RAPORT

Obce manipulacje informacyjne i ingerencja zewnętrzna (FIMI).

Zagrożenia i przeciwdziałanie w Polsce za okres od 2014 do 2024 r.

RAPORT 09/2024

INFO OPS POLSKA

www.infoops.pl | www.iri.org

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

Rekomendacje dla parlamentarzystów dotyczące odpowiedzi na FIMI

REDAKCJA NA DZIEŃ 16092024

Spis treści

Autorzy: Maksym Sijer, Wojciech Pokora

This report has been prepared with support from IRI's Beacon Project. The opinions expressed are solely those of the author and do not reflect those of IRI.

Streszczenie

- **Pojęcie FIMI jest w istocie interpretacją wybranych aspektów środków aktywnych.** Sowieckie środki aktywne (ros. активные мероприятия) to termin używany w odniesieniu do szerokiego zakresu działań propagandowych, dezinformacyjnych i operacji wpływu prowadzonych przez Związek Sowiecki w okresie zimnej wojny.

- **Przeciwdziałanie FIMI wymaga skoordynowanych wysiłków zarówno ze strony sektora państwowego (bezpieczeństwo cywilne i wojskowe), jak i podmiotów pozarządowych,** w tym środowisk akademickich i mediów. Zaangażowanie organizacji pozarządowych i społeczeństwa obywatelskiego odgrywa znaczącą rolę.

- **W Polsce** problematyka związana z Foreign Information Manipulation and Interference (FIMI), czyli manipulacją informacyjną i ingerencją z zagranicy, **nie ma bezpośredniego włączenia do ram prawnych i regulacyjnych jako zamknięty akt prawny i definicyjny.**

- **W Polsce istnieją pojedyncze przepisy i regulacje, których umiejętne wykorzystanie pozwala ograniczać potencjał wrogich operacji FIMI ale nie są one dostatecznie wykorzystywