli. Strach, dezorientacja i utrata lojalności w jego myśli stanowią w tym sensie broń najskuteczniejszą. Teoria Messnera, rozwijana na emigracji w Argentynie, przewidywała wojnę hybrydową na dziesięciolecia przed jej doktrynalnym skodyfikowaniem w Rosji.

Zdjęcie: trybun.org.pl

Igor Panarin [13] [14] [15]

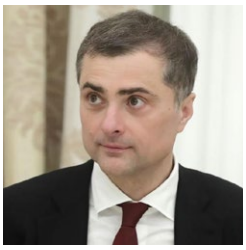
Były analityk KGB i naukowiec, Panarin rozwinął koncepcję wojny informacyjno-psychologicznej stanowiącej ciągłą i uprawnioną formę dyplomacji. W swoich pracach, m.in. „*Wojna informacyjna i Geopolityka*" (1999), opowiada się za prewencyjnym nasycaniem przestrzeni narracyjnej w celu kształtowania percepcji przeciwnika, stabilizacji opinii publicznej oraz tworzenia psychologicznej strefy buforowej. Panarin normalizuje militaryzację mediów jako standardowe zachowanie międzypaństwowe i wzywa do permanentnej gotowości w domenie kognitywnej.

Zdjęcie: Wikipedia

Gleb Pawłowski [16] [17] [18] [19]

Dawny dysydent sowiecki, później technolog polityczny Kremla. Pawłowski opracował doktrynę „demokracji sterowanej" oraz koncepcję „polityki wirtualnej". Według jego koncepcji skuteczna strategia powinna zalewać środowisko informacyjne starannie dobranymi sprzecznościami, rozbijając dyskurs polityczny na performatywny chaos. Metoda Pawłowskiego nie opiera się na kontroli narracji poprzez cenzurę, lecz na tworzeniu apatii emocjonalnej i wyczerpania epistemicznego za pomocą medialnego teatru.

Zdjęcie: Wikipedia



Władisław Surkow [20] [21]

Surkow, dramaturg i zarazem rozgrywający polityczny, sformalizował metodologię chaosu jako narzędzia rządzenia. W anglojęzycznym artykule *Samotność półkrwi* (*The Loneliness of the Half-Breed*) kreśli wizję polityki nielinearnej, w której to państwo aranżuje sprzeczne narracje tak, by neutralizować opór i tworzyć epistemiczną zależność. Wizja Surkowa łączy sprzeczności i niejednoznaczności mające ukształtować społeczeństwo, w którym każda wersja prawdy jest prawdopodobna, ale żadna nie jest możliwa do wykorzystania.

Zdjęcie: Wikipedia

Aleksandr Dugin [22] [23] [24] [25]

Dugin, ideolog eurazjanizmu, postrzega informację nie jako propagandę, lecz jako narzędzie wojny metafizycznej. W *Czwartej teorii politycznej* opowiada się za konfliktem cywilizacyjnym, w którym liberalizm zostaje rozmontowany poprzez infekcję kulturową, religijną i psychologiczną. Informacja, strach, mit i archetypy religijne mają służyć podważeniu ontologii opartych na Oświeceniu. Choć wpływ instytucjonalny Dugina bywa kwestionowany, jego poglądy dot. uwarunkowań cywilizacyjnych przenikają sieci wojskowo-intelektualne i media nacjonalistyczne w całym aparacie państwowym Rosji.

Zdjęcie: Wikipedia

Valeri Gierasimow [26]

Generał i od 2012 roku szef Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, w artykule *The Value of Science Is in the Foresight* opublikowanym w 2013 roku wskazał, że współczesne konflikty opierają się w coraz większym stopniu na działaniach pozamilitarnych. Jego koncepcja, nazwana „nowym podejściem do osiągania celów polityczno-wojskowych", zakłada użycie środków politycznych, gospodarczych, informacyjnych i społecznych w taki sposób, aby wywoływać destabilizację przeciwnika i osłabiać jego odporność zanim dojdzie do otwartej konfrontacji zbrojnej. Tego rodzaju operacje mają być prowadzone permanentnie i w połączeniu z ograniczonymi działaniami militarnymi, co tworzy charakterystyczną szarą strefę pomiędzy pokojem a wojną.

Photo source: Wikipedia

Kluczowe cele strategiczne

Celem Rosji nie jest jedynie klasyczna ekspansja terytorialna, lecz **parytet przez odejmowanie** – zmniejszenie dystansu wobec Zachodu poprzez szybszą degradację jego spójności, zdolności i klarowności niż tempo reform wewnętrznych Rosji. Jak wskazywał Timothy Snyder w *Drodze do niewolności*, gdy Kreml uświadomił sobie, że konwergencja z Zachodem jest nieosiągalna, zwrócił się ku strategii rozkładu od wewnątrz, starając się ukazać demokracje liberalne jako chaotyczne, wewnętrznie sprzeczne i niegodne naśladowania.

Cele strategiczne Rosji i Białorusi obejmują: zachowanie reżimu, odbudowę uprzywilejowanej strefy wpływów, osłabienie i wyczerpanie wsparcia dla Ukrainy oraz stworzenie sprzyjającego środowiska bezpieczeństwa, w którym przymus poniżej progu otwartego konfliktu staje się normą. Operacyjnie przekłada się to na erozję zaufania do instytucji, fragmentację cykli decyzyjnych UE i NATO oraz narzucanie kosztów tarcia w obszarze innowacji, logistyki i reagowania kryzysowego.

Sukces mierzony jest nie publicznymi zwycięstwami, lecz opóźnioną atrybucją, wydłużeniem czasu reakcji, rosnącymi kosztami obrony oraz powtarzającym się paraliżem politycznym. Białoruś pełni funkcję platformy pomocniczej i bufora ryzyka, poszerzając zasięg działań przy jednoczesnym rozproszeniu odpowiedzialności. To wyjaśnia, dlaczego wysiłki kognitywne, kryminalne i kinetyczne, którym atakujący zaprzecza, są synchronizowane w celu utrzymywania atakowanego w postawie reaktywnej, oraz wprowadzania społeczeństw w stan zmęczenia emocjonalnego.

Kluczowe taktyki wywiadowcze

Rosyjskie i białoruskie służby specjalne funkcjonują jako rozproszony ekosystem, w którym każda instytucja rozwija własną specjalizację. Celowo jednak utrzymywane są obszary nakładania się kompetencji, by zapewnić redundancję i wiarygodną zaprzeczalność. Zrozumienie tego podziału ról jest kluczowe w mapowaniu wektorów zagrożeń hybrydowych.

Federalna Służba Bezpieczeństwa (FSB) pełni funkcję zarówno kontrwywiadu wewnętrznego, jak i operatora zewnętrznego. Jej główne zadania są wewnątrz Rosji, lecz FSB prowadzi także szerokie operacje zagraniczne, korzystając z przykrycia dyplomatycznego, szczególnie w Europie Środkowej i Wschodniej. Przykładem jest aresztowanie w Estonii obywatela Rosji podejrzanego o działalność agenturalną FSB i przygotowywanie cyberataków na instytucje państwowe w 2017 roku [27].

Główny Zarząd Sztabu Generalnego (GU, dawniej GRU) stanowi kinetyczne ramię rosyjskiej wojny hybrydowej. Specjalizuje się w sabotażu militarnym, atakach na infrastrukturę krytyczną, korytarze logistyczne i systemy energetyczne. Głośnym przykładem jego działań była próba otrucia Siergieja Skripala w 2018 roku w Salisbury, przeprowadzona przez Jednostkę 29155 GU z użyciem bojowego środka chemicznego Nowiczok [28]. GU powiązano także z cyberatakiem NotPetya (2017), ukrywającym się pod postacią ransomware, który sparaliżował ukraińską i globalną infrastrukturę, powodując straty liczone w miliardach dolarów [29].

Służba Wywiadu Zagranicznego (SVR) prowadzi tradycyjne, długofalowe działania szpiegowskie i operacje wpływu. Przypisywane jej są kradzieże technologii i infiltracja kręgów politycznych. W 2020 roku atak hakerski na firmę SolarWinds miał zostać zrealizowany przez grupę APT29 (Cozy Bear), działającej na rzecz SVR. W wyniku włamania skompromitowano amerykańskie agencje federalne oraz korporacje, pozyskując strategiczne informacje bez natychmiastowego efektu destrukcyjnego [30].

Federalna Służba Ochrony (FSO) i Spetssviaz zapewniają bezpieczną łączność dla rosyjskich władz i sił zbrojnych. Źródła otwarte i analizy wywiadowcze potwierdzają ich rolę w administrowaniu systemem SORM, rosyjskim mechanizmem masowej inwigilacji i przechwytywania, który równocześnie chroni kanały reżimowe i monitoruje opozycję [31].

Białoruski KGB i jego wewnętrzna jednostka GUBOPiK działają w dwóch sferach. W kraju prowadzą systematyczne represje, rozbijając struktury opozycji i kontrolując społeczeństwo obywatelskie poprzez infiltrację i przymus (funkcja policji politycznej). Głośnym przykładem była operacja z maja 2021 roku, kiedy KGB zmusiło do lądowania w Mińsku samolot linii Ryanair nr 4978, aby aresztować opozycyjnego dziennikarza Ramana Pratasiewicza [32]. Za granicą GUBOPiK infiltruje społeczności białoruskiej diaspory, stosując wobec niej zastraszanie i próby werbunku w zamian za pozwolenie na wyjazd z Białorusi [33].

Razem służby te tworzą **wielowarstwowy system ofensywny**: FSB odpowiada za penetrację kontrwywiadowczą na własnym terenie, gdzie pełni funkcję ochronną przed obcym wywiadem, za granicą zaś prowadzi działania o charakterze wywiadowczym. GU odpowiada za sabotaż, SVR za działania wpływu, KGB Białorusi za represje i operacje w diasporze, a FSO/Spetssviaz za bezpieczeństwo operacyjne. Taki podział pracy sprawia, że operacje hybrydowe mają charakter długofalowy, jak i elastyczny, ponieważ każda służba wspiera działania pozostałych , zachowując jednocześnie autonomię utrudniającą jednoznaczną atrybucję.

Operacje rosyjskich i białoruskich służb bezpieczeństwa nie polegają już na szpiegostwie zorientowanym, lecz na pozyskiwaniu informacji

potrzebnych do przeprowadzania operacji **inżynierii przekonań społecznych na masową skalę**. Proces ten przyspieszył po 2014 roku, gdy Rosja połączyła wpływy online z działaniami kinetycznymi (którym zaprzeczała), testując kolejne sieci w ramach operacji znanych jako *Secondary Infektion* [34], a następnie w kampaniach wieloplatformowych opartych m.in. o Telegram i środowiska niszowe. W latach 2023 i 2024 model ten został przetestowany w państwach bałtyckich [35] [36] i w Polsce poprzez zsynchronizowane działania dezinformacyjne, sabotażowe i kryminalne.

Miara skuteczności takich działań polega nie na zachowaniu tajności czy braku atrybucji, lecz na **nasyceniu narracji i manipulacji uwagą społeczną**. Kryminalni i ekstremistyczni pośrednicy zapewniają zasięg, zaprzeczalność i lokalny dostęp, podczas gdy służby państwowe dostarczają cele, narracje i finansowanie.

Jak szerzej omówiono w rozdziale 3, podejście to funkcjonuje w trzech zależnych od siebie obszarach:

1. Peryferyjne i półzamknięte przestrzenie internetowe służą do krzewienia i wzmacniania narracji nacechowanych emocjonalnie, zorientowane na tożsamość, krzywdy i lęki (Infiltracja kognitywna).

2. Diaspory i społeczności migrantów są wybiórczo wykorzystywane do kształtowania percepcji oraz zadań o niskim koszcie, przy czym rekrutacja i płatności odbywają się przez zaszyfrowane kanały (Tokenizacja wykonawców).

3. Lokalne napięcia obywatelskie i słabości instytucjonalne są przekształcane w strategiczne kliny poprzez starannie dawkowane akty zakłóceń (Skalowalne zakłócenia).

Efektem tych działań jest **otoczenie permanentnej niestabilności**, które podważa zaufanie i jakość procesów decyzyjnych. Metoda łączy ofensywę symboliczną z wybranymi szkodami materialnymi, aby wywołać nieproporcjonalne zainteresowanie medialne i tarcia polityczne. Polem walki staje się zbiorowy metabolizm emocjonalny społeczeństw. Celem jest stopniowa erozja determinacji obywatelskiej i spójności sojuszniczej, a nie pojedyncze rozstrzygające zwycięstwo.

Kluczowe koncepcje operacyjne

Kontrola refleksyjna [37] (*reflexive control*): Wywodząca się z sowieckiej nauki wojskowej koncepcja oznacza manipulowanie decyzjami przeciwnika poprzez uprzednie ukształtowanie jego percepcji i reakcji. Obejmuje ona stosowanie zaprojektowanych bodźców, takich jak fałszywe wybory, informacje pozorne czy manipulacja tempem wydarzeń.

Maskowanie i dezinformacja (*maskirowka – маскировка*) **[38]:** Doktryna wielowarstwowej dezinformacji, w której atrapy, rozproszenia i pozornie nieistotne działania ukrywają rzeczywisty cel operacyjny. Funkcjonuje zarówno na poziomie taktycznym, jak i narracyjnym, odwracając uwagę od właściwych działań i interpretacji. Doktrynalnie koncepcja ta pojawiła się najpierw w rosyjskich operacjach wojskowych, a następnie została włączona w szersze ramy ofensywnych działań hybrydowych.

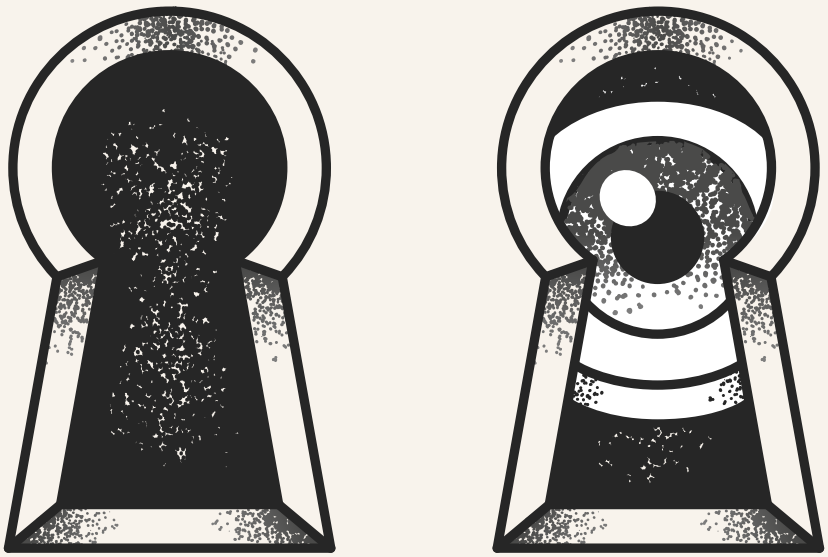
Operacje kształtowania percepcji [39] (*perception shaping operations*): Długofalowy wysiłek mający na celu przekształcenie sposobu, w jaki społeczeństwa interpretują wydarzenia, nadają im znaczenie i rozpoznają zagrożenia. Wykorzystuje subtelne i powtarzane bodźce emocjonalne, nie zawsze powiązane z jednoznacznymi przekazami politycznymi.

„Rozszczelnianie kognitywne” (*cognitive fracking*): Nowa koncepcja zaproponowana w niniejszym raporcie, odnosząca się do eksploatacji istniejących już podatności społecznych, np.: podziałów tożsamościowych, gniewu klasowego, historycznych urazów. Metoda ta polega na wywieraniu presji psychologicznej w sposób, który rozsadza i rozsierdza uśpione napięcia społeczne i prowokuje autodestrukcyjne zachowania polityczne.

3 Ramy koncepcyjne działań prowadzonych przez rosyjskie i białoruskie służby specjalne

Operacje wywiadowcze Rosji i Białorusi na wschodniej flance NATO nie są prowokacjami reaktywnymi. Są osadzone w świadomie zaprojektowanej architekturze zakłóceń, skalibrowanej tak, by wykorzystywać słabości bez wywoływania otwartego konfliktu. Zasadniczym celem nie jest militarne pokonanie państw Zachodu, lecz ich rozbicie kognitywne, wyczerpanie percepcyjne i korozja instytucjonalna. Każda warstwa operacjonalizuje strategię ww. „parytetu przez odejmowanie": infiltracja niszczy zaufanie, tokenizacja wzmacnia niejednoznaczność, a mikrooperacje nakładają stałe tarcie na zarządzanie i logistykę.

Ta filozofia operacyjna przedkłada niejednoznaczność nad atrybucję i niespójność nad eskalację. Rezultatem jest wielowarstwowa, zdecentralizowana kampania wymierzona w przekonania, legitymację i odporność psychologiczną w długiej perspektywie. Poniżej opisane są trzy zasadnicze poziomy tego modelu.



Poziom 1: Infiltracja kognitywna

U podstaw ww. modelu operacyjnego leży systematyczna penetracja ekosystemu informacyjnego. Rosyjska kampania informacyjna przebiega w dwóch wyraźnych fazach: najpierw buduje podziały społeczne i podważa zaufanie do instytucji, a następnie eskaluje napięcia, by wymusić reakcję polityczną i psychologiczną. Nie jest to zwykła propaganda, lecz metodyczne wykorzystanie istniejących napięć, symboli i lęków w celu nasycenia dyskursu publicznego zamętem, podejrzliwością i polaryzującymi emocjami. Rosyjskie i białoruskie służby posługują się sieciami diaspory, influencerami online oraz rozwiązaniami algorytmicznymi tak, aby osadzać wrogie treści w krajowych dyskusjach, a nawet debatach publicznych.

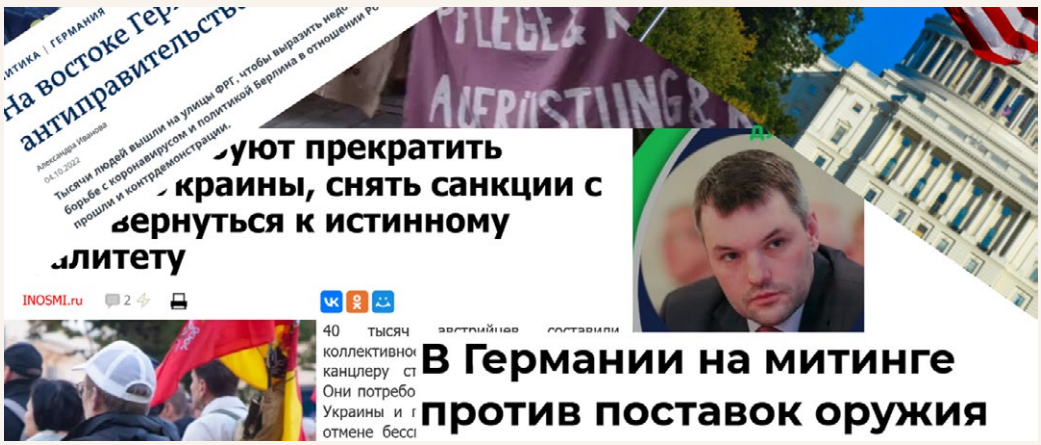
Narracje takie często eksploatują:

- rzekome poczucie oblężenia Rosji czy Białorusi („NATO nas otacza")
- krzywdy narodowe („Polska to marionetka", „Ukraińcy to uprzywilejowani goście")
- tezy o upadku moralnej legitymizacji Zachodu („ideologia gender", „samobójstwo kulturowe")
- historyczne antagonizmy polsko-ukraińskie
- niechęć do „obcych" w społeczeństwie"

Przykład: W okresie poprzedzającym wybory prezydenckie w Polsce w 2025 roku, powiązane z Rosją sieci wpływu używały platform X (dawniej Twitter) oraz kanałów Telegram o polskojęzycznej tożsamości do rozpowszechniania ukierunkowanej dezinformacji, przedstawiającej uchodźców z Ukrainy jako ciężar dla państwa. Narracje obejmowały fałszywe statystyki i materiały wizualne, które przedstawiały uchodźców jako destabilizujących systemy socjalne i demograficzne. Kampania była zintegrowana w wielu społecznościach internetowych, co zwiększało jej wiarygodność przy jednoczesnym maskowaniu skoordynowanego, zagranicznego pochodzenia [40].

Koncepcja znajdująca zastosowanie: Operacje kształtowania percepcji poprzez *kontrolę refleksyjną* nie są perswazyjne w klasycznym znaczeniu. Relatywizują prawdę, sprawiając, że dana pozycja lub propozycja wydaje się ideologicznie skażona, emocjonalnie wyczerpująca lub kontekstowo nieweryfikowalna.

Przykłady rosyjskiej propagandy na temat Ukrainy.



Źródło: www.gov.pl/web/special-services/russian-propaganda-wants-to-stop-aid-to-ukraine

Poziom 2: Tokenizacja wykonawców

Środkowy poziom modelu stanowi outsourcing zadań taktycznych do osób niskiego kosztu i o niskiej widoczności. To kluczowy element rosyjsko-białoruskiego skalowania niejednoznaczności: zamiast wysyłać przeszkolonych agentów, służby wywiadowcze „tokenizują" pracę, oddzielając własne intencje od wykonawstwa zadań (tj. wykorzystanie agentury „proxy").

Do takich aktorów zalicza się:

- Migrantów ekonomicznych werbowanych w internecie, często za pośrednictwem szyfrowanych kanałów, którzy pełnią rolę agentów proxy; rekrutacja ta bywa powiązana z płatnościami w kryptowalutach i poczuciem bezkarności
- elementy kryminalne motywowane kryptowalutą i bezkarnością
- rozczarowanych obywateli przekonanych o korupcji krajowej polityki
- osoby z zaburzeniami osobowościowymi lub problemami ze zdrowiem psychicznym

Zadania są maskowane jako logistyczne, ideologiczne lub pozornie błahe. Mężczyzna fotografujący bazę wojskową przedstawiany jest jako pasjonat kolei. Pożar magazynu przypisywany jest wojnom gangów. Dzięki temu sabotaż lub dywersja pozostają wiarygodnie zaprzeczalne, fragmentaryczne i de facto apolityczne w oczach opinii publicznej.

Definiującą cechą metod rosyjskich i białoruskich stało się rosnące wykorzystanie doraźnych modelów rekrutacji, zwłaszcza tzw, **„jednorazowych szpiegów"** (*disposable spies*): wykonawców rekrutowanych do pojedynczych, ściśle określonych zadań, z minimalnym przeszkoleniem i bez trwałego związku instytucjonalnego. Konstrukcja ta odpowiada koncepcji tożsamości „jednorazowych" w świecie wywiadu: agentów wykorzystywanych do jednej misji i następnie porzucanych, by chronić zaprzeczalność i ograniczyć obciążenia biurokratyczne [41]. Zjawisko to nasiliło się szczególnie po masowych wydaleniach rosyjskich dyplomatów na początku 2022 roku: do połowy tego roku usunięto z Europy ponad 600 takich osób, w tym około 400 w jednej tylko fali, co zmusiło Kreml do odejścia od wywiadu opartego na ambasadach ku doraźnym modelom rekrutacji, z użyciem zachęt finansowych lub ideologicznych [42]. Ponadto wykorzystywane są także inne formy agentury, takie jak nielegałowie działający pod fałszywą tożsamością, oferenci samodzielnie zgłaszający chęć współpracy, defektorzy przekazujący informacje po przejściu na stronę przeciwnika oraz agenci wpływu kształtujący opinię publiczną i decyzje polityczne.

Przykład: Od końca 2023 do połowy 2024 roku w Polsce, Wielkiej Brytanii i Niemczech odnotowano serię podpaleń i incydentów sabotażowych, początkowo przypisywanych lokalnym sporom lub przestępczości zorganizowanej. W Polsce ataki na restaurację w Gdyni, magazyn w Gdańsku i skład palet w Markach początkowo powiązano z gangami, lecz później powiązano je z rosyjskimi zleceniami wywiadowczymi [43]. W Wielkiej Brytanii pożar magazynu w Londynie i próba podpalenia biznesu powiązanego z Ukrainą również początkowo wyglądały na działania kryminalne, dopóki kontrwywiad nie powiązał ich koordynacji z rosyjskimi oficerami prowadzącymi [44]. W obu przypadkach werbunek przeprowadzono głównie online wśród osób podatnych, które opłacono w kryptowalutach, a wykonawcy pozostawali nieświadomi szerszego celu operacyjnego, co sprawiało, że każde zdarzenie wyglądało na odosobnione.

Koncepcja znajdująca zastosowanie: *Maskirowka* działa poprzez nakładanie niespójności taktyki na spójność strategii. Rozpraszając wykonanie pomiędzy cywilnych pośredników, operacja unika jednoznacznej atrybucji, a jednocześnie zwiększa swój zasięg.

Poziom 3: Intensyfikacja skalowalnych zakłóceń

Ostatni poziom opisywanego modelu ma charakter czasowy i symboliczny. Jego celem nie jest kryzys natychmiastowy, lecz stopniowa degradacja. Skalowalne zakłócenia łączą drobne zdarzenia w efekty o znaczeniu strategicznym: cykle strachu, kompromitację instytucji, paraliż opinii publicznej. Model ten jest iteracyjny i odporny: jeśli jedna operacja zawodzi, inna szybko ją zastępuje.

Typowe skutki obejmują:

- wyczerpanie psychospołeczne spowodowane powtarzającymi się zagrożeniami niskiej skali (np. alarmy bombowe, fałszywe cyberataki);
- utratę wiarygodności instytucji poprzez dramatyzację i sprzeczności;
- przeciążenie zdolności państwa do reagowania poprzez prowokowanie nadmiernych reakcji.

Przykład: Tylko od 2024 roku w Polsce miało miejsce ponad tuzin skoordynowanych podpaleń centrów logistycznych, w tym wielki pożar hali Marywilskiej w Warszawie, gdzie zniszczeniu uległo około 1400 sklepów i punktów usługowych [45]. Incydenty te przyciągnęły ogromną uwagę mediów i skutecznie ukształtowały ogólnonarodową debatę, pokazując, jak sabotaż fizyczny można wykorzystać w celach politycznych.

Koncepcja znajdująca zastosowanie: *Rozszczelnianie kognitywne* polega na wykorzystaniu utajonych pęknięć społecznych – takich jak resentyment kulturowy, niepewność ekonomiczna czy nieufność po pandemii – aby wywołać nieproporcjonalne reakcje psychologiczne. Nie chodzi tu o propagandę, lecz o przyspieszanie istniejącej entropii społecznej.

Działania w ramach rosyjskiej wojny hybrydowej wg. kraju i roku, styczeń 2018 – czerwiec 2024

		Cele komunikacyjne	Cele energetyczne	Cele rządowe	Cele zdrowotne	Cele przemysłowe	Cele wojskowe	Cele transportowe	Cele podwodne	Cele wodne	SUMA
2018	Grecja			1							1
2019	Bułgaria			1							1
2020	Finlandia		1					1			2
2022	Albania						1				1
	Bośnia i Hercegowina			2							2
	Bułgaria						2	1			3
	Dania		1								1
	Finlandia			1							1
	Niemcy						1				1
	Włochy	1									1
	Norwegia		3								3
	Polska			1							1
2023	Bułgaria						2				2
	Czechy			1							1
	Estonia								1		1
	Niemcy		1								1
	Polska							4			4
2024	Czechy							1			1
	Dania									1	1
	Finlandia								1	6	7
	Francja							3		1	4
	Niemcy						5			2	7
	Norwegia	1					1				2
	Polska						1		1	1	3
	Rumunia				1						1
	Słowacja						1				1
	Hiszpania					1					1
	Szwecja	1							1	1	3
	Wielka Brytania				1	1					2
2025	Morze Bałtyckie								1		1
	Czechy						1				1
	Niemcy						1	1	1		3
	Grecja		1								1
	Holandia							1			1
	Norwegia		1								1
	Serbia						1				1
	Szwecja								1	1	2

Źródło: International Institute for Security Studies

4 Typologia operacji: od podpaleń po fałszywe narracje

Poniższy rozdział przedstawia sześć głównych kategorii operacji hybrydowych prowadzonych przez rosyjskie i białoruskie służby wywiadowcze. Każda kategoria zilustrowana jest sprawdzonymi studiami przypadków.

Sabotaż i Dywersja

Rosyjskie i białoruskie służby wywiadowcze stopniowo udoskonaliły sabotaż jako narzędzie wojny hybrydowej, umożliwiające działanie poniżej progu otwartego konfliktu przy jednoczesnym wywoływaniu maksymalnych zakłóceń politycznych i społecznych. Podejście to czerpie z doktryny sowieckiej [46], lecz wzbogacone jest o elastyczność operacyjną XXI wieku, ścisłe dzielenie zadań oraz synchronizację z wojną informacyjną. Zmiana ta przyspieszyła po 2022 roku, gdy korytarze logistyczne przez Polskę, państwa bałtyckie i Niemcy stały się niezbędne dla podtrzymania obrony Ukrainy, co było formą udzielenia jej wsparcia przez kraje Zachodu. Raport IISS z 2025 r. wskazuje na czterokrotny wzrost rosyjskich operacji sabotażowych przeciw infrastrukturze krytycznej w Europie w latach 2023–2024, przy czym większość działań była prowadzona przez zdecentralizowane, doraźnie zwerbowanych wykonawców [47].

Zamiast widowiskowych ataków kinetycznych, obecnie preferowany jest wzorzec uporczywych działań o niskiej lub średniej intensywności, które w sposób skumulowany podważają zaufanie publiczne do legalnych władz politycznych i wiarygodność instytucji państwowych. Noc z 9 na 10 września 2025 roku, gdy kilkanaście rosyjskich dronów naruszyło polską przestrzeń powietrzną, należy traktować jako studium przypadku skalowalnego sabotażu: przeciwnik testował procedury NATO, sondował czas reakcji i sprawdzał odporność psychologiczną polskich instytucji.

Znakiem rozpoznawczym tej doktryny sabotażu jest **wiarygodna zaprzeczalność**. Operatorzy często działają poprzez nieświadomych pośredników, rekrutowanych za pomocą mediów społecznościowych i szyfrowanych komunikatorów oraz opłacanych kryptowalutami. Zadania przedstawiane są jako niepolityczne lub pozornie błahe, aby maskować strategiczne intencje. Obejmują one zarówno fotografowanie obiektów i konwojów wojskowych, jak i podkładanie ładunków zapalających w obiektach cywilnych.

Tego rodzaju metody pozwalają służbom na utrzymanie dystansu od fizycznego aktu dywersji, utrudniając atrybucję, a jednocześnie gwarantują, że zakłócenia zbiegają się z politycznie wrażliwymi momentami. Działania te operują w szarej strefie, w której celem przeciwnika jest nakładanie tarcia i niepewności na procesy decyzyjne, a nie natychmiastowa przewaga na polu bitwy.

Norwegia doświadczyła pożaru kanału kablowego między Asker i Drammen, który sparaliżował ruch kolejowy [48], a Oslo odnotowało falę co najmniej szesnastu celowych podpaleń pojazdów od kwietnia 2024 roku [49]. W **Finlandii** miało miejsce co najmniej jedenaście prób włamań do systemów zaopatrzenia w wodę w Turku, Tampere, Porvoo i Sipoo, a także pożary w fabryce sklejki UPM w Joensuu, na terenie koszar w Santahaminie, w ratuszu w Ruovesi, w hali przemysłowej w Lahti (podejrzewane jest podpalenie) oraz w zakładzie recyklingu w Oulu [50] [51].

Estonia odnotowała zniszczenie hali magazynowej PVC w Lööra i eksplozję w zbiorniku oleju opałowego w porcie w Północnym Tallinnie [52]. Na **Łotwie [53]** zgłoszony został pożar w zakładzie utylizacji odpadów niebezpiecznych w ryskiej dzielnicy Bolderaja [54], a na **Litwie** pożar w Zakładach Lotniczych w Kownie, w pobliżu nieczynnego lotniska wojskowego [55]. Dochodzenia ujawniły, że rekrutacja wykonawców i instrukcje operacyjne odbywały się przez platformy online, takie jak Telegram, gdzie podejrzani otrzymywali konkretne zadania rozpoznawcze i sabotażowe.

Podobne techniki odnotowano w **Niemczech**. W kwietniu 2024 roku władze niemieckie aresztowały dwie osoby posiadające podwójne obywatelstwa podejrzane o planowanie ataków sabotażowych na bazy wojskowe na rzecz Rosji [56]. W 2025 roku przed sądem stanęło kilku mężczyzn oskarżonych o udział w rosyjskich operacjach, w tym w planach wysyłania paczek zawierających materiały zapalające i wybuchowe [57]. W tym samym roku celem sabotażu stały się placówki kurierskie w Niemczech i **Wielkiej Brytanii**. Przesyłki były zamaskowane jako zwykłe towary konsumpcyjne, takie jak masażery czy zestawy kosmetyczne, a w rzeczywistości zawierały związki zapalne i systemy czasowego zapłonu [58]. Urządzenia te spowodowały ograniczone straty materialne, jednak celem ich było przede wszystkim testowanie procedur kontroli przesyłek, zakłócenie łańcuchów dostaw i wytworzenie wrażenia podatności systemowej.

Skala wrogiej aktywności wykrytej w Polsce między 2023 a 2025 rokiem jest bezprecedensowa w Europie Środkowej w okresie po zimnej wojnie. Za szpiegostwo, sabotaż lub współpracę z rosyjskimi i białoruskimi służbami aresztowanych zostało co najmniej 49 osób [59]. Zatrzymani to zarówno cudzoziemcy, jak i lokalni pośrednicy oraz rekruci oportunistyczni, rekrutowani przy użyciu szyfrowanych komunikatorów,

niskoprogowych ofert online lub pośredników z darknetu. Władze rozbiły 19 odrębnych grup operacyjnych, w tym wiele skrajnie zatomizowanych i nieświadomych wzajemnych zadań, odzwierciedlające systemowe dążenie do zalewania środowiska dużą liczbą pozornych wykonawców zaangażowanych w proste, lecz liczne misje – takie jak fotografowanie transportów kolejowych wojska, monitorowanie lotnisk czy podpalanie obiektów przy strategicznych magazynach.

W ciągu zaledwie kilku tygodni 2024 roku, Polska doświadczyła niezwykle gęstej i zróżnicowanej serii incydentów wymierzonych w aktywa przemysłowe, logistyczne, gospodarcze i symboliczne. Jak omówiono powyżej, w maju tego roku operujący na zlecenie Kremla agenci podpalili centrum handlowe Marywilska 44 w Warszawie, niszcząc ponad 1400 lokali handlowych i usługowych oraz powodując straty szacowane na setki milionów złotych.

Pod koniec czerwca tempo ataków wzrosło. 28 czerwca ogień strawił zbiorniki z olejem napędowym w terminalu przeładunkowym LHS w Sławkowie [60], zagrażając kluczowej arterii kolejowej. Tego samego dnia pożar objął siedem hektarów poligonu w Żaganiu [61]. Zniszczenia przemysłowe obejmowały dwie hale obróbki drewna w Klonowie [62] oraz wielki pożar w zakładzie Synthos w Oświęcimiu, którego opanowanie wymagało 25 jednostek straży pożarnej.

Atakom uległy także obiekty kultury i dziedzictwa narodowego: Pałac Stolbergów we Wrocławiu, zabytkowy pałac w Jelczu-Laskowicach oraz XVII-wieczny drewniany kościół w Nowym Sączu [63]. Straty gospodarcze i rolne potwierdza natomiast zniszczenie 500 ton zboża w magazynie w Sierpcu [64] [65]. We Wrocławiu [66] policja zatrzymała mężczyznę próbującego podpalić fabrykę farb; śledczy wykazali bezpośrednie powiązania mężczyzny z rosyjskimi oficerami prowadzącymi, którzy przekazali mu ok. 5 tys. dolarów na wykonanie zadania.

Istotną domeną o znaczeniu strategicznym, w której Polska zmaga się z rosyjskim sabotażem, jest **zakłócanie infrastruktury światłowodowej**. Ostatnie incydenty w Warszawie, w tym duże uszkodzenia podziemnych linii [67] pokazują, że obce służby mogą zamieniać działania z obszaru morskiego (tj. ataków na bałtyckie kable podmorskie) na operacje lądowe przeciwko kluczowej infrastrukturze telekomunikacyjnej.

Nagromadzenie tak różnorodnych incydentów w krótkim czasie wydaje się zaprojektowane po to, by przeciążyć krajowe zdolności reagowania (lub je przetestować) i utrzymać stałe poczucie zagrożenia. Rosja i Białoruś zdają się doskonalić na terytorium Polski generację narzędzi hybrydowych, traktując kraj jako poligon doświadczalny dla trwałych operacji wymierzonych w poznanie społeczne, infrastrukturę, podatności diaspory i zaufanie publiczne. Działania te nie zmierzają do rozstrzygających przełomów, lecz do stopniowej erozji, gdzie każdy incydent wywołuje szerokie instytucjonalne, informacyjne i psychologiczne reperkusje.

Łącznie incydenty te ujawniają **spójną doktrynę operacyjną**, w której obiekty wojskowe, energetyczne i przemysłowe atakowane są równolegle z aktywami cywilnymi i kulturowo istotnymi. Schemat ma na celu zmuszanie służb bezpieczeństwa do stałej reaktywności, tworzenie widocznych dowodów słabości państwa oraz podtrzymywanie podskórnego poczucia zagrożenia społecznego, które można wykorzystać w domenie informacyjnej.

Z teoretycznego punktu widzenia akty te nie są odosobnione, lecz wpisują się w logikę systemowej kampanii, w której ataki fizyczne sekwencjonuje się i rozprasza, aby stworzyć atmosferę niestabilności. Efekt operacyjny wynika z utrzymywanego tempa i geograficznego rozproszenia, zmuszając służby bezpieczeństwa do nadmiernego rozciągania zdolności monitorowania i dochodzenia. Każdy akt zostaje wzmocniony równoległą operacją informacyjną, która albo wyolbrzymia niekompetencję państwa, albo podsyca narracje spiskowe, co dodatkowo pogłębia wpływ psychologiczny.

Integracja dywersji, sabotażu i działań o charakterze terrorystycznym w szersze ramy działań hybrydowych pokazuje, jak Moskwa i Mińsk zaadaptowały dawne techniki do współczesnych słabości. Łączą zakłócenia fizyczne o niskiej widoczności z dopasowaną eksploatacją narracji, tworząc sprzężenia zwrotne, w którym każdy incydent przygotowuje grunt informacyjny pod kolejny. Rezultatem jest trwała erozja odporności społecznej, osiągana bez przekraczania progów konwencjonalnych, które wywołałyby bezpośrednią militarną odpowiedź.

Outsourcing szpiegostwa

Outsourcing szpiegostwa jest jednym z kluczowych elementów obecnej strategii wojny hybrydowej stosowanej przez rosyjskie i białoruskie służby wywiadowcze, ale nie oznacza całkowitego odejścia od klasycznych metod. Oficerowie wywiadu pod przykryciem dyplomatycznym, jak i nielegałowie operujący na fałszywych tożsamościach nadal funkcjonują, natomiast nowością jest rosnące znaczenie rekrutacji osób o niskiej widoczności, często migrantów lub obywateli państw trzecich, pozyskiwanych przez szyfrowane platformy komunikacyjne, takie jak Telegram, WhatsApp czy fora internetowe.

Tego rodzaju model nie zastępuje tradycyjnego wywiadu, lecz go uzupełnia, tworząc elastyczne i trudniej wykrywalne sieci. Pozwala to łączyć działania prowadzone przez kadrowych oficerów z tanimi i doraźnymi operacjami wykonywanymi przez osoby zwerbowane ad hoc, co razem wzmacnia zdolność prowadzenia operacji wpływu i sabotażu na szeroką skalę. Rekruci, często migranci, nowo przybyli uchodźcy lub osoby marginalizowane ekonomicznie, otrzymują ściśle określone zadania, takie jak obserwacja, infiltracja czy drobny sabotaż. Płatności wahają się od symbolicznych kwot za proste działania po kilkaset dolarów lub kryptowaluty za bardziej złożone operacje. Tego rodzaju misje przemyślane są w taki sposób, aby były zaprzeczalne, skalowalne i trudne do powiązania z centralnymi strukturami dowodzenia.

Śledztwa ujawniły przypadki, w których wielu rekrutów było w praktyce traktowanych jak zasoby jednorazowe. Niektórzy mylili swoich oficerów prowadzących z partnerami biznesowymi czy sympatykami nacjonalizmu, zgadzając się na zadania takie jak rozwieszanie anty-natowskich ulotek czy instalowanie kamer monitorujących transport wojskowy kierowany na Ukrainę. W zamian otrzymywali płatności w kryptowalutach w przedziale od 5 do 400 dolarów [68]. Ofiary werbunku często były wyszukiwane poprzez platformy oferujące zatrudnienie, na których migranci szukali prac dorywczych,

Źródło: prima91 – stock.adobe.com

co utrudniało wykrycie procesu rekrutacyjnego. Zostali oni pozyskani w taki sposób, by nie wiedzieć lub nie rozumieć, dla kogo faktycznie pracują, co wynikało także z ograniczonego potencjału intelektualnego rekrutowanych. Jest to rutynowa technika operacyjna, nawet w procesie werbunku tzw. klasycznej agentury- werbunek odbywa się tak, by werbowany nie wiedział, że jest werbowany.

W 2024 roku 17-letni Kanadyjczyk został zwerbowany przez FSB do wykonywania zadań szpiegowskich, zanim jego aresztowanie doprowadziło do ujawnienia portfeli kryptowalutowych powiązanych z sieciami prania pieniędzy FSB [68] [69]. Czeski kontrwywiad udokumentował przypadki, w których migranci spoza Unii Europejskiej byli zatrudniani przez Telegram pod pretekstem działań przestępczych lub legalnych prac, często nie zdając sobie sprawy, że pomagają obcym służbom wywiadowczym, co sprzyjało wzrostowi nieufności w lokalnych społecznościach [70].

Podobny schemat pojawił się w Wielkiej Brytanii, gdzie bułgarska siatka szpiegowska kierowana przez Orlina Rousseva wykorzystywała pośredników do rekrutowania wykonawców obserwujących dysydentów, dziennikarzy i ukraińskich wojskowych. Rekruci byli motywowani finansowo, a część z nich twierdziła, że została oszukana i nie miała ideologicznego związku z reżimem [71]. Takie grupy pokazują, w jaki sposób sieci kryminalne i nieformalne mogą zostać przekształcone w aktywa wywiadowcze, dodatkowo zacierając granice między szpiegostwem a przestępczością zorganizowaną.

Model takiego działania rozciąga się także na operacje dywersyjne i sabotażowe. W marcu 2024 roku brytyjski sąd skazał trzech mężczyzn za podpalenie magazynu z pomocą humanitarną dla Ukrainy. Ich oficer prowadzący, powiązany z rosyjskim wywiadem, koordynował operację przez Telegram i wychwalał ich po rosyjsku, gdy pożar się rozpoczął [72]. Przypadek ten ilustruje celowe wykorzystanie niewyszkolonych i łatwo zastępowalnych wykonawców do działań destabilizacyjnych prowadzonych pod zdalnym kierownictwem, przy minimalnym ryzyku dla samej służby wywiadowczej.

Outsourcing wpisuje się w doktrynę wojny hybrydowej, która przedkłada stopniową erozję zaufania i wiarygodności instytucjonalnej nad bezpośrednią konfrontację. Rozdzielając zadania między luźno powiązanych wykonawców niebędących częścią formalnych sieci, rosyjskie i białoruskie służby zmniejszają podatność operacyjną, a jednocześnie utrzymują ciągłość działań. Metoda ta pozwala na stałą obecność operacyjną, kształtując zarówno środowisko fizyczne, jak i przestrzeń informacyjną, bez wchodzenia w otwarty konflikt.

Operacje kognitywne i dezinformacja

Operacje kognitywne mają na celu kształtowanie tego, co ludzie zauważają, co czują i jakie wnioski wyciągają. Obecnie funkcjonują jak linia produkcyjna łącząca fałszywe tożsamości, treści syntetyczne i skoordynowaną działalność wieloplatformową. Celem jest nasycenie i niepewność, a nie przekonanie spójnym komunikatem. Europejscy śledczy opisują powtarzalny mechanizm: zainicjowanie tezy w niszowych kanałach, przepuszczenie jej przez strony podszywające się pod lokalne źródła, a następnie wzmocnienie jej automatyzacją i skoordynowanymi publikacjami, coraz częściej wspieranymi przez konsumenckie narzędzia AI zwiększające tempo i skalę przekazu [73].

W Polsce analitycy udokumentowali wieloplatformową kampanię, która łączyła prorosyjskie klastry z technikami wykorzystanymi w tzw. Operacji Overload, mającą na celu wzbudzenie wrogości wobec uchodźców z Ukrainy podczas cyklu prezydenckiego w 2025 roku. Wykorzystywano wizualizacje generowane przez AI oraz strony podszywające się pod lokalne media, aby zwiększyć wiarygodność i zasięg spreparowanych informacji. Kampania była zsynchronizowana z kluczowymi momentami politycznymi i wykorzystywała kanały Telegram powiązane z diasporą, aby udawać oddolny gniew społeczny [74]. Niezależni monitorujący śledzący te same schematy w całej Europie wykazali, że sieć intensyfikowała działania podczas wyborów i momentów kryzysowych, wykorzystując luki w egzekwowaniu przepisów przez duże platformy, aby utrzymać krążenie ich własnej narracji [75].

We Francji organy państwowe zmapowały duże farmy treści prorosyjskich, które kopiowały marki mediów głównego nurtu i rozpowszechniały spreparowane treści. Paryż powiązał to z trwałą siecią 193 fałszywych portali informacyjnych oraz z szerszymi ekosystemami „Portal Kombat" i „Doppelgänger", które atakowały francuską przestrzeń informacyjną i Igrzyska Olimpijskie w Paryżu 2024. Władze opublikowały szczegóły techniczne, noty atrybucyjne i przykłady sfabrykowanych nagrań wideo oraz artykułów podszywających się pod francuskie media [76] [77] [78]. W późniejszym raporcie krajowym opisano, w jaki sposób generatywne AI wpłynęła na ten ekosystem/przyspieszyła ten proces, umożliwiając produkcję syntetycznych prezenterów, klonowanych głosów i szablonowych nagrań wideo na masową skalę, a następnie ich redystrybucję na Telegramie, X i mniejszych platformach wideo w celu ominięcia moderacji [79].

W Wielkiej Brytanii rząd objął sankcjami rosyjskie firmy zajmujące się dezinformacją i ich kierownictwo po udokumentowaniu prób wywołania antyukraińskich protestów oraz prowadzenia skoordynowanych operacji wpływu podszywających się pod brytyjskie media i lokalne strony społecznościowe. W oficjalnych dokumentach wymieniono tzw. Agencję Social Design i powiązane z nią podmioty, łącząc je z klonowanymi domenami i operacjami narracyjnymi wymierzonymi w odbiorców brytyjskich i sojuszniczych [80] [81]. Zespoły badaczy śledziły także ww. sieć z operacji Overload używającą darmowych narzędzi AI do zalewania europejskich platform syntetycznymi obrazami, klonowanymi nagraniami głosowymi, przekierowaniami QR i szablonowymi stronami, w tym masowymi zgłoszeniami do fact-checkerów, które miały przechwytywać cykle uwagi [82] [83].

W Stanach Zjednoczonych Departament Sprawiedliwości wraz z agencjami partnerskimi rozbił farmę botów zasilaną sztuczną inteligencją zbudowaną na oprogramowaniu rosyjskiej, państwowej telewizji RT i obsługiwaną przez FSB. Jej celem było szerokie rozsiewanie narracji podziałowych w serwisie X i na innych platformach. W oddzielnej akcji przejęto 32 domeny Doppelgänger, które podszywały się pod legalne media i strony rządowe, aby wprowadzać narracje państwa rosyjskiego do amerykańskiej przestrzeni informacyjnej [84] [85]. Wspólny komunikat FBI i CISA zawierał szczegółowe informacje o pakiecie automatyzacyjnym „Meliorator",

opisując, w jaki sposób proces tworzenia kont, harmonogramowania treści i targetowania odbiorców został zintegrowany, aby zwiększać zasięgi operacji przy jednoczesnym ukrywaniu jej koordynacji [86].

We wszystkich tych sferach działań generatywna AI zmieniła naturę dezinformacji z pracy „rzemieślniczej" w proces zautomatyzowany. Śledztwa wykazały, że przeciwnicy korzystają z ogólnodostępnych modeli do tworzenia obrazów syntetycznych, klonowania głosów, szybkiego tłumaczenia i lokalizacji treści, a następnie stosują testy A/B dla wariantów narracji i scenariuszy person, aby wybrać te najbardziej wywołujące gniew. Analitycy, którzy śledzili Overload w Europie i Wielkiej Brytanii, stwierdzili, że darmowe narzędzia konsumenckie wystarczały, aby prowadzić nieustanną „eksplozję treści", która mnożyła liczbę aktywów i kanałów szybciej, niż możliwości dostosowania się mechanizmów egzekwowania [87] [88]. Europejskie raporty strategiczne dodają, że linie działań kognitywnych są synchronizowane z wydarzeniami fizycznymi i online, np. wtargnięciami dronów, incydentami sabotażu czy awariami infrastruktury, aby zacierać świadomość sytuacyjną i zmuszać instytucje do reakcji zamiast przewidywania.

Wreszcie, wiele rządów i ośrodków badawczych podkreśla, że wpływ na wyniki wyborów nie jest jedyną miarą zagrożenia. Badania dotyczące wyborów w Wielkiej Brytanii i UE w 2024 roku wykazały ograniczony bezpośredni wpływ deepfake'ów AI na głosowanie, jednocześnie ostrzegając przed skutkami ubocznymi, takimi jak zastraszanie kandydatów, dezorientacja co do źródeł informacji czy normalizacja syntetycznych cykli plotek, które trwają poza okresem kampanii [89]. To rozróżnienie ma znaczenie polityczne, ponieważ operacje kognitywne mają na celu erozję zaufania i spójności w długiej perspektywie, nawet jeśli krótkoterminowe przesunięcia w sondażach są trudne do uchwycenia.

Instrumentalizacja diaspor

Środowiska diaspor w całej Europie stały się terenem operacyjnym dla rosyjskich i białoruskich służb wywiadowczych. Zapewniają one dostęp językowy, sieci zaufania i osłonę cywilną, które umożliwiają rekrutację, obserwację, logistykę i działania narracyjne w ramach otwartych przestrzeni społecznych [90]. Powtarzającym się mechanizmem jest wykorzystywanie przykrywkowych organizacji charytatywnych i "rodaków" przedstawiających się jako podmioty zapewniające pomoc prawną i kulturową, a w praktyce przekazujące środki finansowe, pomoc prawną i przekazy propagandowe aktywom osadzonym w diasporach.

Najlepiej udokumentowanym przykładem jest fundacja **Pravfond**, która – jak pokazują przechwycone maile i dokumentacja finansowa – wspierała skazanych szpiegów, propagandystów i punkty wpływu w Europie [91]. Równolegle funkcjonują mechanizmy bezpośredniej presji wobec wspólnot emigracyjnych, w ramach których służby bezpieczeństwa organizują wizyty, nękanie online i groźby wobec krewnych w kraju, co wywołuje efekt mrożący i zniechęca do aktywności obywatelskiej oraz opozycyjnej w państwach przyjmujących.

Przestrzenie diaspory są także wykorzystywane do powierzania zadań osobom, które nie są wyszkolonymi oficerami, lecz posiadają odpowiedni dostęp i zapewniają zaprzeczalność. Czeski kontrwywiad raportuje, że rekruterzy zwracają się do migrantów i obywateli spoza UE, kontaktując się z nimi za pośrednictwem Telegrama i płacąc niewielkie kwoty bądź kryptowaluty za działania takie jak rozpoznanie, sabotaż czy zastraszanie, których celem jest erozja zaufania do władz i tworzenie atmosfery strachu [92]. Podobny schemat odnotowano w Polsce, gdzie

udokumentowano próby werbunku imigrantów i osób niepewnych ekonomicznie do zadań szpiegowskich i podpaleń [93] [94]. Efektem jest rozproszona sieć ludzka, trudna do zmapowania i jeszcze trudniejsza do odstraszania, ponieważ jej działania często stapiają się z życiem diaspory i jej legalną działalnością.

Diaspory są również eksploatowane za pośrednictwem pośredników kryminalnych, którzy już wcześniej przerzucali ludzi, pieniądze i towary przez granicę. Raport Europolu o zagrożeniach z 2025 roku opisuje rozwijający się **„cienisty sojusz" między podmiotami państwowymi a przestępczością zorganizowaną**, w którym logistyka kryminalna jest przekształcona do sabotażu politycznego, szpiegostwa i operacji wpływu. Zapewnia to zarówno wiarygodne zaprzeczenie, jak i odporne łańcuchy dostaw wewnątrz UE [95]. W praktyce oznacza to kurierów gotówkowych, fałszywe dokumenty, wynajęte lokale i floty pojazdów powiązane z grupami przestępczymi, lecz obsługujące operacje hybrydowe wymierzone w infrastrukturę, aktywistów i organizacje diasporyczne. Ponieważ przestępczość często badana jest oddzielnie od spraw o ingerencję zagraniczną, te same sieci mogą funkcjonować nawet po aresztowaniu poszczególnych wykonawców, co pozwala przeciwnikowi utrzymać tempo działań.

Konkretne sprawy sądowe pokazują, jak przykrycie diasporyczne i role outsourcingowe się zazębiają. W Wielkiej Brytanii śledztwo Metropolitan Police oraz procesy sądowe ujawniły rosyjską siatkę szpiegowską kierowaną przez Orlina Rousseva, który – powiązany z aferzystą Wirecard Janem Marsalkiem – koordynował działalność bułgarskich obywateli mieszkających w Wielkiej Brytanii. Zbierali oni wrażliwe informacje i wspierali operacje pod przykryciem codziennych ról społecznych i zawodowych w środowisku migrantów. Roussev został skazany na prawie jedenaście lat więzienia po przyznaniu się do winy, a akta sprawy ujawniają tysiące wiadomości łączących obecność diaspory z tajnymi misjami [96] [97]. W innej brytyjskiej sprawie ława przysięgłych skazała trzech mężczyzn za podpalenie magazynu w East London, w którym składowano sprzęt wojskowy dla Ukrainy. Spiskowcy zostali zwerbowani i kierowani przez rosyjskiego oficera prowadzącego za pośrednictwem portalu Telegram, a swoje działania usprawiedliwiali w środowiskach internetowych powiązanych z diasporą, które usprawiedliwiały kolaborację jako płatne zlecenia, a nie szpiegostwo [98]. Ilustruje to jak kanały diaspory mogą zostać wykorzystane do osiągnięcia efektów kinetycznych przy jednoczesnym zachowaniu separacji między atakiem a jego sponsorem.

Białoruskie służby stosują podobne narzędzia wobec swoich diaspor, dodając element przymusu poprzez groźby wobec członków rodzin pozostających na Białorusi. Litewski coroczny raport nt. oceny zagrożeń państwowych dowodzi, że białoruskie służby wywiadowcze zmuszają członków licznej diaspory białoruskiej na Litwie do współpracy poprzez szantaż wobec krewnych w kraju. Zadania obejmują zbieranie informacji, infiltrację organizacji czy wywieranie presji na aktywistów, często pod przykryciem ambasad, konsulatów i wydarzeń diasporycznych [99]. Rezolucje Parlamentu Europejskiego odnotowują również transnarodowe zastraszanie przez białoruskie struktury, takie jak Komitet Śledczy, które starają się przenieść represje wewnętrzne na teren UE, m.in. poprzez wszczynanie spraw zaocznych i publiczne listy stygmatyzujące aktywistów, czyniące ich łatwiejszymi celami inwigilacji i nękania [100].

Dziennikarskie i analityczne rekonstrukcje fali dywersji i sabotażu w Europie potwierdzają, że rekrutacja osób przebiega przez kanały diaspory. Śledztwa transgraniczne wykazały, że rekruterzy z Rosji i Białorusi identyfikowali ekonomicznie wrażliwych migrantów w państwach UE i przekazywali im zadania przez Telegram oraz fora pracy dorywczej, co skutkowało serią podpaleń i misji rozpoznawczych. Wykonawcy często nie wiedzieli, jaki był strategiczny cel, interesowała ich jedynie zapłata. Dane te zostały potwierdzone przez akta sądowe, logi czatów i zapisy płatności [101]. Tam, gdzie dochodziło do ujęcia oficerów prowadzących okazywało się, że niewielka grupa koordynatorów porusza się w sferze czatów diaspory, kanałów nacjonalistycznych i pośredników kryminalnych zmieniając tożsamości, ale zachowując te same schematy rekrutacji i płatności. Dowodzi to, że mamy do czynienia z odpornym, wymiennym modelem pracy zamiast tradycyjnego *agent running* z epoki zimnej wojny [102] [103].

Efekt strategiczny eksploatacji diaspor jest kumulatywny. Instytucje wspólnotowe, które powinny służyć integracji i wzajemnej pomocy, stają się przestrzeniami spornymi, gdzie programy kulturalne i pomoc prawna są nie do odróżnienia od przekazów propagandowych i osłony aktywów. Osoby korzystające z grup wsparcia stają się celem rekrutacji lub zastraszania, co podważa zaufanie wewnątrz społeczności i między diasporami a państwami przyjmującymi. Służby bezpieczeństwa muszą poświęcać zasoby na badanie działań balansujących na granicy legalności, podczas gdy przeciwnik może twierdzić, że to aktywność obywatelska, a nie ingerencja obcego państwa. Dlatego europejskie instytucje bezpieczeństwa klasyfikują dziś ingerencję w diaspory jako priorytetowe zagrożenie dla demokracji – atakuje ona tkankę łączną społeczeństw otwartych, wykorzystując wolności oferowane nowo przybyłym i uchodźcom.

Warto podkreślić, że instrumentalizacja diaspor jest bezpośrednim dziedzictwem praktyk wywiadowczych ZSRR, który postrzegał emigrantów zarówno jako zagrożenie, jak i potencjalny rezerwuar rekrutacyjny [104]. KGB systematycznie infiltrowało grupy emigracyjne w okresie zimnej wojny, a dzisiejsze FSB, SVR i białoruski KGB kontynuują tę linię działań, korzystając z nowych narzędzi i praktyk. Wzorzec ten szczególnie wyraźnie widoczny jest w Polsce, na Litwie i w Niemczech, gdzie organizacje emigracyjne są monitorowane, infiltrowane i czasami zmuszane do współpracy.

Najnowsze przypadki pokazują, że dziedzictwo to zostało dostosowane do rekrutacji „jednorazowych szpiegów" wśród podatnych grup migrantów. Na przykład w 2024 roku niemieckie władze rozbiły sieć, w której rosyjskie służby rekrutowały migrantów z Ameryki Łacińskiej do tanich operacji sabotażowych, w tym podpaleń obiektów logistycznych i handlowych powiązanych z łańcuchem dostaw na rzecz Ukrainy [105]. W 2025 roku sądy w Wielkiej Brytanii skazały osoby, które rosyjscy oficerowie prowadzący skierowali do podpalenia magazynu powiązanego z transportem pomocy [106]. Wykonawców wybierano ze względu na anonimowość i wymienność, bez żadnych planów wobec ich długofalowej kariery wywiadowczej. Tymczasem w Polsce w 2023 r. rozbito siatkę składającą się z 16 osób, które zostały zrekrutowane do działań szpiegowskich, m.in. monitorowania infrastruktury transportowej oraz instalowania urządzeń śledzących [107] [108].

Nowe możliwości dzięki postępom technologicznym oprogramowania

Sztuczna inteligencja i nowoczesne narzędzia algorytmiczne przekształciły wojnę hybrydową z działalności manualnej, rzemieślniczej w system zautomatyzowany, adaptacyjny, skalujący się ponad językami, platformami i grupami odbiorców. Europejskie oceny zagrożeń dokumentują dziś, w jaki sposób manipulacja informacyjna z wykorzystaniem technologii AI służy industrializacji tworzenia treści, przyspiesza precyzyjne adresowanie grup odbiorczych i łączy operacje psychologiczne z tanimi próbami technicznymi przeciwko infrastrukturze i usługom publicznym [109]. Wyniki badań RAND [110] wskazują, że przewagę zyska ta strona, która najlepiej połączy masowość, dezinformację, elastyczne dowodzenie i odporność sieciową, ponieważ technologie te premiują szybkie interakcje i zdecentralizowane systemy C2[1].

Generatywne media stały się podstawowym narzędziem operacji wpływu. Dochodzenia dotyczące rosyjskich kampanii od 2022 roku wykazały rutynowe korzystanie z generatorów obrazów i wideo opartych na sztucznej inteligencji, klonowania głosu i automatycznych tłumaczeń, aby fabrykować lokalne „dowody", z dużą prędkością siać nowe plotki i dopasowywać narracje do różnych społeczności językowych, także wewnątrz UE [111]. **Centrum NATO StratCom COE** w swoich raportach o wirtualnych manipulacjach odnotowuje wymierny wzrost liczby treści generowanych przez AI na dziesięciu platformach, gdzie przeciwnicy testują kopie, obrazy i personalia nadawców, aby zwiększyć zaangażowanie i obciążyć możliwości fact-checkingu podczas kryzysów [112]. Analizy **RUSI** dokumentują z kolei, jak rosyjskie ekosystemy powiązane z wojskiem eksperymentowały z chatbotami na zamówienie i sztucznymi rzecznikami, którzy imitują autorytatywne głosy aby uwiarygadniać fałszywe twierdzenia, a następnie powtarzać je w zamkniętych kanałach jako rzekome potwierdzenie [113].

Automatyzacja nie ogranicza się do samego generowania treści. Kampanie wykorzystują obecnie pełne „linie produkcyjne wpływu", w których agenci i skrypty AI tworzą, oznaczają, tłumaczą, planują i testują tysiące materiałów, podczas gdy botnety dystrybuują najlepiej działające warianty do segmentów odbiorców zidentyfikowanych na podstawie danych platformowych i sygnałów OSINT. Dochodzenie z 2025 roku w sprawie ww. operacji Overload (*Matryoshka*) wykazało, że prorosyjscy działacze korzystali z darmowych, konsumenckich narzędzi AI, aby doprowadzić do „eksplozji treści" na Telegramie, X i innych platformach, w tym do tworzenia deepfake'ów z klonowanymi głosami, a nawet do spamowania fact-checkerów w celu manipulowania widocznością [114]. Ma to znaczenie dla demokracji: targetowanie algorytmiczne i personalizacja syntetyczna obniżają koszt prowadzenia równoległych mikrokampanii, które utwardzają polaryzację i wykorzystują istniejące resentymenty zamiast próbować przekonać niezdecydowanych [115].

Nowym polem starcia stało się zatruwanie modeli i danych, którego celem jest wpływanie na wyniki systemów AI. Doniesienia z 2025 roku opisują prorosyjską sieć, która nasyca otwarty internet pseudo-dziennikarskimi stronami i edycjami w pobocznych bazach wiedzy tak, aby chatboty ogólnego przeznaczenia powielały spreparowane fałsze – badacze nazwali tę taktykę groomingiem LLM [116]. Dostrzeżone zostały podobne skoordynowane działania, których celem jest „zatruwanie" modeli AI poprzez masowe publikowanie treści widocznych dla crawlerów na temat np. narracji o broni biologicznej, co z czasem zniekształca rozkład odpowiedzi mniej zabezpieczonych systemów [117]. Literatura wskazuje, że nawet niewielki odsetek skażonych danych może degradować filtry bezpieczeństwa i ukierunkowywać wyniki zgodnie z narracją przeciwnika [118].

1 C2 (*command and control*) oznacza strukturę dowodzenia i kontroli, w której decyzje zapadają centralnie, lecz wykonanie i dostosowanie odbywa się zdecentralizowanie, co zapewnia elastyczność i odporność na zakłócenia.

Prorosyjskie farmy botów zlikwidowane przez władze ukraińskie

Źródło: Wikicommons

AI zacieśnia również pętlę między operacjami cyfrowymi a działaniami przeciw celom fizycznym. Badania RAND dotyczące procesów poznawczych pokazują, że wspomagana przez maszyny analiza strumieni OSINT może przyspieszać identyfikację podatnych aktywów, zachowań tłumu i okien medialnych, co skraca cykl planowania działań hybrydowych, które mają skupić uwagę, a nie decydujący wynik kinetyczny [119] [120]. Europejskie raporty bezpieczeństwa dokumentują także, jak deepfake'i i treści generatywne są parowane z cyberpróbami lub incydentami dronowymi o niskich kosztach tak, aby wywoływać wielowymiarową presję, odciągać uwagę obrońców, generować fałszywe alarmy i następnie eksploatować powstałe zamieszanie online, zwłaszcza wokół Polski i regionu bałtyckiego.

Środki zaradcze ewoluują, ale są niespójne i sporne. Europejska odpowiedź polityczna podkreśla znaczenie pochodzenia i transparentności, w tym standardu C2PA służącego kryptograficznemu potwierdzaniu źródła i edycji treści, który duże platformy i wydawcy zaczęli wdrażać w przepływach redakcyjnych [121] [122]. Agencje bezpieczeństwa wskazują także na „content credentials" jako fundament programów integralności multimediów w erze generatywnej [123]. Równocześnie analitycy ostrzegają, że sama transparentność nie rozwiąże problemu przechwytywania uwagi czy zdolności przeciwnika do manipulowania treściami nieobjętymi certyfikacją i systemami rekomendacji platform. To wymaga wielowarstwowej obrony łączącej pochodzenie treści, wzmocnienie modeli, zwalczanie botnetów i odporność obywatelską [124] [125].

Pojawia się konsensus, że AI nie tylko przyspiesza istniejącą dezinformację, ale zmienia funkcję produkcji wpływu. Umożliwia przeciwnikom skalowanie wielojęzycznych treści, autogenerowanie sztucznych person prowadzących rozmowę zamiast emisji, i dostrajanie przekazów w czasie rzeczywistym, równocześnie korumpując bazę wiedzy, z której korzystają kolejne systemy AI [126] [127]. Dla państw frontowych, takich jak Polska, i sojuszników na północno-wschodniej flance NATO konsekwencje są jednoznaczne : sondowanie przestrzeni powietrznej, akcje sabotażowo-dywersyjne, podpalenia paczkowe i cyberintruzje są obecnie synchronizowane z kampaniami algorytmicznymi i manipulacjami na poziomie modeli, które łącznie nakładają koszty uwagi, eksploatują tarcia instytucjonalne i erodują zaufanie społeczne na dużą skalę. Skuteczna obrona wymaga traktowania manipulacji wspomaganej przez AI nie jako problemu medialnego, lecz jako zagrożenia operacyjnego, które łączy sferę informacyjną, cybernetyczną i fizyczną w jednym koncepcie działań.

Nowe możliwości dzięki postępom technologicznym w sprzęcie komputerowym

Rosyjskie i białoruskie służby dostosowały swoje operacje hybrydowe, wykorzystując rotacyjny zestaw systemów bezzałogowych, improwizowanych ładunków wybuchowych i cyfrowych kanałów koordynacyjnych, które kładą nacisk na zaprzeczalność i skalowalność. Celem nie jest jedno przełomowe rozwiązanie technologiczne, lecz iteracyjne, niskokosztowe innowacje, które obciążają europejskie systemy obronne z wielu kierunków jednocześnie, szczególnie na styku Polski i państw bałtyckich, gdzie najbardziej narażone są przestrzeń powietrzna, kolej i węzły logistyczne. Ostatnie incydenty pokazują schemat wykorzystywania dronów rozpoznawczych i kamikadze do testowania czasów reakcji, przeciążania obrony powietrznej i wywoływania efektów uwagi, które wzmacniają równoległe operacje informacyjne, podczas gdy cyberataki i zadania przekazywane przez aplikacje tworzą płynne przejście między sferą fizyczną i kognitywną [128].

Wyraźnym sygnałem tej ewolucji było pojawienie się rosyjskich dronów „Gerbera" nad terytorium NATO, w tym incydent z 10 lipca 2025 r., kiedy maszyna przekroczyła granicę białorusko-litewską i rozbiła się około kilometr w głąb terytorium kraju. Władze litewskie opisały ten bezzałogowiec jako drewnianą kopię irańskiego Shaheda, zoptymalizowaną pod kątem niskiego kosztu i zmylenia radarów, a później potwierdziły, że podobna maszyna znaleziona w rejonie poligonu w Gaižiūnai była wyposażona w ładunek wybuchowy, który musieli zneutralizować saperzy. Incydenty te skłoniły Wilno do ponownego wezwania NATO o dodatkowe środki antydronowe oraz do przyspieszenia krajowych planów obrony przed systemami bezzałogowymi [129] [130] [131]. W ciągu kilku tygodni urzędnicy odnotowali kolejne prawdopodobne naruszenie przestrzeni powietrznej z kierunku Białorusi, podkreślając intencję normalizacji presji na przestrzeń powietrzną NATO i testowania koordynacji sojuszniczej w szarej strefie poniżej progu eskalacji kinetycznej [132].

Nacisk w przestrzeni powietrznej zbiegł się z przemysłowym wysiłkiem wewnątrz Białorusi na rzecz rozbudowy produkcji bezzałogowców blisko granic NATO. W marcu 2025 r. białoruscy i rosyjscy urzędnicy ogłosili plany budowy zakładu dronów na Białorusi o masowej zdolności produkcji, potwierdzone przez doniesienia medialne i eksperckie wskazujące aktywność w Mińsku i przedstawiające inicjatywę jako element szerszej strategii relokacji wrażliwej produkcji pod osłoną Białorusi. Publiczne wypowiedzi władz w Mińsku o tworzeniu dedykowanych „wojsk dronowych" jako niezależnego rodzaju sił zbrojnych potwierdziły instytucjonalizację tego potencjału oraz jego integrację z funkcjami rozpoznawczymi, uderzeniowymi i wskazywania celów w strukturze sił zbrojnych Białorusi [133] [134] [135]. Analitycy ostrzegają, że nawet linie produkcyjne oznaczane jako „cywilne" mogą być wykorzystane dwojako, co uwidoczniły raporty wskazujące, że projekt początkowo koncentruje się na bezpilotowych statkach powietrznych (UAV) do celów rolniczych, ale pozostawia możliwości do adaptacji wojskowej w gospodarce wojennej [136].

Po stronie polskiej władze mierzą się z mieszanką incydentów powietrznych i cybernetycznych, które ilustrują, jak innowacje technologiczne służą kumulatywnemu efektowi zakłócania. Po serii alarmów w 2024 r. dotyczących możliwych naruszeń dronowych w trakcie rosyjskich ataków na Ukrainę, Polska uruchomiła poszukiwania i wzmocniła postawę obrony powietrznej, choć później odwołała jedno szeroko komentowane zdarzenie po analizie kryminalistycznej. Sam epizod ujawnił jednak obciążenie cyklami szybkiej reakcji w warunkach spornego obrazu powietrznego oraz trudność rozróżniania w czasie rzeczywistym prawdziwych naruszeń od anomalii sensorów, zwłaszcza gdy przeciwnicy wykorzystują tę niejednoznaczność do efektów narracyjnych [137] [138]. Równolegle Polska odnotowała utrzymującą się presję cybernetyczną wobec usług krytycznych, w tym udaremnioną

próbę przejęcia kontroli nad systemem wodociągowym w dużym mieście, którą urzędnicy przypisali szerszej kampanii wymierzonej w rolę Polski jako hubu logistycznego dla Ukrainy. Incydent ten pokazuje, że próby cybernetyczne i bezzałogowe stanowią jeden ciąg operacyjny, który szuka zarówno dostępu, jak i efektu uwagi, zmuszając obrońców do ponoszenia kosztów odporności przy jednoczesnym utrzymywaniu niepewności co do atrybucji i intencji [139].

Innowacje technologiczne w tym środowisku mają charakter celowo inkrementalny. Tanie lokalizatory GPS i elektronika konsumencka mogą być przekształcane w moduły czasowe lub inicjujące do urządzeń zapalających przenoszonych przez systemy kurierskie, podczas gdy tanie drony budowane z komponentów komercyjnych można konfigurować do rozpoznania, przenoszenia ładunków lub symbolicznych przelotów wywołujących nadmierny niepokój społeczny. Europejskie studia przypadków z początku 2025 r. dokumentowały paczki maskowane jako towary konsumenckie zawierające domowej roboty ładunki zapalające i mechanizmy czasowe oparte na lokalizatorach GPS, dostarczane do centrów dystrybucyjnych w celu testowania procedur kontroli i zakłócania operacji, przy zachowaniu kosztów na poziomie sprzyjającym powtarzalności. Tą samą logiką kieruje się wybór drewnianych lub kompozytowych kadłubów dla dronów typu Gerbera, które komplikują wykrywanie radarowe i pozwalają przeciwnikowi „wydrenować" budżet uwagi obrońcy przy minimalnych kosztach [140] [141].

Reakcje obronne w regionie zaczynają dostosowywać się do tej zmiany technologicznej. Litwa zwróciła się o sojusznicze wsparcie antydronowe i uruchomiła programy szkolenia i edukacji dronowej dla ludności, aby zbudować cywilną rezerwę operatorów i obserwatorów – krok, który uznaje, że sieć sensorów obejmująca całe społeczeństwo może skracać czasy reakcji i komplikować plany przeciwnika. Władze zapowiadają etapowe uruchamianie ośrodków szkoleniowych, programów dla dorosłych i uczniów oraz ich integrację z narodowymi planami obrony cywilnej aby podnieść minimalny poziom kompetencji w populacji [142]. Polska z kolei przyspieszyła prace nad wzmocnieniem obrony przestrzeni powietrznej i strukturą sił dronowych, a w komunikatach publicznych podkreśla częstotliwość rosyjskich cyberataków i konieczność łączenia obrony cywilnej i wojskowej. Jest to narracja spójna z hybrydową naturą zagrożenia i logiką nakładania kosztów [143].

Razem zjawiska te pokazują, że innowacja technologiczna w obecnej kampanii hybrydowej nie dotyczy systemów przełomowych, lecz gotowości przeciwnika do iteracji . Tanie drony, które łączą rozpoznanie z sygnałami psychologicznymi, paczki z ładunkami zapalającymi testujące łańcuchy dostaw i uporczywe próby cybernetyczne wobec usług krytycznych tworzą współzależne linie działania. Zmuszają one rządy europejskie do wydawania pieniędzy i kapitału politycznego na zabezpieczenia trudne do dojrzenia i jeszcze trudniejsze do zmierzenia, podczas gdy inicjator zachowuje zaprzeczalność i swobodę eskalacji lub wycofania się według własnego wyboru. Efekt strategiczny wynika ze stopniowego wyczerpywania uwagi i zasobów, a nie z pojedynczego uderzenia i jest możliwy dzięki cyklowi pozyskiwania i innowacji, który traktuje technologię konsumencką jako gotowy arsenał [144] [145] [146].

Czas: pięć faz w cyklach narracyjnych i operacyjnych

Pięć opisanych powyżej typologii operacyjnych nie stanowi odizolowanych aktów, lecz zintegrowane węzły w ramach szerszej kampanii hybrydowej, zaprojektowanej pod kątem skumulowanej destabilizacji w wielu domenach. Fragmentacja sprawia, że każdy incydent, choć sam w sobie drobny i wiarygodny, dokłada się do szerszej atmosfery chaosu percepcyjnego. Maskowanie zaciera atrybucję, nadając operacjom pozory działalności kryminalnej lub lokalnej, co zapewnia wiarygodną zaprzeczalność.

Harmonogram wydarzeń synchronizuje je z debatami politycznymi, ruchami wojsk NATO lub symbolicznymi rocznicami maksymalizując efekt psychologiczny. Sprzężenie narracji wzmacnia każde fizyczne zakłócenie poprzez zsynchronizowane działania informacyjne, mnożąc dezorientację i pogłębiając nieufność społeczną. Ułożone w kolejności moduły te tworzą sprzężenia zwrotne: incydent wywołuje kampanię informacyjną, oficjalna reakcja staje się widowiskiem medialnym, a zaufanie eroduje krok po kroku, prowadząc do degradacji bez eskalacji do otwartego konfliktu.

Typy operacji opisane powyżej są ustrukturyzowane w sekwencjach fazowych, które rozciągają się tygodniami lub miesiącami. Ich rytm wydaje się losowy, lecz w rzeczywistości podąża za zaplanowaną logiką kognitywną:

- **Faza pierwsza** inicjuje przygotowanie narracyjne. Obejmuje to sianie plotek, memów, przecieków lub ram interpretacyjnych poprzez mikroinfluencerów. Treści często obracają się wokół rzekomych „prowokacji" NATO, hipokryzji Zachodu czy niekompetencji instytucjonalnej.
- **Faza druga** wprowadza markery kinetyczne. Najczęściej są to drobne akty dywersji lub sabotażu, takie jak pożary magazynów, wtargnięcia dronów czy zakłócenia w logistyce kolejowej. Celem nie jest masowe zniszczenie, lecz psychologiczna ingerencja i niejednoznaczność
- **Faza trzecia** łączy incydent z ramą narracyjną. Odbywa się to poprzez dyfuzję diaspory, automatyczne udostępnienia i ukierunkowane plotki. Wprowadzane są narracje emocjonalne, które zostają zapętlone, by wytworzyć chwytliwe interpretacje. Ten sam pożar może być przedstawiony jako dowód eskalacji NATO, porażki państwa albo obojętności elit – w zależności od odbiorcy.
- **Faza czwarta** wykorzystuje reakcję instytucji. Wszelkie sprzeczności w komunikatach, niespójności w atrybucji lub opóźniona reakcja publiczna są interpretowane jako dowód oszustwa lub bezsilności. To właśnie tutaj teren kognitywny staje się najbardziej podatny.
- **Faza piąta** resetuje cykl. Uruchamiany jest nowy mikroincydent lub przekaz, budujący na wcześniej osiągniętej erozji .

Powtarzalność tych pięciu faz podtrzymuje środowisko podejrzliwości, zmęczenia i przeciążenia percepcyjnego, stopniowo osłabiając spójność społeczną nawet w sytuacji braku ataków o dużej skali.

5 Martwe punkty, błędy adaptacyjne i jak je naprawić

Pomimo wieloletniej ekspozycji na rosyjskie i białoruskie kampanie hybrydowe, Zachód nadal funkcjonuje z krytycznymi deficytami strukturalnymi i kognitywnymi . Te ślepe punkty nie są wyłącznie technicznymi przeoczeniami. Mają charakter systemowy, instytucjonalny i koncepcyjny, a ich źródłem są przestarzałe modele zagrożeń oraz fragmentaryczne ramy zarządzania. Niniejszy rozdział wskazuje cztery główne linie pęknięć: **deficyt poznawczy, lukę systemową, próżnię interoperacyjności oraz próżnię regulacyjną**.

Deficyt poznawczy: brak zintegrowanego rozumienia zagrożeń

Istotną słabością wykazywaną przez państwa zachodnie jest niezdolność do koncepcyjnej integracji zagrożeń subpercepcyjnych i hybrydowych w ramach systemów bezpieczeństwa narodowego. Instytucje zachodnie często traktują dywersję, sabotaż, dezinformację, szpiegostwo i przymus symboliczny jako zjawiska odrębne, a nie jako wyraz spójnej architektury strategicznej.

Służby kontrwywiadowcze wciąż priorytetowo traktują zagrożenia kinetyczne i techniczne, zaniedbując długofalowe zarządzanie percepcją. Szczególnie widoczne jest to w podejściu do rosyjskich operacji informacyjnych, które nadal bywają lekceważone jako zwykła „propaganda" lub traktowane jako odizolowane przypadki ingerencji wyborczej, zamiast być postrzegane jako przygotowanie kognitywne pod szerszą destabilizację. Brak wspólnej mapy poznawczej w instytucjach utrudnia rozpoznawanie wzorców w dyfuzji narracji, imitacji transgranicznej i zakłócaniu procesów psychologicznych [147]. Podobnie brak horyzontalnej, państwowej strategii przeciwdziałania dezinformacji oraz tolerowanie mikrotargetingu politycznego sprawiają, że państwo pozostaje podatne na manipulacje podważające spójność społeczną i bezpieczeństwo informacyjne.

Co więcej, niewiele rządów zinstytucjonalizowało mechanizmy antycypacyjnego monitorowania środowisk narracyjnych. Zdolności otwartego wywiadu (OSINT) są słabo rozwinięte, a profile analityczne potrzebne do długoterminowej analizy percepcji rzadko występują w systemach biurokratycznych bezpieczeństwa narodowego. Rosja i Białoruś wykorzystują to opóźnienie, kształtując dyskurs na długo przed formalnym pojawieniem się kryzysów [148].

Rekomendacje:

- Rządy krajowe powinny ustanowić stałe komórki służb specjalnych ds. zagrożeń hybrydowych jako zintegrowane centra łączące kontrwywiad wojskowy, obronę cybernetyczną, kontrwywiad i komunikację strategiczną. W przypadku Polski najbardziej zasadnym miejscem byłoby Rządowe Centrum Bezpieczeństwa lub Kancelaria Premiera, aby zapewnić koordynację komórki ponad resortami.
- Komórki te powinny wykrywać i analizować agresję poniżej progu konfliktu łącząc wiele strumieni informacji, w tym wzorce obecne w mediach społecznościowych poprzedzające kampanie dezinformacyjne, anomalie wskazujące na włamania cybernetyczne oraz sygnały sabotażu pośredniego wobec infrastruktury krytycznej.
- Nacisk na identyfikację wskaźników "left of launch" powinien być położony w ramach NATO tak, aby zapewnić wczesne ostrzeganie, zanim operacje hybrydowe zdążą się zmaterializować.
- W ramach UE jednostki krajowe powinny być sieciowane i koordynowane poprzez Hybrid Fusion Cell, będące centralnym punktem analizy zagrożeń hybrydowych w Unii.
- Rządy muszą wyposażyć personel tych komórek w zaawansowane szkolenia analityczne i narzędzia oparte na AI, aby zwiększyć zdolności wykrywania i rozpoznawania wzorców międzydomenowych.
- Należy zinstytucjonalizować ciągłą transgraniczną wymianę informacji między rządami, aby przyspieszyć atrybucję, ograniczyć niejednoznaczności wykorzystywane przez przeciwników i umożliwić szybkie, skoordynowane reakcje.

Luka systemowa: fragmentacja kontrwywiadu, cyberbezpieczeństwa i polityki wewnętrznej

Rosyjskie i białoruskie operacje płynnie przekraczają granice administracyjne. Jedna kampania może obejmować rekrutację aktorów z diaspory, użycie botów na Telegramie, penetrację lokalnych mediów i manipulację protestami. Tymczasem reakcje Zachodu są podzielone pomiędzy ministerstwa, agencje i mandaty, z niewielką integracją horyzontalną czy koordynacją w czasie rzeczywistym. Efektem jest poślizg operacyjny. Informacje zebrane przez służby krajowe rzadko trafiają na czas do władz lokalnych. Centra dowodzenia cybernetycznego są często odcięte od kontekstu społeczno-politycznego i nie potrafią ocenić narracyjnych skutków naruszeń. W Polsce NASK łączy te dwie sfery. Taka segmentacja tworzy opóźnienie między wykryciem a reakcją, które może być potem wykorzystane przez wrogie służby.

Konferencja NATO w sprawie zobowiązań dotyczących cyberobrony w Hadze, Holandia, 17 maja 2024 r.

Źródło: Wikimedia

Rekomendacje:

- Rządy muszą zintegrować wszystkich istotnych aktorów w ramach jednolitej struktury obronnej, aby zamknąć luki systemowe w przeciwdziałaniu zagrożeniom hybrydowym.
- Na poziomie krajowym państwa powinny ustanowić międzyagencyjne centra koordynacji łączące kontrwywiad, obronę cybernetyczną, komunikację strategiczną i decydentów politycznych w celu oceny zagrożeń i koordynacji odpowiedzi.
- Modele z Wielkiej Brytanii i państw bałtyckich (szczególnie estoński) stanowią skuteczne przykłady i powinny być upowszechniane w ramach forów NATO i UE.
- Na poziomie UE wezwanie zawarte w Strategii Bezpieczeństwa Wewnętrznego 2025 do stworzenia „prawdziwego europejskiego koncertu" powinno zostać zoperacjonalizowane poprzez stałą Radę ds. Zagrożeń Hybrydowych, łączącą instytucje ds. bezpieczeństwa, spraw wewnętrznych i polityki zagranicznej.
- NATO powinno uzupełnić te działania poprzez promowanie kompleksowych ram odpornościintegrujących obronę cywilną, wojskową i informacyjną.
- Propozycje takie jak wezwanie prezydenta Sauli Niinistö do utworzenia europejskiej służby współpracy wywiadowczej i sieci „antysabotażowej" podkreślają potrzebę struktur transgranicznych w celu zaadresowania niedociągnięć instytucjonalnych.
- Sojusznicy powinni prowadzić wspólne ćwiczenia z wykorzystaniem scenariuszy kontr-hybrydowych, wymagających współpracy w czasie rzeczywistym między specjalistami od cyberbezpieczeństwa, służb specjalnych, policji i polityki w obszarze bezpieczeństwa.

Integracja tych działań pozwoli państwom NATO i UE stworzyć jednolitą siłę przeciwdziałania, zdolną szybko wykrywać i zakłócać operacje hybrydowe, wzmacniając odporność i umacniając efekt odstraszania.

Deficyt interoperacyjności: silosy danych między służbami państw członkowskich

W państwach UE i NATO dane i informacje wywiadowcze oraz kontrwywiadowcze (lub pochodzące ze służb specjalnych) dotyczące zagrożeń hybrydowych pozostają nierównomiernie udostępniane albo nie są wymieniane wcale. Problem ten ma charakter nie tylko techniczny, lecz także prawny, polityczny i kulturowy.

Służby działające w obszarze bezpieczeństwa wciąż ograniczone są mandatami narodowymi i niechętnie dzielą się efektami swoich operacji i działań operacyjno-rozpoznawczych, zwłaszcza w politycznie wrażliwych obszarach, takich jak dezinformacja czy radykalizacja wewnętrzna. Co więcej, różne definicje tego, co stanowi zagrożenie hybrydowe, prowadzą do niekompatybilnych systemów klasyfikacji. Incydent dywersyjno-sabotażowy uznany w jednym kraju za terroryzm w innym może być traktowany jako drobne przestępstwo. Taka niespójność tworzy transgraniczne luki poznawcze, które przeciwnicy mogą swobodnie wykorzystywać.

Wspólne platformy świadomości sytuacyjnej, takie jak unijna Hybrid Fusion Cell czy Dywizja ds. Zagrożeń Hybrydowych NATO istnieją, lecz brakuje im zarówno uprawnień wykonawczych, jak i głębokich zdolności analitycznych. Ich produkty są często ograniczone do biuletynów zagrożeń zamiast do operacyjnej integracji. Sprzyja to postawie reaktywnej i utrudnia rozwój zdolności do przeciwdziałania zagrożeniom hybrydowym.

Rekomendacje:

- Państwa członkowskie NATO i UE muszą priorytetowo potraktować bezpieczne i proaktywne dzielenie się informacjami wywiadowczymi, aby naprawić obecne luki interoperacyjności.
- Praktyczne rozwiązania, w tym kierowanie informacji przez Biuro Bezpieczeństwa NATO jako neutralny kanał, mogą zapewnić dostęp do danych wszystkim interesariuszom bez konieczności zawierania pełnych traktatów.
- NATO powinno traktować informacje udostępniane jako zasób strategiczny, rozwijając interoperacyjne sieci o klauzuli tajności i przyjąć wspólne standardy oznaczania danych.
- Agencje krajowe powinny przyjąć kulturę „dare to share", wzmacniając wymianę bilateralną i multilateralną, prowadząc wspólne operacje i delegując oficerów do służb partnerskich. Niezbędne przy tym będzie jednoczesne wypracowanie mechanizmów rozwiązujących kwestie kosztów ich utrzymania, ochrony tajemnicy państwowej oraz budowania zaufania, co jest szczególnie istotne mimo, że wspólne operacje z partnerami są już prowadzone.
- Ramy takie jak G7 Rapid Response Mechanism i Zespoły Wsparcia Przeciwhybrydowego NATO powinny zostać przekształcone w struktury stałe i rozwinięte.
- Państwa NATO i UE powinny opracować mechanizmy bezpiecznej wymiany danych o zagrożeniach hybrydowych, które nie zastąpią spotkań osobistych, ale pozwolą szybko udostępniać techniczne alerty. Post-kwantowe algorytmy kryptograficzne, elementy kryptografii kwantowej dla kluczowych kanałów, rozproszone systemy uwierzytelniania oraz sieci wczesnego ostrzegania oparte na AI mogą być elementami wsparcia tych mechanizmów.

Instytucjonalizacja kultury wymiany informacji zamknie luki podatne na wykorzystanie, umożliwi szybszą atrybucję i reakcję oraz wzmocni odstraszanie poprzez zapewnienie, że wrogie operacje będą zbiorowo demaskowane.

Próżnia regulacyjna: brak skutecznych instrumentów prawnych do przeciwdziałania obcym wpływom

W przeciwieństwie do Stanów Zjednoczonych, które dysponują instrumentami prawnymi takimi jak Foreign Agents Registration Act (FARA), większość państw europejskich nie ma instytucjonalnych mechanizmów do monitorowania, regulowania czy ujawniania operacji obcego wpływu. Aktorzy rosyjscy i białoruscy wykorzystują tę lukę prawną, osadzając struktury wpływu w think tankach, sieciach kościelnych, instytucjach kultury czy pseudo-mediach. Te ośrodki funkcjonują jako mnożniki dezinformacji i kanały miękkiego przymusu, pozostając jednocześnie chronione prawnie jako podmioty społeczeństwa obywatelskiego. Zachodnie demokracje często wahają się przed nakładaniem wymogów ujawniania czy transparentności w obawie przed naruszeniem wolności słowa lub zrzeszania się [149].

Rezultatem jest paradoks- normy liberalne stają się tarczą dla ingerencji nieliberalnych. Państwa są sparaliżowane nie przez bezpośrednie zagrożenie, lecz przez tarcia pomiędzy własną prawną otwartością a strategiczną nieprzejrzystością przeciwnika. Nawet gdy podejrzenie złowrogiego wpływu jest wyraźne, brak kategorii prawnych do jego zakwalifikowania lub ścigania prowadzi do proceduralnej inercji.

Rekomendacje:

Zaradzenie tej próżni wymaga zdecydowanych działań legislacyjnych i politycznych, które ujawnią i zneutralizują sieci obcego wpływu, nie podważając jednocześnie fundamentów demokracji:

- Liderzy NATO i UE powinni uznać przejrzystość działalności politycznej finansowanej z zagranicy za podstawowy wymóg bezpieczeństwa, a nie opcjonalny środek.
- Państwa członkowskie powinny wprowadzić lub wzmocnić przepisy dotyczące rejestracji wpływów zagranicznych, wzorowane na amerykańskim prawie FARA i brytyjskim Foreign Influence Registration Scheme.
- Takie przepisy muszą zobowiązywać osoby i podmioty działające w imieniu obcych rządów do rejestrowania działań obejmujących lobbing, operacje medialne, finansowanie NGO i inne formy wywierania wpływu.
- Niezastosowanie się do przepisów powinno skutkować poważnymi sankcjami, w tym grzywnami i potencjalną odpowiedzialnością karną.
- UE powinna przyspieszyć prace nad własnym mechanizmem transparentności obcych wpływów, zapewniając wzajemne uzupełnianie się rejestrów krajowych i unijnych, a nie prowadząc do ich fragmentacji.
- NATO i UE powinny powołać wspólną grupę zadaniową ds. prawa, która zintegruje najlepsze praktyki i zamknie luki prawne wykorzystywane przez wrogich aktorów.
- Egzekwowanie musi być wspierane przez dobrze finansowane jednostki dochodzeniowe, uprawnione do żądania ujawnienia informacji i sankcjonowania ukrytego wpływu, w tym fałszywych mediów czy organizacji powiązanych z zagranicznym wywiadem.
- Przepisy muszą być elastyczne, z regularnymi aktualizacjami obejmującymi nowe taktyki, takie jak dezinformacja wspomagana AI, ukryte finansowanie influencerów czy deepfake'i.
- Wymogi przejrzystości powinny być połączone z systematyczną analizą, przy czym centra doskonałości NATO i UE powinny przetwarzać dane rejestrowe w celu identyfikacji złowrogich kampanii.
- W razie potrzeby operacje obcego wpływu powinny być publicznie ujawniane, tak aby przejrzystość stała się narzędziem odstraszania.

Tworząc egzekwowalne rejestry wzorowane na FARA, koordynując działania międzynarodowe i dostosowując się do zmian technologicznych, sojusznicy mogą odebrać Moskwie i Mińskowi anonimowość, na której polegają, wzmacniając odporność demokratyczną i chroniąc otwarte społeczeństwa przed wrogą infiltracją.

Odwrócenie ról: legalne działania hybrydowe przeciwko Rosji i Białorusi

Reakcje Zachodu były dotychczas w przeważającej mierze reaktywne. Tymczasem dysponuje on ogromnym, w dużej mierze niewykorzystanym potencjałem, który może narzucać trwałe tarcia kognitywne, prawne, finansowe i operacyjne w ekosystemach wywiadowczych Rosji, bez uciekania się do nielegalnych metod czy atakowania ludności cywilnej. Do tych zasobów należą m.in. niezrównane możliwości wywiadu finansowego banków i sieci płatniczych, które pozwalają identyfikować powiązania finansowe, śledzić przepływy podejrzanych środków i blokować mechanizmy prania pieniędzy wspierające operacje wywiadowcze. Istotna jest także kontrola eksportu w łańcuchach dostaw półprzewodników i obrabiarek, przewaga morska dzięki ubezpieczeniom i kontroli państw portowych, a także konsorcja dziennikarstwa śledczego i społeczności OSINT. Te ostatnie nie mogą być formalnie wykorzystywane przez państwa do działań niejawnych, ale mogą być wspierane poprzez finansowanie, dostęp do danych i mechanizmy wymiany informacji, co zwiększa ich skuteczność i komplementarność względem działań instytucjonalnych.

Kolejnym zasobem jest dostęp do platform cyfrowych poprzez wiążące mechanizmy transparentności i programy „trusted flagger", sieci diaspory oraz antyreżimowych Rosjan i Białorusinów na uchodźstwie, a także wykorzystanie jurysdykcji uniwersalnej, czyli możliwości ścigania sprawców najpoważniejszych przestępstw niezależnie od miejsca ich popełnienia i obywatelstwa sprawcy. Wsparciem są również sankcje w stylu tych wprowadzonych w Magnitsky Act, cyber zdolności organów ścigania pozwalające przejmować infrastrukturę i blokować domeny, co jest już praktykowane m.in. we wspólnych działaniach polsko-czeskich czy amerykańskich, a także dane satelitarne i system AIS służące do atrybucji w czasie rzeczywistym. Całość uzupełnia siła sprawcza NATO, UE i G7 w zakresie synchronizacji ekspozycji i sankcji.

Wykorzystane spójnie, narzędzia te umożliwiają ofensywę opartą na prawdzie, która zakłóca logistykę tajnych operacji Rosji, podnosi koszty działań zlecanych pełnomocnikom i osłabia kontrolę reżimu nad narracjami wewnątrz kraju i za granicą, pozostając przy tym w zgodzie z prawem międzynarodowym i krajowym.

Rekomendacje:

- NATO, UE i państwa członkowskie powinny powołać Inicjatywę Transparentności i Zakłócania, łączącą jednostki wywiadu finansowego, organy kontroli eksportu, regulatorów morskich, organy ścigania w cyberprzestrzeni oraz śledczych OSINT w celu mapowania i publicznego ujawniania sieci pełnomocników Rosji, firm przykrywkowych, szlaków logistycznych i łańcuchów dezinformacyjnych w trybie ciągłym.
- Utworzyć wspólną komórkę sankcyjno-prawną, która będzie przekształcać każde ujawnienie w skoordynowane działania: wpisy na listy sankcyjne Magnitskiego[2], zamrożenia aktywów, zakazy eksportu, konfiskaty cywilne oraz postępowania sądowe przeciwko podmiotom wspierającym.
- Wykorzystać kontrolę państw portowych, towarzystwa klasyfikacyjne i przewagę ubezpieczeniową do blokowania „floty cieni" oraz odmowy świadczenia usług statkom i operatorom powiązanym z obchodzeniem sankcji.
- Powołać wyspecjalizowany zespół ds. cyber bezpieczeństwa na poziomie krajowym,

2 Listy sankcyjne Magnitskiego to zestawienia osób i podmiotów objętych zakazem wjazdu oraz zamrożeniem aktywów na podstawie ustaw Magnitskiego, które pozwalają karać sprawców poważnych naruszeń praw człowieka i korupcji niezależnie od miejsca ich popełnienia. Takie mechanizmy wdrożyły m.in. Stany Zjednoczone, Kanada, Wielka Brytania, Unia Europejska oraz kraje bałtyckie. Nazwa pochodzi od Siergieja Magnitskiego, rosyjskiego prawnika, który ujawnił wielką aferę korupcyjną w Rosji i zmarł w 2009 roku w moskiewskim areszcie w wyniku tortur.

działający w ramach uprawnień i pod nadzorem sądów krajowych, odpowiedzialny za przejmowanie botnetów, likwidację klastrów podszywających się pod inne podmioty i blokowanie domen służących wrogim wpływom.

- Rozszerzyć wsparcie dla niezależnych mediów rosyjskojęzycznych, narzędzi omijania cenzury i bezpiecznych kanałów cyfrowych dla sygnalistów, aby prowadzić ofensywę prawdy wymierzoną w korupcję, ukrywanie strat wojennych i przywileje elit, koordynowaną z partnerami diaspory i organizacjami uchodźców.
- Zobowiązać duże platformy cyfrowe do wdrożenia weryfikowalnych systemów pochodzenia treści i interfejsów API transparentności, umożliwiających zaufanym badaczom i regulatorom śledzenie międzyplatformowego prania narracji, z możliwością szybkiego usuwania skoordynowanych działań nieautentycznych.
- Zbudować Tarczę Zakupową Sojuszu, która oznacza komponenty i obrabiarki wysokiego ryzyka, wdraża mechanizmy weryfikacji końcowego użytkowania i ściga przekierowywanie dostaw przez huby tranzytowe.
- Utworzyć zweryfikowane kanały odpowiedzialnej współpracy z antyreżimowymi Rosjanami i Białorusinami na Zachodzie, skupiając się na zeznaniach świadków, przekazywaniu dokumentów i działaniach obywatelskich, które delegitymizują służby bezpieczeństwa przy jednoczesnej ochronie uczestników.

Łącznie te działania mogą odwrócić sytuację, zabrać Rosji inicjatywę i zmusić ją do obrony własnych sieci pod stałą presją prawną i informacyjną, zwiększając koszty agresji poniżej progu wojny i wzmacniając odstraszanie bez rezygnacji z zasad demokratycznych.

Polska: ograniczenia krajowe i potrzeba instytucjonalnej zmiany paradygmatu

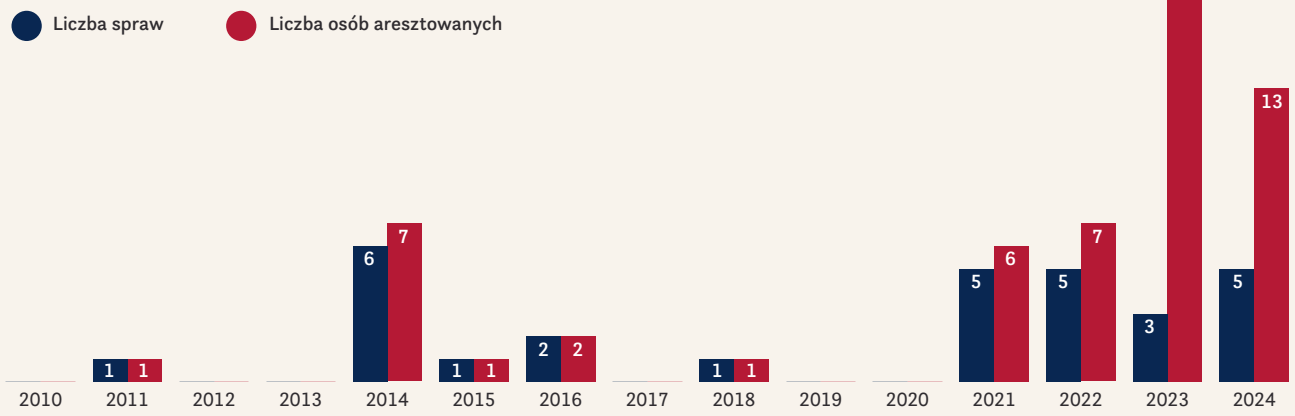
Polski system służb specjalnych i bezpieczeństwa nadal funkcjonuje w oparciu o koncepcje odziedziczone z czasów zimnej wojny, a nie w realiach konfliktu hybrydowego XXI wieku. Architektura ta jest zdefiniowana przez silosy, w których kontrwywiad, obrona cybernetyczna, organy ścigania i zarządzanie kryzysowe działają w ramach wąskich mandatów, uniemożliwiających szybkie i zintegrowane działania. Przeciwnicy wykorzystują tę fragmentację poprzez niskokosztowych, tokenizowanych operatorów, jednorazowe komórki szpiegowskie i techniki saturacji narracyjnej, które mogą przeciążyć reaktywne biurokracje. Zamiast obrony antycypacyjnej , system faworyzuje kolekcjonowanie informacji i procedury, co oznacza, że wrogie operacje są rozumiane dopiero wtedy, gdy już wywołały skutki w domenie poznawczej lub infrastrukturalnej. Rezultatem jest strukturalne opóźnienie: Rosja i Białoruś iterują swoje operacje szybciej, niż polskie instytucje są w stanie je przetwarzać, badać i reagować.

W tym kontekście rządowa propozycja reformy Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu wprowadza dodatkowy nadzór proceduralny poprzez rozszerzenie kontroli sądowej nad metodami operacyjnymi i dostępem do materiałów wywiadowczych [150]. Choć kroki te mają zwiększyć transparentność, która jest powodem wielu opóźnień i braku dynamizmu w działaniu służb specjalnych, głębsze deficyty w elastyczności, integracji i zdolnościach antycypacyjnych nie zostają zaadresowane. Projekt ustawy proponuje udoskonalenie tych procesów, lecz nie zmienia fundamentalnej inercji struktur odziedziczonych po zimnej wojnie, ryzykując paradoks wzmocnienia systemu, który przeciwnicy już nauczyli się obchodzić. Należy jednak odnotować także sygnały pozytywne: zatrzymanie w 2025 r. obywatela Białorusi podejrzanego o działalność sabotażową w Polsce i równoczesne wydalenie dyplomaty białoruskiego wskazują na coraz silniejszą regionalną współpracę kontrwywiadowczą, obejmującą także Czechy, Węgry, Rumunię i Mołdawię [151].

Ważnym, lecz przerwanym źródłem wiedzy o operacjach wpływu rosyjskiego i białoruskiego była praca **Komisji Parlamentarnej ds. wpływów rosyjskich i białoruskich (2004–2024)**. Komisja zgromadziła i przeanalizowała blisko 17 000 stron dokumentów oraz przygotowała studia przypadków dotyczące kampanii dezinformacyjnych, ingerencji w wybory i destabilizacji migracyjnej na polsko-białoruskim pograniczu [152] [153]. Jak zauważyła prof. Irena Lipowicz, jej ustalenia mogłyby stanowić cenne fundamenty dla reform systemowych i bardziej zintegrowanego podejścia do przeciwdziałania wojnie kognitywnej [154]. Komisja została jednak rozwiązana, zanim jej pełne wyniki ujrzały światło dzienne, co przerwało proces konsolidacji wiedzy instytucjonalnej i uniemożliwiło wykorzystanie zgromadzonych dowodów do zmian politycznych i operacyjnych.

Warto także podkreślić działania NASK, które uzupełniają lukę po przerwanej pracy Komisji Parlamentarnej. W swoich raportach instytut systematycznie dokumentuje operacje dezinformacyjne i cybernetyczne. Raport CERT Polska z 2023 roku wskazuje na gwałtowny wzrost incydentów, w tym falę ataków DDoS powiązanych z wyborami w Polsce, a także na aktywność grup APT związanych z Rosją, które ingerowały w infrastrukturę i kampanie polityczne [155]. Dodatkowo, analizy NASK z 2023 roku dokumentują destabilizujące kampanie narracyjne na polsko-białoruskim pograniczu, łączące dezinformację migracyjną z działaniami w cyberprzestrzeni [156]. Te materiały stanowią dziś jedno z najpełniejszych publicznie dostępnych źródeł wiedzy o narzędziach wojny poznawczej wymierzonych w Polskę i jej otoczenie. Z kolei „Raport o światowej dezinformacji wyborczej 2024" pokazuje, jak Rosja i Chiny adaptują narracje do lokalnych kontekstów, w Meksyku poprzez deepfake'i, w Tajwanie przez systematyczne kampanie Pekinu, a w Stanach Zjednoczonych poprzez wzmacnianie polaryzacji społecznej [157].

Aresztowania za rosyjskie szpiegostwo i sabotaż w Polsce, 2018–2025



Źródło: Agencja Bepieczeństwa Wewnętrznego (ABW)

Rekomendacje:

- Utworzyć Program Wczesnego Ostrzegania Poznawczego przy Krajowej Radzie Mediów, zintegrowany z CERT-PL. Program ten łączyłby wywiad otwarty (OSINT), telemetrykę platform w czasie rzeczywistym (poprzez obowiązkowy dostęp API dla dużych platform) oraz analizę sądową materiałów medialnych. Skoki narracyjne wokół tematów takich jak napływ uchodźców czy domniemane luki w bezpieczeństwie uruchamiałyby z góry określone protokoły ochronne, np. wzmocnione monitorowanie bocznic kolejowych, wzmocnioną obecność policji w węzłach logistycznych czy aktywację kontrnarracji poprzez lokalne media o wysokim poziomie zaufania.
- Powołać sektorowe zespoły zadaniowe dla korytarzy logistycznych (porty, węzły kolejowe, ośrodki transgraniczne) oraz węzłów telekomunikacyjnych. Każdy zespół łączyłby operatorów infrastruktury z ABW, Policją i CERT-PL, spotykając się co miesiąc na symulacjach red-team, testujących wrogie metody: rekrutację kurierów przez Telegram, urządzenia zapalające w paczkach, niskopodpisowe ataki dronowe. Wyniki zasilałyby sektorowe podręczniki obronne.
- Budowa niskokosztowej warstwy obrony antydronowej, obejmującej czujniki akustyczne, mobilne zespoły przechwytujące i systemy zakłócające, powinna stać się priorytetem modernizacyjnym Europy Środkowej, aby zniwelować kosztową asymetrię wobec rosyjskich ataków.
- Wprowadzić obowiązek wspólnych szkoleń i kwartalnych ćwiczeń międzyresortowych pod nadzorem Rządowego Centrum Bezpieczeństwa. Ćwiczenia obejmowałyby zakłócanie działań wrogich komórek przed aktywacją i koordynowane komunikaty publiczne, by uniemożliwić przeciwnikowi wykorzystanie błędów instytucjonalnych.
- Wyposażyć służby specjalne w platformy wspomagane AI do wykrywania i korelacji przypadków, opracowane we współpracy z NASK i zaufanymi dostawcami. Służby miałyby obowiązek przyjęcia wspólnych TTP (tactics, techniques, procedures) w zakresie skanowania paczek, przechwytywania dronów i szybkiego wyłączania infrastruktury wspierającej, takiej jak konta jednorazowe czy nielegalne łańcuchy dostaw.
- Powiązać reformę prawną z mandatami operacyjnymi, łącząc nowe przepisy nadzorcze z egzekwowalnymi wymogami integracji i metrykami odpowiedzialności. Niezależny nadzór parlamentarny współistniałby z wiążącymi wymogami obrony wyprzedzającej oraz przejrzystym raportowaniem skuteczności działań zakłócających, zapewniając, że legalność nie odbywa się kosztem elastyczności.

Łącznie, środki te przekształcają usprawnienia proceduralne w transformację operacyjną, zamykając luki strukturalne, które uwidoczniły się w ostatnich polskich przypadkach, oraz podnosząc koszt prowadzenia kampanii hybrydowych jeszcze przed ich aktywacją.

6 Zakończenie

Dowody z różnych domen jasno pokazują, że Rosja i jej pełnomocnicy prowadzą wieloletnią strategię wojny poniżej progu, zaprojektowaną w celu korozji spójności, wykorzystywania szczelin i wyczerpywania odporności sojuszników. Dywersja lub sabotaż, szpiegostwo, dezinformacja i manipulacja prawna tworzą skoordynowaną ofensywę, która rozwija się dzięki zachodniej zwłoce. Rosja poszukuje parytetu poprzez odejmowanie, a nie modernizację, i dlatego będzie dalej eksportować entropię, dopóki demokracje nie wzmocnią odporności poznawczej i koordynacji. Zachód pozostaje natomiast związany krótkimi cyklami wyborczymi, zbyt często zmieniając priorytety lub nie utrzymując stałego, długofalowego działania i porozumienia ponad podziałami, podczas gdy Moskwa utrzymuje presję bez przerwy, gdyż cechuje ją ciągłość i niezmienność władzy i priorytetów. Istnieje też wyraźna dysproporcja między intensywnymi, dobrze finansowanymi wysiłkami Rosji i jej sprzymierzeńców, aby rozumieć i wpływać na Zachód, a ograniczonym, nadmiernie akademickim i powolnym podejściem Zachodu do badania współczesnej Rosji [158]. Ta asymetria definiuje pole walki.

Nie możemy porzucić rządów prawa, które stanowią fundament naszej legitymacji i siły. Jednak kurczowe trzymanie się komfortu prawnego i proceduralnego, podczas gdy przeciwnicy działają w cieniu, oznacza oddanie inicjatywy. Nie bez znaczenia w tej kwestii pozostaje presja praw obywatelskich i wolności słowa kardynalne dla postrzegania siły i wartości kultury Zachodu. NATO, UE i rządy narodowe dysponują już bezkonkurencyjnymi zasobami w zakresie wywiadu finansowego, uprawnień, zdolności cybernetycznych i zasięgu narracyjnego. Brakuje jedynie determinacji, aby zintegrować je w trwałą strategię, która traktuje zagrożenia hybrydowe jako kontinuum wojny, a nie pojedyncze incydenty.

Stawka nie może być wyższa. Albo Europa i jej sojusznicy podejmą zdecydowane działania, łącząc potencjał służb specjalnych, prawo i potencjał operacyjny w spójną obronę i ofensywę, albo Rosja będzie dalej erodować zaufanie i spójność od wewnątrz. Wojna już trwa. Wybór sprowadza się do pozostania w zamkniętym cyklu reaktywności albo do udowodnienia, że liberalna demokracja, zakorzeniona w rządach prawa, potrafi walczyć i zwyciężyć w starciu z autorytarną wojną hybrydową.

Recenzja 1 oraz komentarz: dr Anna Grabowska-Siwiec

Raport Macieja Filipa Bukowskiego przygotowany dla Fundacji Pułaskiego podejmuje problematykę współczesnych zagrożeń hybrydowych generowanych przez Federację Rosyjską i Republikę Białorusi. Dokument stanowi próbę kompleksowego ujęcia zjawisk mieszczących się w spektrum wojny hybrydowej, ze szczególnym uwzględnieniem implikacji dla bezpieczeństwa państw NATO i Unii Europejskiej.

Raport adresuje zagadnienia o fundamentalnym znaczeniu dla współczesnych studiów bezpieczeństwa międzynarodowego. Problematyka zagrożeń hybrydowych, szczególnie w kontekście rosyjsko-białoruskich operacji wpływu, stanowi jeden z kluczowych przedmiotów analiz w zakresie bezpieczeństwa narodowego państw zachodnich. Autor słusznie identyfikuje lukę poznawczą w obszarze systematycznej analizy zjawisk lokujących się poniżej progu otwartego konfliktu zbrojnego.

Szczególną wartość naukową przedstawia konceptualizacja „wyważonej postawy ofensywnej" jako odpowiedzi na działania hybrydowe. Propozycja ta wykracza poza tradycyjne, reaktywne podejście do zagrożeń bezpieczeństwa i postuluje proaktywną strategię przeciwdziałania, co stanowi istotny wkład w rozwój teorii bezpieczeństwa.

Raport wnosi znaczący wkład w dyskurs naukowy poprzez analizę transformacji, jakiej sztuczna inteligencja dokonała w obszarze operacji informacyjnych. Teza o przekształceniu działań dezinformacyjnych z „pracy rzemieślniczej w proces zautomatyzowany" stanowi trafną obserwację, która wymaga dalszego rozwoju w analizach i badaniach naukowych. Ta konstatacja ma istotne implikacje dla teorii i praktyki bezpieczeństwa informacyjnego, wskazując na konieczność redefinicji dotychczasowych podejść do przeciwdziałania dezinformacji.

Autor wprowadza wartościową koncepcję „sprzężeń zwrotnych", zgodnie z którą „incydent wywołuje kampanię informacyjną, oficjalna reakcja staje się widowiskiem medialnym, a zaufanie eroduje krok po kroku". Ten mechanizm przedstawia systematyczną analizę procesów, poprzez które pozornie izolowane wydarzenia przekształcają się w instrumenty degradacji społecznego zaufania i spójności instytucjonalnej.

Raport prezentuje istotną obserwację dotyczącą natury współczesnych zagrożeń hybrydowych. Autor słusznie identyfikuje, że skuteczność tych działań nie wynika ze skali pojedynczych ataków, lecz z ich powtarzalności i zdolności do „podtrzymywania atmosfery podejrzliwości, zmęczenia i przeciążenia percepcyjnego". Ta konstatacja stanowi znaczący wkład w teoretyczne rozumienie mechanizmów wojny hybrydowej.

Szczególnie wartościowa jest identyfikacja problemu braku integracji analitycznej między działaniami przestępczymi a operacjami wywiadowczymi państw obcych. Autor trafnie wskazuje, że opóźnienia w rozpoznawaniu tych połączeń „pozwalają przeciwnikowi utrzymać tempo działań", co stanowi istotną lukę w systemach bezpieczeństwa.

Dokument wnosi istotny wkład w zrozumienie wyzwań, przed jakimi stoją współczesne służby kontrwywiadowcze. Analiza ograniczeń strukturalnych i proceduralnych w obliczu ewoluujących zagrożeń hybrydowych stanowi wartościowy element dla praktyki bezpieczeństwa narodowego.

Raport formułuje ambitne, nie zawsze możliwe do realizacji, postulaty dotyczące „instytucjonalizacji kultury wymiany informacji wywiadowczych i kontrwywiadowczych". Propozycje te, mimo że dyskutowane w różnych formatach międzynarodowych, nie zostały dotychczas w pełni zaimplementowane, co wskazuje na ich praktyczną skuteczność.

Istotną wartością raportu jest jego potencjalny wkład w budowanie społecznej odporności na

działania hybrydowe. Poprzez systematyczną analizę mechanizmów i metod stosowanych przez służby wywiadowcze Rosji i Białorusi, dokument może przyczynić się do zwiększenia świadomości społecznej odnośnie charakteru i skali współczesnych zagrożeń.

Dokument wypełnia istotną lukę w polskim dyskursie naukowym dotyczącym bezpieczeństwa, oferując systematyczną analizę zjawisk dotychczas fragmentarycznie opisywanych w literaturze. Szczególnie cenny jest interdyscyplinarny charakter analizy, łączący perspektywę studiów bezpieczeństwa, psychologii społecznej, nauk o komunikacji oraz informatyki. Takie podejście pozwala na holistyczne ujęcie problematyki wojny hybrydowej jako zjawiska wielowymiarowego, wymagającego kompleksowych odpowiedzi na poziomie narodowym i międzynarodowym.

Komentarz dr Anny Grabowskiej-Siwiec do Raportu Agenci Chaosu: ukryta kampania przeciwko Zachodowi

Wojna kognitywna i ofensywne operacje rosyjskich oraz białoruskich służb specjalnych (Agenci chaosu: ukryta kampania przeciwko Zachodowi")

Współczesne zagrożenia wywiadowcze charakteryzują się znaczącym przesunięciem pola działania z domeny tradycyjnie pojmowanej tajności ku sferze społecznie dostępnej i percepcyjnie widocznej. Ta transformacja nie stanowi przypadkowej ewolucji, lecz świadomą strategię operacyjną, której celem jest maksymalizacja efektu psychologicznego przy jednoczesnym zachowaniu wiarygodnej zaprzeczalności na poziomie państwowym. Terytorium Ukrainy zostało wykorzystane jako przestrzeń testowa dla zinstytucjonalizowanych działań hybrydowych. Mechanizmy wypracowane w procesie destabilizacji Ukrainy zostały następnie zaadaptowane i skierowane przeciwko państwom Zachodu, po ich jednoznacznym sprzeciwie wobec rosyjskiej agresji. Ta progresja wskazuje na systematyczny charakter rozwoju doktryny hybrydowej.

Wykorzystanie działań jawnych lub słabo zakamuflowanych nie stanowi deficytu operacyjnego służb wywiadowczych, lecz celową metodę budowania określonych efektów psychospołecznych. Strategia ta ma na celu generowanie: chaosu percepcyjnego – zakłócenie zdolności społeczeństwa do racjonalnej oceny zagrożeń; klimatu strachu – systematyczne podwyższanie poziomu lęku społecznego oraz poczucia osaczenia poprzez kreowanie wrażenia wszechobecności zagrożenia ze strony rosyjskich i białoruskich służb wywiadowczych, a także erozji zaufania instytucjonalnego poprzez systematyczne podważanie wiarygodności struktur państwowych.

Długofalowa intencjonalność opisywanych działań koncentruje się na: osłabieniu spójności społecznej, dyskredytacji wartości demokratycznych – podważeniu legitymacji systemów demokratycznych oraz docelowo na zmianie konfiguracji politycznej – doprowadzeniu do władzy ugrupowań przyjaznych polityce rosyjskiej. Ta sekwencja celów wskazuje na systemowy charakter operacji hybrydowych generowanych przez Rosję, wykraczający poza doraźne korzyści taktyczne.

Mając na uwadze, że agresję wywiadowczą rozpoznają oraz neutralizują służby kontrwywiadowcze, kluczowe postulaty modernizacyjne powinny koncentrować się na tym segmencie aparatu bezpieczeństwa państwa. Wymaga to: wzmocnienia zasobowego służb kontrwywiadowczych, solidnego umocowania prawnego ich uprawnień operacyjnych, a także integracji z niezależnymi ośrodkami analitycznymi w celu zwiększenia potencjału eksperckiego. Niezbędne jest także rozróżnienie działań wywiadu od działań kontrwywiadu. Definicyjne mylenie kompetencji i narzędzi obu typów służb specjalnych powoduje zarówno chaos informacyjny jak i negatywny wizerunek służb wewnętrznych, co jednoznacznie szkodzi ich skuteczności. Służby kontrwywiadowcze są umieszczone w porządku prawnym państwa, gdyż działają na jego terytorium. Ich kompetencje oraz narzędzia operacyjne muszą być oparte na prawie i dawać społeczeństwu poczucie skuteczności i ważności kontrwywiadu dla bezpieczeństwa społecznego.

Transgraniczny charakter działań hybrydowych i dezinformacyjnych implikuje również konieczność rozwoju mechanizmów współpracy międzynarodowej. Jednakże efektywność współpracy służb specjalnych napotyka na istotne ograniczenia systemowe w postaci operowania danymi objętymi najwyższymi klauzulami tajności, ograniczonego zaufanie nawet wobec partnerów sojuszniczych oraz zagrożenia ujawnienia metod pracy operacyjnej i źródeł

operacyjnych. Postulując jakiekolwiek zmiany w tym zakresie należy powyższe ograniczenia brać pod uwagę.

W wielu państwach, w tym w Polsce, służby specjalne podlegają fluktuacjom i naciskom politycznym, co przekształca je w instrumenty wzmacniania aktualnie sprawujących władzę ugrupowań. Ta instrumentalizacja osłabia ich zdolności operacyjne i wiarygodność międzynarodową. Do słabości struktur służb specjalnych należą: niedofinansowanie (nieadekwatność budżetów do skali wyzwań), brak wykwalifikowanych kadr, ograniczona współpraca z sektorem prywatnym i akademickim, brak dostępu do najnowszych rozwiązań technicznych. Te słabości systemowe ograniczają zdolność skutecznego reagowania na skomplikowane zagrożenia, szczególnie w cyberprzestrzeni. Aby efektywnie zwalczać zagrożenia hybrydowe należy rozpocząć od naprawienia tych wewnętrznych problemów służb specjalnych.

Istotnym elementem efektywności działań kontrwywiadowczych jest rozwój kanałów komunikacji między służbami a społeczeństwem. Bez wsparcia społecznego służby nie są w stanie skutecznie realizować swoich funkcji ochronnych.

Dyskurs dotyczący wzmocnienia kompetencji służb specjalnych nieuchronnie wiąże się z potencjalnym ograniczeniem praw i swobód obywatelskich. Niezwykle trudno o uzyskanie optymalnego punktu równowagi między: skutecznością ochrony przed działaniami wrogich wywiadów a zachowaniem fundamentalnych wolności charakterystycznych dla społeczeństw demokratycznych. Dlatego też społeczeństwa demokratyczne stają przed paradoksem konieczności ograniczenia własnych swobód w celu ochrony przed zagrożeniami zewnętrznymi, które te właśnie swobody wykorzystują wrogie wywiady jako wektor ataku.

Obecnie mamy do czynienia z fundamentalną transformację charakteru zagrożeń wywiadowczych, wymagającą odpowiedniej adaptacji systemów obronnych państw demokratycznych. Kluczowe wyzwanie stanowi wypracowanie efektywnych mechanizmów odpowiedzi, które nie naruszą fundamentalnych wartości demokratycznych, jednocześnie zapewniając skuteczną ochronę przed działaniami hybrydowymi.

Recenzja 2: Grzegorz Małecki

Raport obrazowo i sugestywnie prezentuje dynamicznie narastające w ostatnich latach zjawisko szeroko pojętych agresywnych operacji w ramach tzw. wojny hybrydowej prowadzonych przez rosyjskie i białoruskie służby wywiadowcze na terytorium Polski oraz innych krajów Unii Europejskiej i NATO. Zawiera wyczerpujący opis ich celów i założeń metodologicznych oraz drobiazgowy katalog mechanizmów i instrumentarium stosowanych przez służby wywiadowcze Rosji i Białorusi w ich niewypowiedzianej wojnie przeciwko Zachodowi. Ten sugestywny opis pozwala odbiorcy zrozumieć źródła i istotę zjawisk jakich jesteśmy w ostatnich latach świadkami, których celem jest destrukcja poczucia bezpieczeństwa zachodnich społeczeństw oraz wywołanie wewnętrznych konfliktów, obniżających ich zdolność do obrony przez zewnętrznymi zagrożeniami.

Istotną wartością dodaną raportu jest umiejętne połączenie syntetycznego opisu teoretycznego z bogatą paletą najbardziej aktualnych, sugestywnych przykładów opisywanych operacji na terytorium całej Europy (nie tylko Polski), z których wiele jest w Polsce zupełnie nieznanych. Wyłaniający się z tego zestawienia obraz ukazuje niepokojącą skalę zagrożeń o charakterze egzystencjalnym dla bezpieczeństwa Polski i Europy, których społeczeństwa nie uświadamiają sobie na co dzień, pozbawione całościowego obrazu zjawiska zobrazowanego w raporcie. Dopiero ujęcie pojedynczych zdarzeń będących efektem działania wrogich służb wywiadowczych w całościowy układ oraz wpisanie ich kontekst operacji hybrydowych unaocznia ich destrukcyjny potencjał i pozwala zrozumieć skalę niebezpieczeństwa z jakim przyszło się nam mierzyć.

Ten niepokojący obraz w oczywisty sposób rodzi naturalne pytania o zdolność aparatu państwa oraz wspólnoty euro-atlantyckiej do neutralizacji tych zagrożeń i obrony przed nimi. Raport z zimną precyzją ukazuje smutną rzeczywistość, że Polska oraz UE i NATO są ewidentnie w defensywie na tym polu a Rosja i Białoruś dynamicznie rozwijają swoją ofensywę bez adekwatnej reakcji, o charakterze w przeważającej mierze pasywnej, skoncentrowanej na minimalizacji skutków i ściganiu fizycznych wykonawców ataków sabotażowo – dywersyjnych, zamiast wyprzedzającym neutralizowaniu tych działań oraz ich inspiratorów i struktur kierowniczych. Raport celnie punktuje zaniedbania, błędy i deficyty systemowe krajów Zachodu, w tym Polski, na polu zwalczania hybrydowej agresji Rosji i Białorusi, kładąc szczególny nacisk na anachronizm i przywiązanie do utartych schematów działań z odległej przeszłości, jakie cechują większość europejskich wywiadowczych.

Największą wartością raportu są jednak niezwykle trafne rekomendacje wskazujące na konkretne przedsięwzięcia, których podjęcie pozwoli Zachodowi skutecznie odeprzeć ataki ze strony Rosji i Białorusi i przejść do ofensywy w wojnie hybrydowej. Zgadzając się w pełni z zawartymi w nich propozycjami, kładę szczególny nacisk na postulat podjęcia aktywnych operacji o charakterze kontrofensywy, które pozwolą przenieść pole operacyjne na terytorium przeciwnika. Bez podjęcia agresywnych operacji ofensywnych przez działające wspólnie europejskie służby wywiadowcze nie ma szans na skuteczną neutralizację jego służb wywiadowczych .

Endnotes

[1] Wither, J. (2020). Outsourcing warfare: Proxy forces in contemporary armed conflicts. *Security and Defence Quarterly*, *31*(4), 17–34. https://doi.org/10.35467/sdq/127928

[2] Kozera, C., Bernat, P., Gürer, C., Popławski, B., & Sözer, M. (2020). Game of Proxies – Towards a new model of warfare: Experiences from the CAR, Libya, Mali, Syria, and Ukraine. *Security and Defence Quarterly*, *31*(4), 77–97. https://doi.org/10.35467/sdq/131787

[3] Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

[4] Bilal, A. (2021, November 30). Hybrid Warfare – New Threats, Complexity, and "Trust" as the Antidote. *NATO Review*. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

[5] Cordesman, A. H. (2016, May 4). *The future of hybrid warfare*. Center for Strategic and International Studies (CSIS). http://csis.org/analysis/future-hybrid-warfare

[6] Horn , C. B. (2016). On hybrid warfare. Publications.gc.ca; Royal Canadian Air Force Centre for Operational Research and Analysis. https://publications.gc.ca/collections/collection_2017/mdn-dnd/D4-10-19-2016-eng.pdf

[7] Connable, B., Young, S., Pezard, S., Radin, A., Cohen, R., Migacheva, K., & Sladden, J. (2020). Russia's Hostile Measures Combating Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2500/RR2539/RAND_RR2539.pdf

[8] Canada's Security Intelligence Service. (2025). The Military Aspects of Russian Grey Zone Activities. Canada.ca; Government of Canada. https://www.canada.ca/en/security-intelligence-service/corporate/publications/hybrid-methods-in-the-grey-zone/military-aspects-russian-grey-zone-activities.html

[9] Mumford, A., & Carlucci, P. (2022). Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security, 8(2), 1–15. https://doi.org/10.1017/eis.2022.19

[10] Messner, E. (2004). Forma przyszłych wojen. Bellona.

[11] Klutz, A. (2016). Myatezh Voina: The Russian Grandfather of Western Hybrid Warfare. Small Wars Journal. https://archive.smallwarsjournal.com/jrnl/art/myatezh-voina-the-russian-grandfather-of-western-hybrid-warfare

[12] Messner, E. (2007). Mutiny War as a New Form of Armed Struggle. In Rácz, A. (2015). Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist. Finnish Institute of International Affairs. https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf

[13] Rácz, A. (2015). Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist (pp. 1–104). The Finnish Institute of International Affairs. https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf

[14] Panarin, I. (2003). Information Warfare and Geopolitics. Cited in Darczewska, J. (2014). The Anatomy of Russian Information Warfare. OSW Studies. https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

[15] Tsygankov, A. (2015). Vladimir Putin's last stand: the sources of Russia's Ukraine policy. Post-Soviet Affairs, 31(4), 279–303. https://doi.org/10.1080/1060586x.2015.1005903

[16] Pomerantsev, P. (2019). *This Is Not Propaganda*. Faber & Faber.

[17] Pavlovsky, G. (2014). Putin's World Outlook [Interview]. In *New Left Review*.; Wilson, A. (2005). *Virtual Politics: Faking Democracy in the Post-Soviet World*. Yale University Press.

[18] Pomerantsev, P. (2014). *Nothing is true and everything is possible: the surreal heart of the new Russia*. PublicAffairs.

[19] Pavlovsky, G. [Interview]. (2012). *The Reality We Create.* In Walker, S. (2016). *The Long Hangover*. Oxford University Press. https://www.penguinrandomhouse.com/books/553053/the-long-hangover-by-shawn-walker/

[20] Surkov, V. (2019). *The Loneliness of the Half-Breed*. Russia in Global Affairs. https://eng.globalaffairs.ru/articles/the-loneliness-of-the-half-breed/

[21] Snyder, T. (2018). *The Road to Unfreedom*. Tim Duggan Books.

[22] Dugin, A. (2012). *The Fourth Political Theory*. Arktos.

[23] Dugin, A. (1997) *Osnovy geopolitiki (Foundations of Geopolitics)*. Arktogeja.

[24] Laruelle, M. (2015). *Eurasianism and the Ideology of Russian Empire*. Woodrow Wilson Center.

[25] Fridman, O. (2018). *Russian Hybrid Warfare: Resurgence and Politicization.* Oxford University Press.

[26] Bartles, C. K. (2016). Getting Gerasimov Right. *Military Review*, *96*(1), 30–38. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf

[27] Reuters Staff. (2017, November 7). Estonia arrests suspected Russian FSB agent. *Reuters*. https://www.reuters.com/article/world/estonia-arrests-suspected-russian-fsb-agent-idUSKBN1D71HZ/

[28] UK Government. (2018, September 5). *PM statement on the Salisbury investigation: 5 September 2018*. GOV.UK. https://www.gov.uk/government/speeches/pm-statement-on-the-salisbury-investigation-5-september-2018

[29] UK Government. (2018, February 15). *Foreign Office Minister condemns Russia for NotPetya attacks*. GOV.UK. https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

[30] National Cyber Security Centre. (2021, April 15). *UK and US Call out Russia for SolarWinds Compromise*. Www.ncsc.gov.uk. https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise

[31] Popescu, N., Secrieru, S., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., Limnell, J., Pawlak, P., Pernik, P., Reinhold, T., Reshetnikov, A., Soldatov, A., & Vilmer, J.-B. (2018). *Hacks, leaks and disruptions Russian cyber strategies EDITED BY Chaillot Papers*. European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

[32] U.S. Department of Justice. (2022, January 20). *Belarusian Government Officials Charged with Aircraft Piracy for Diverting Ryanair Flight 4978 to Arrest Dissident Journalist in May 2021*. Justice.gov. https://www.justice.gov/archives/opa/pr/belarusian-government-officials-charged-aircraft-piracy-diverting-ryanair-flight-4978-arrest

[33] Gerdžiūnas, B., & Valkauskas, T. (2024, August 15). *Belarusian exiles in Vilnius fight off KGB infiltration, recruitment attempts*. Lrt.lt. https://www.lrt.lt/en/news-in-english/19/2337733/belarusian-exiles-in-vilnius-fight-off-kgb-infiltration-recruitment-attempts.

[34] Nimmo, B., François, C., Eib, C. S., Ronzaud, L., Ferreira, R., Hernon, C., & Kostelancik, T. (2020). *Secondary Infektion*. Graphika. https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

[35] Praks, H. (2024, May 30). *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage – Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats*. Hybrid CoE – the European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage/

[36] Estonian Internal Security Service. (2025). *Annual Review 2024-2025*. KAPO. https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf
[37] Thomas, T. (2004). Russia's Reflexive Control Theory and the Military. *The Journal of Slavic Military Studies*, *17*(2), 237–256. https://doi.org/10.1080/13518040490450529
[38] Dąbrowska, I. (2021). Maskowanie operacyjne (maskirowka) jako rosyjska zdolność zaskakiwania przeciwnika. *Przegląd Bezpieczeństwa Wewnętrznego*, *25*(13), 293–321. https://ejournals.eu/czasopismo/przeglad-bezpieczenstwa-wewnetrznego/artykul/maskowanie-operacyjne-maskirowka-jako-rosyjska-zdolnosc-zaskakiwania-przeciwnika
[39] Fridman, O. (2018). *Russian "Hybrid Warfare."* Oxford University Press. https://doi.org/10.1093/oso/9780190877378.001.0001
[40] Institute for Strategic Dialogue. (2025, May 20). *Investigation: Russia-aligned campaigns amplify negative sentiment towards Ukrainians in Poland ahead of a decisive presidential vote*. ISD. https://www.isdglobal.org/digital_dispatches/russia-aligned-campaigns-amplify-negative-sentiment-towards-ukrainians-in-poland-ahead-of-a-decisive-presidential-vote
[41] Lucas, E. (2019). *The Spycraft Revolution*. Foreign Policy. https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/
[42] Riehle, K. P. (2023). Soviet and Russian Diplomatic Expulsions: How Many and Why? *International Journal of Intelligence and Counterintelligence*, *37*(4), 1–26. https://doi.org/10.1080/08850607.2023.2272216
[43] Reuters Staff. (2025, August 13). Poland charges group with sabotage on behalf of foreign intelligence. *Reuters*. https://www.reuters.com/world/poland-charges-group-with-sabotage-behalf-foreign-intelligence-2025-08-13/
[44] Burrows, E. (2025, July 8). *UK court convicts 3 men over arson attack authorities say was organized by Russian intelligence*. AP News. https://apnews.com/article/russia-ukraine-london-arson-warehouse-intelligence-a00f7429e0688731ff1718d2c3bb855f
[45] Gera, V. (2025, May 11). *Poland blames Russian intelligence for Warsaw shopping center arson attack*. AP News. https://apnews.com/article/poland-russia-420187f5755036f6f61c65122c11348f
[46] Radin, A., Demus, A., & Marcinek, K. (2020). *Understanding Russian Subversion: Patterns, Threats, and Responses* (pp. 1–32). RAND Corporation. https://www.rand.org/pubs/perspectives/PE331.html
[47] Reynolds, S. (2025, August 14). *The scale of Russian operations against Europe's critical infrastructure*. International Institute for Strategic Studies. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/
[48] Øvrebø, E. F. (2024, June 13). *Brann ved Lierâstunnelen: – Mye innstillinger og forsinkelser*. VG. https://www.vg.no/nyheter/i/EywVrl/brann-ved-lieraasen-tunnel-togstrekning-mellom-asker-og-drammen-stengt
[49] Langvik, S. (2024, June 19). *Ingen pågrepet etter bilbranner i Oslo*. VG. https://www.vg.no/nyheter/i/4B7LAQ/bilbrann-paa-haugerud-i-oslo
[50] Jegoroff, M. (2024, June 30). *Yhtäkkiä alkoi hämärien vesihuolto-kohteiden murtosarja – tämä tapauksista tiedetään*. Ilta-Sanomat. https://www.is.fi/kotimaa/art-2000010531133.html
[51] IS. (2024, June 30). *Pääkirjoitus: Onko Putinin Venäjä siirtynyt Suomen häirinnässä jo vakavammalle tasolle? Salamurhat ja sabotaasit eivät välttämättä ole enää pelkkää mielikuvitusta*. Ilta-Sanomat. https://www.is.fi/paakirjoitus/art-2000010532602.html
[52] Kusma, E. (2024, June 3). *Kose vallas põles viilhall, päästjad reageerisid suurte jõududega*. Ohtuleht.ee. https://www.ohtuleht.ee/1108159/fotod-kose-vallas-poles-viilhall-paastjad-reageerisid-suurte-joududega?utm_source=ground.news&utm_medium=referral
[53] Moulson, G. (2025, May 14). *Germany and Switzerland arrest 3 over suspected plans to send explosive parcels to Ukraine*. Apnews.com. https://apnews.com/article/germany-ukraine-russia-packages-arson-explosives-arrests-c032a532ffc94585d70501ff6a4d4bda
[54] LETA. (2024, June 29). *Bolderājā notikušais ugunsgrēks izcēlies bīstamo atkritumu apsaimniekotāja teritorijā*. Tv3.Lv. https://tv3.lv/degpunkta/ugunsdrosiba/vides-piesarnojuma-izplatisanas-ugunsgreka-bolderaja-ir-ierobezota/
[55] Matonis, J. (2024, June 24). *Pranešama apie gaisrą Kauno aviacijos gamykloje*. Delfi. https://www.delfi.lt/news/daily/crime/pranesama-apie-gaisra-kauno-aviacijos-gamykloje-120031866
[56] Sychev, A., & Ratz, A. (2024, April 18). *Germany arrests two for alleged military sabotage plot on behalf of Russia*. Reuters. https://www.reuters.com/world/europe/germany-arrests-two-alleged-military-sabotage-plot-behalf-russia-2024-04-18/
[57] Moulson, G. (2025, May 14). *Germany and Switzerland arrest 3 over suspected plans to send explosive parcels to Ukraine*. Apnews.com. https://apnews.com/article/germany-ukraine-russia-packages-arson-explosives-arrests-c032a532ffc94585d70501ff6a4d4bda
[58] Koper, A., Strzelecki, M., Lebedev, F., & Sytas, A. (2025, April 10). *Insight: Sex toys and exploding cosmetics: anatomy of a "hybrid war" on the West.* Reuters. https://www.reuters.com/world/europe/sex-toys-exploding-cosmetics-anatomy-hybrid-war-west-2025-04-05/
[59] Kang-Stryker, A., & Bugajski, J. (2025). Poland on the Frontlines Against Russia's Shadow War. *Eurasia Daily Monitor*, *22*(66). https://jamestown.org/program/poland-on-the-frontlines-against-russias-shadow-war
[60] Todur, W. (2024, June 28). *Pożar w Sławkowie nie był przypadkowy? "Trzeba brać pod uwagę ten fatalny rosyjski ślad."* Wyborcza.pl Sosnowiec. https://sosnowiec.wyborcza.pl/sosnowiec/7,93867,31101652,pozar-w-slawkowie-nie-byl-przypadkowy-trzeba-brac-pod-uwage.html
[61] Kozioł, M. (2024, June 28). *Samoloty gaśnicze i strażacy walczą z ogniem na poligonie w Żaganiu. Pożar pojawił się podczas ćwiczeń*. Wyborcza.pl Zielona Góra. https://zielonagora.wyborcza.pl/zielonagora/7,35182,31101980,samoloty-gasnicze-i-strazacy-walcza-z-ogniem-na-poligonie-w.html
[62] Gruszczyński, A. (2024, June 27). *Wielki pożar pod Działdowem. Stu strażaków walczy z ogniem*. Wyborcza.pl Olsztyn. https://olsztyn.wyborcza.pl/olsztyn/7,48726,31096605,wielki-pozar-pod-dzialdowem-100-strazakow-walczy-z-ogniem.html
[63] Danielewicz, M. (2024, June 26). *Ogromny pożar zabytkowego pałacu w Jelczu-Laskowicach. Dym było widać z odległości kilku kilometrów*. Wyborcza.pl Wrocław. https://wroclaw.wyborcza.pl/wroclaw/7,35771,31094238,strazacy-walcza-z-pozarem-neogotyckiego-palacu-w-jelczu-laskowicach.html
[64] MG. (2024, June 24). *Pożar magazynu ze zbożem. Podano przypuszczalną przyczynę*. Tvn24.Pl; TVN Warszawa. https://tvn24.pl/tvnwarszawa/najnowsze/gozdowo-sierpc-pozar-magazynu-ze-zbozem-st7977366
[65] Matusiak, T. (2024, June 24). *Pożar magazynu na zboże. Chmura ciemnego dymu w okolicach Sierpca i Płocka*. Wyborcza.pl Płock. https://plock.wyborcza.pl/plock/7,35681,31088324,pozar-magazynu-na-zboze-chmura-ciemnego-dymu-w-okolicach-sierpca.html
[66] Kijek, K., & Zieliński, R. (2024, June 17). *Ogromny pożar zabytkowego pałacu Stolbergów we Wrocławiu. Strażacy przez całą noc walczyli z ogniem*. Wyborcza.pl Wrocław. https://wroclaw.wyborcza.pl/wroclaw/7,35771,31065769,pozar-zabytkowego-palacu-stolbergow-we-wroclawiu-strazacy-przez.html
[67] Informacja prasowa. (2025, August 6). *Sabotaż światłowodów w Warszawie – szybka reakcja Intelligent Technologies*. Elektrotechnik Automatyk. https://elektrotechnikautomatyk.pl/artykuly/sabotaz-swiatlowodow-w-warszawie-szybka-reakcja-intelligent-technologies
[68] Walker, S. (2025, May 4). *"These people are disposable": how Russia is using online recruits for a campaign of sabotage in Europe*. The Guardian. https://www.theguardian.com/world/ng-interactive/2025/may/04/these-people-are-disposable-how-russia-is-using-online-recruits-for-a-campaign-of-sabotage-in-europe
[69] Saito, M., Koper, A., Zverev, A., Lebedev, F., & Nikolskaya, P. (2025, June 12). *Russia recruited a teenage spy. His arrest led to a crypto money trail.* Reuters. https://www.reuters.com/investigates/special-report/europe-espionage-teen-spy/
[70] Jochecová, K. (2025, July 10). *Russia hires migrants to wreak havoc, Czech intel report says*. POLITICO. https://www.politico.eu/article/russia-hiring-migrants-fear-weaken-trust-state-czech-republic-secret-service-telegram-arson-military/
[71] Warrell, H., & Mosolova, D. (2025, May 12). *Bulgarian who led Russia-backed spy ring in the UK jailed for 10 years*. Financial Times. https://www.ft.com/content/65c17f2f-64ad-42f3-b035-fef3f22c6bda

[72] Burrows, E. (2025, July 9). *European intelligence officials warn that a Russian sabotage campaign is escalating*. AP News. https://apnews.com/article/russia-sabotage-europe-ukraine-13ee37cf869139839f0d4a3ebe7bd80d

[73] Strategic Communications. (2024). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*. EEAS. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

[74] Institute for Strategic Dialogue. (2025, May 20). *Investigation: Russia-aligned campaigns amplify negative sentiment towards Ukrainians in Poland ahead of a decisive presidential vote*. ISD. https://www.isdglobal.org/digital_dispatches/russia-aligned-campaigns-amplify-negative-sentiment-towards-ukrainians-in-poland-ahead-of-a-decisive-presidential-vote

[75] Atanasova, A., Poldi, F., & Kuster, G. (2025). *Operation Overload: More Platforms, New Techniques, Powered by AI*. (pp. 1–138). Check First. https://checkfirst.network/wp-content/uploads/2025/06/Overload%C2%A02_%20Main%20Draft%20Report_compressed.pdf

[76] VIGINUM. (2024). *Summary of the Information Threat to the Paris 2024 Olympic and Paralympic Games Public report*. General Secretariat for Defence and National Security. https://www.sgdsn.gouv.fr/files/files/Publications/20240919_NP_SGDSN_VIGINUM_Summary%20information%20threat%20Paris2024Games_EN_0.pdf

[77] Hinnant, L. (2024, July 4). *Russian-linked cybercampaigns put a bull's-eye on France. Their focus? The Olympics and elections*. AP News. https://apnews.com/article/france-election-disinformation-russia-olympics-be18d688677240686df200096018f221

[78] Reynaud , F., & Ricard, P. (2024, February 12). France uncovers vast network of Russian disinformation sites. *Le Monde*. https://www.lemonde.fr/en/pixels/article/2024/02/12/france-uncovers-vast-network-of-russian-disinformation-sites_6518362_13.html

[79] VIGINUM. (2025). *Challenges and opportunities of artificial intelligence in the fight against information manipulation* (pp. 1–28). General Secretariat for Defence and National Security. https://www.sgdsn.gouv.fr/files/files/Publications/20250207_NP_SGDSN_VIGINUM_Rapport%20menace%20informationnelle%20IA_EN_0.pdf

[80] Foreign, Commonwealth & Development Office. (2024, October 28). *UK sanctions Putin's interference actors*. GOV.UK. https://www.gov.uk/government/news/uk-sanctions-putins-interference-actors

[81] Reuters Staff. (2024, October 28). UK sanctions Russian "disinformation agencies." *Reuters*. https://www.reuters.com/world/uk/uk-sanctions-russian-disinformation-agencies-2024-10-28/

[82] Gilbert, D. (2025, July 1). *A Pro-Russia Disinformation Campaign Is Using Free AI Tools to Fuel a "Content Explosion."* WIRED. https://www.wired.com/story/pro-russia-disinformation-campaign-free-ai-tools/

[83] Bergmanis-Korāts, G., Isupova, M., & Vecmanis, R. R. (2025). *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty*. Stratcomcoe.org; StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia. https://stratcomcoe.org/publications/virtual-manipulation-brief-2025-from-war-and-fear-to-confusion-and-uncertainty/320

[84] U. S. Department of Justice. (2024, July 9). *Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm*. Justice.gov. https://www.justice.gov/archives/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners

[85] U. S. Department of Justice. (2024, September 4). *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere*. Justice.gov. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

[86] Federal Bureau of Investigation, Cyber National Mission Force, Netherlands Military Intelligence and Security Service, Netherlands General Intelligence and Security Service, Netherlands National Police, & Canadian Centre for Cyber Security. (2024). *State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity* (pp. 1–14). Cisa.gov. https://www.ic3.gov/CSA/2024/240709.pdf

[87] Gilbert, D. (2025, July 1). *A Pro-Russia Disinformation Campaign Is Using Free AI Tools to Fuel a "Content Explosion."* WIRED. https://www.wired.com/story/pro-russia-disinformation-campaign-free-ai-tools/

[88] Bergmanis-Korāts, G., Isupova, M., & Vecmanis, R. R. (2025). *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty*. Stratcomcoe.org; StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia. https://stratcomcoe.org/publications/virtual-manipulation-brief-2025-from-war-and-fear-to-confusion-and-uncertainty/320

[89] Stockwell, S. (2024). *AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections*. Centre for Emerging Technology and Security; The Alan Turing Institute. https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-threat-analysis-2024-uk-and-european-elections

[90] General Intelligence and Security Service of the Netherlands, & National Coordinator for Counterterrorism and Security. (2024). *Crossing borders: State-sponsored interference in diaspora communities in the Netherlands* (pp. 20–21). AIVD and NCTV. https://english.aivd.nl/binaries/aivd-en/documenten/publications/2025/03/25/phenomenon-analysis-crossing-borders/Crossing-Borders-AIVD-NCTV.pdf

[91] Lozovsky, I., & Laine, M. (2025, May 21). *Russian Foundation, Aimed at Helping "Compatriots" Abroad, Supports Spies, Criminals, and Propagandists*. OCCRP. https://www.occrp.org/en/project/dear-compatriots/russian-foundation-aimed-at-helping-compatriots-abroad-supports-spies-criminals-and-propagandists

[92] Jochecová, K. (2025, July 10). *Russia hires migrants to wreak havoc, Czech intel report says*. POLITICO. https://www.politico.eu/article/russia-hiring-migrants-fear-weaken-trust-state-czech-republic-secret-service-telegram-arson-military/

[93] Agencja Bezpieczeństwa Wewnętrznego. (2024, October 25). *Komunikat dotyczący działalności dywersyjnej FR*. Abw.gov.pl. https://www.abw.gov.pl/pl/informacje/2569,Komunikat-dotyczacy-dzialalnosci-dywersyjnej-FR.html

[94] Lelonek, A. (2025, April 9). *Russia's recruitment of immigrants to carry out spying and sabotage is a new threat to Poland*. Notes from Poland. https://notesfrompoland.com/2025/04/09/russias-recruitment-of-immigrants-to-carry-out-spying-and-sabotage-is-a-new-threat-to-poland/

[95] EUROPOL. (2025). *European Union Serious and Organised Crime Threat Assessment" The Changing DNA of Serious and Organised Crime*. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

[96] Reuters Staff. (2025, May 12). Russian spy ring leader jailed in UK for nearly 11 years. *Reuters*. https://www.reuters.com/world/europe/russian-spy-ring-leader-jailed-uk-nearly-11-years-2025-05-12/

[97] Holden, M., & Tobin, S. (2025, March 7). Bulgarians convicted in UK of being Russian spies working for Wirecard fugitive. *Reuters*. https://www.reuters.com/world/europe/three-bulgarians-convicted-spying-russia-after-uk-trial-2025-03-07/

[98] Burrows, E. (2025, July 8). *UK court convicts 3 men over arson attack authorities say was organized by Russian intelligence*. AP News. https://apnews.com/article/russia-ukraine-london-arson-warehouse-intelligence-a00f7429e0688731ff1718d2c3bb855f

[99] State Security Department of the Republic of Lithuania, & Defence Intelligence and Security Service under the Ministry of National Defence. (2025). *2025 National Threat Assessment*. Ministry of National Defence. https://kam.lt/wp-content/uploads/2025/03/2025-GR-ENG-02-21-El-be-uzraso_.pdf

[100] European Parliament. (2025, April 3). *European Parliament resolution of 3 April 2025 on the immediate risk of further repression by Lukashenka's regime in Belarus – threats from the Investigative Committee (2025/2629(RSP))*. Www.europarl.europa.eu. https://www.europarl.europa.eu/doceo/document/TA-10-2025-0063_EN.html

[101] European Parliament. (2025, April 3). *Resolution of 3 April 2025 on the immediate risk of further repression by Lukashenka's regime in Belarus – threats from the Investigative Committee* (P10_TA(2025)0063). European Parliament. http://www.europarl.europa.eu/doceo/document/TA-10-2025-0063_EN.html

[102] Walker, S. (2025, May 4). *"These people are disposable": how Russia is using online recruits for a campaign of sabotage in Europe*. The Guardian. https://www.theguardian.com/world/ng-interactive/2025/may/04/these-people-are-disposable-how-russia-is-using-online-recruits-for-a-campaign-of-sabotage-in-europe

[103] EUROPOL. (2025). *European Union Serious and Organised Crime Threat Assessment" The Changing DNA of Serious and Organised Crime*. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

[104] Central Intelligence Agency. (1987). *Soviet active measures in the United States*. U. S. Department of State. https://www.cia.gov/readingroom/docs/CIA-RDP11M01338R000400470089-2.pdf

[105] Sychev, A., & Ratz, A. (2024, April 18). *Germany arrests two for alleged military sabotage plot on behalf of Russia*. Reuters. https://www.reuters.com/world/europe/germany-arrests-two-alleged-military-sabotage-plot-behalf-russia-2024-04-18/

[106] Reuters Staff. (2025, May 12). Russian spy ring leader jailed in UK for nearly 11 years. *Reuters*. https://www.reuters.com/world/europe/russian-spy-ring-leader-jailed-uk-nearly-11-years-2025-05-12/

[107] Counter Terrorism Policing. (2025, July 11). *Group convicted after Russian-ordered arson attack in London*. Counter Terrorism Policing. https://www.counterterrorism.police.uk/group-convicted-after-russian-ordered-arson-attack-in-london/

[108] Walker, S. (2025, May 4). *"These people are disposable": how Russia is using online recruits for a campaign of sabotage in Europe*. The Guardian. https://www.theguardian.com/world/ng-interactive/2025/may/04/these-people-are-disposable-how-russia-is-using-online-recruits-for-a-campaign-of-sabotage-in-europe

[109] Strategic Communications. (2024). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*. EEAS. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

[110] Burdette, Z., Phillips, D., Heim, J. L., Geist, E., Frelinger, D. R., Heitzenrater, C., & Mueller, K. P. (2025, July 3). *An AI Revolution in Military Affairs? How Artificial Intelligence Could Reshape Future Warfare*. Rand.org; RAND Corporation. https://www.rand.org/pubs/working_papers/WRA4004-1.html

[111] Osadchuk, R. (2024, July 9). *AI tools usage for disinformation in the war in Ukraine*. DFRLab. https://dfrlab.org/2024/07/09/ai-tools-usage-for-disinformation-in-the-war-in-ukraine/

[112] Bergmanis-Korāts, G., Isupova, M., & Vecmanis, R. R. (2025). *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty*. Stratcomcoe.org; StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia. https://stratcomcoe.org/publications/virtual-manipulation-brief-2025-from-war-and-fear-to-confusion-and-uncertainty/320

[113] Wallner, C., Copeland, S., & Giustozzi, A. (2025). *Emerging Insights Russia, AI and the Future of Disinformation Warfare*. Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/russia-ai-and-the-future-of-disinformation-warfare.pdf

[114] Gilbert, D. (2025, July 1). *A Pro-Russia Disinformation Campaign Is Using Free AI Tools to Fuel a "Content Explosion."* WIRED. https://www.wired.com/story/pro-russia-disinformation-campaign-free-ai-tools/

[115] Pita, A., & Wirtschafter, V. (2024, June 26). *What role is AI playing in election disinformation?* Brookings. https://www.brookings.edu/articles/what-role-is-ai-playing-in-election-disinformation/

[116] Menn, J. (2025, April 17). *Russia seeds chatbots with lies. Any bad actor could game AI the same way.* The Washington Post. https://www.washingtonpost.com/technology/2025/04/17/llm-poisoning-grooming-chatbots-russia/

[117] Châtelet, V. (2025, April 18). *Exposing Pravda: How pro-Kremlin forces are poisoning AI models and rewriting Wikipedia*. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/exposing-pravda-how-pro-kremlin-forces-are-poisoning-ai-models-and-rewriting-wikipedia/

[118] Alber, D. A., Yang, Z., Alyakin, A., Yang, E., Rai, S., Valliani, A. A., Zhang, J., Rosenbaum, G. R., Amend-Thomas, A. K., Kurland, D. B., Kremer, C. M., Eremiev, A., Negash, B., Wiggan, D. D., Nakatsuka, M. A., Sangwon, K. L., Neifert, S. N., Khan, H. A., Save, A. V., & Palla, A. (2025). Medical large language models are vulnerable to data-poisoning attacks. *Nature Medicine*, *31*. https://doi.org/10.1038/s41591-024-03445-1

[119] Marcellino, W., Welch, J., Clayton, B., Webber, S., & Goode, T. (2025, July 22). *Acquiring Generative Artificial Intelligence to Improve U. S. Department of Defense Influence Activities*. Rand.org; RAND Corporation. https://www.rand.org/pubs/research_reports/RRA3157-1.html

[120] Warren, K., Menthe, L., Kane, B. R., Kessler, S., Lee, M., Lumpkin, D., Snyder, D. J., Zhang, L. A., Hartunian, A. E., & Konetzki, S. (2025). *Improving Sense-Making with Artificial Intelligence*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA3152-1.html

[121] Coalition for Content Provenance and Authenticity. (2025). *Advancing digital content transparency and authenticity*. C2pa.org. https://c2pa.org/

[122] European Brodcasting Union. (2024, December 18). *EBU joins early implementers of new standard to track media content provenance*. Tech.ebu.ch. https://tech.ebu.ch/news/2024/12/ebu-joins-early-implementers-of-new-standard-to-track-content-provenance

[123] National Security Agency, Australian Signals Directorate, Australian Cyber Security Centre, Canadian Centre for Cyber Security, & National Cyber Security Centre. (2025). *Content Credentials: Strengthening Multimedia Integrity in the Generative AI Era* (pp. 1–25). National Security Agency. https://media.defense.gov/2025/Jan/29/2003634788/-1/-1/0/CSI-CONTENT-CREDENTIALS.PDF

[124] Revitsky Locker, A., Heitzenrater, C., & Helmus, T. C. (2025, June 4). *Overpromising on Digital Provenance and Security*. Rand.org; RAND Corporation. https://www.rand.org/pubs/commentary/2025/06/overpromising-on-digital-provenance-and-security.html

[125] European Commission. (2023). *Strategic communication and countering information manipulation*. European Commission. https://commission.europa.eu/topics/countering-information-manipulation_en

[126] Bergmanis-Korāts, G., Isupova, M., & Vecmanis, R. R. (2025). *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty*. Stratcomcoe.org; StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia. https://stratcomcoe.org/publications/virtual-manipulation-brief-2025-from-war-and-fear-to-confusion-and-uncertainty/320

[127] Galicia, B. (2025, July 3). *In the fight against foreign information manipulation, the US can't afford to disarm*. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/in-the-fight-against-foreign-information-manipulation-the-us-cant-afford-to-disarm/

[128] Reuters Staff. (2025, August 14). *Poland foiled cyberattack on big city's water supply, deputy PM says.* Reuters. https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/

[129] Gerdžiūnas, B. (2025, July 11). *Russian drone crashed in Lithuania – what you should know*. Lrt.lt. https://www.lrt.lt/en/news-in-english/19/2606122/russian-drone-crashed-in-lithuania-what-you-should-know

[130] Jakučionis, S. (2025, August 5). *Explosive device found in drone from Belarus that crashed in Lithuania*. Lrt.lt. https://www.lrt.lt/en/news-in-english/19/2634744/explosive-device-found-in-drone-from-belarus-that-crashed-in-lithuania

[131] Biržietis, D. (2025, August 6). *Lithuania asks NATO to deploy anti-drone systems after explosive drone incident*. Lrt.lt. https://www.lrt.lt/en/news-in-english/19/2635106/lithuania-asks-nato-to-deploy-anti-drone-systems-after-explosive-drone-incident

[132] Bajarūnas, E. (2025, July 31). *Flight Risk: Baltics Scramble to Counter Hybrid Drone Threat*. CEPA. https://cepa.org/article/flight-risk-baltics-scramble-to-counter-hybrid-drone-threat/

[133] The Moscow Times. (2025, March 6). *Russia to Build Drone Factory in Belarus*. The Moscow Times. https://www.themoscowtimes.com/2025/03/06/russia-to-build-drone-factory-in-belarus-a88273

[134] Taradiuk, Y. (2025, March 7). *Russia proposes to build drone factory in Belarus to "ensure security."* The Kyiv Independent. https://kyivindependent.com/russia-proposes-to-build-drone-factory-in-belarus-to-ensure-security/

[135] Belta. (2025, June 13). *Lukashenko briefed on creation of drone troops in Belarus*. Eng.belta.by. https://eng.belta.by/president/view/lukashenko-briefed-on-creation-of-drone-troops-in-belarus-168907-2025/
[136] Loh, M. (2025, March 7). *Russia gearing up to build 100,000 drones on nato's doorstep*. Business Insider. https://www.businessinsider.com/russia-gearing-up-produce-drones-nato-doorstep-belarus-2025-3?ir=T
[137] Erling, B., & Charlish, A. (2024, August 26). *Poland says drone likely entered its airspace during Russian attack on Ukraine*. Reuters. https://www.reuters.com/world/europe/polish-army-says-object-entered-poland-during-russian-attack-ukraine-2024-08-26/
[138] Reuters Staff. (2024, September 5). *Poland backs off claim drone violated airspace during Russian attack on Ukraine.* Reuters. https://www.reuters.com/world/europe/poland-backs-off-claim-drone-violated-airspace-during-russian-attack-ukraine-2024-09-05/
[139] Reuters Staff. (2025, August 14). *Poland foiled cyberattack on big city's water supply, deputy pm says*. Reuters. https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/
[140] Koper, A., Strzelecki, M., Lebedev, F., & Sytas, A. (2025, April 10). *Insight: Sex toys and exploding cosmetics: anatomy of a "hybrid war" on the West*. Reuters. https://www.reuters.com/world/europe/sex-toys-exploding-cosmetics-anatomy-hybrid-war-west-2025-04-05/
[141] Gerdžiūnas, B. (2025, July 11). *Russian drone crashed in Lithuania – what you should know*. Lrt.lt. https://www.lrt.lt/en/news-in-english/19/2606122/russian-drone-crashed-in-lithuania-what-you-should-know
[142] Desmarais, A. (2025, August 14). *Lithuania joins Baltic neighbours in teaching children to build and fly drones*. Yahoo News. https://ca.news.yahoo.com/lithuania-joins-baltic-neighbours-teaching-110216590.html?guccounter=1
[143] Adamowski, J. (2024, April 8). *Polish defense leaders push "dronization" of the armed forces*. Defense News. https://www.defensenews.com/global/europe/2024/04/08/polish-defense-leaders-push-dronization-of-the-armed-forces/
[144] Koper, A., Strzelecki, M., Lebedev, F., & Sytas, A. (2025, April 10). *Insight: Sex toys and exploding cosmetics: anatomy of a "hybrid war" on the West*. Reuters. https://www.reuters.com/world/europe/sex-toys-exploding-cosmetics-anatomy-hybrid-war-west-2025-04-05/
[145] Biržietis, D. (2025, August 6). *Lithuania asks nato to deploy anti-drone systems after explosive drone incident*. Lrt.lt. https://www.lrt.lt/en/news-in-english/19/2635106/lithuania-asks-nato-to-deploy-anti-drone-systems-after-explosive-drone-incident
[146] Reuters Staff. (2025, August 14). *Poland foiled cyberattack on big city's water supply, deputy pm says*. Reuters. https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/
[147] Fried, D., & Polyakova, A. (2018, March 5). *Democratic defense against disinformation*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation/
[148] Lanoszka, A. (2019, January). *Disinformation in international politics*. Cambridge University Press. https://www.cambridge.org/core/journals/european-journal-of-international-security/article/abs/disinformation-in-international-politics/49121D3134C4079bf51E5012E6be247A
[149] Cornelissen, M. (2015, 1 kwietnia). *The Baltic States' struggle for hearts and minds*. Łotewski Instytut Spraw Międzynarodowych. http://www.liia.lv/en/opinions/the-baltic-states-struggle-for-hearts-and-minds-440
[150] Ministerstwo Sprawiedliwości. (2025). *Raport Zespołu ds. Dezinformacji Komisji ds. badania wpływów rosyjskich i białoruskich – Ministerstwo Sprawiedliwości – Portal Gov.pl*. Ministerstwo Sprawiedliwości. https://www.gov.pl/web/sprawiedliwosc/raport-zespolu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich
[151] Grabowska-Siwiec, A. (2025, September 11). *abw zatrzymała obywatela Białorusi podejrzanego o działalność szpiegowską*. LinkedIn. https://www.linkedin.com/posts/anna-grabowska-siwiec-mjr-dr-phd-b68265113_msz-bis-ah-activity-7371262983597023234-fFRl?utm_source=share&utm_medium=member_desktop&rcm=ACoAADhaxWgB2zzJziryDQtJN5LzDt8osTEFJbk
[152] Górnicka, B. (2025, August 8). Obywatel Rosji legalnie kupuje uczelnię a potem rekrutuje żołnierzy. Gazeta Wyborcza – Magazyn. http://wyborcza.pl/magazyn/7,124059,32159950,obywatel-rosji-legalnie-kupuje-uczelnie-a-potem-rekrutuje-zolnierzy.html
[153] Kancelaria Prezesa Rady Ministrów. (2025). *Projekt ustawy o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz niektórych innych ustaw – Kancelaria Prezesa Rady Ministrów – Portal Gov.pl*. Kancelaria Prezesa Rady Ministrów. https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-agencji-bezpieczenstwa-wewnetrznego-oraz-agencji-wywiadu-oraz-niektorych-innych-ustaw
[154] Ministerstwo Sprawiedliwości. (2025). *Raport Zespołu ds. Dezinformacji Komisji ds. badania wpływów rosyjskich i białoruskich – Ministerstwo Sprawiedliwości – Portal Gov.pl*. Ministerstwo Sprawiedliwości. https://www.gov.pl/web/sprawiedliwosc/raport-zespolu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich
[155] cert. (2024). *Raport roczny z działalności cert Polska 2023*. nask. https://www.nask.pl/media/2024/10/Raport_cert_2023.pdf
[156] Gwozdowska, A., Doleśniak-Harczuk, O., Rutke, G., Biernat, J., Oksińska, P., Jarka, I., Gromada, M., & Majka, A. (2023). *Wojna informacyjna 2022-2023: Przebieg i wnioski* (pp. 1–78). nask. https://www.nask.pl/media/2024/10/Raport__wojna_informacyjna.pdf
[157] Nawrotkiewicz, J., Majchrowski, T., Chorny Elizalde, V., Badji, S. D., & Mikulski, K. (2024). *Dezinformacja w wyborach na świecie* (pp. 1–135). nask. https://www.nask.pl/media/2024/12/Raport_Disinformation_pl_28112024_02.pdf
[158] Myslovskyi, I. (2025, 18 sierpnia). *European academia studies Russia too little, too refined, and too slowly*. *New Eastern Europe*. https://neweasterneurope.eu/2025/08/18/european-academia-studies-russia-too-little-too-refined-and-too-slowly/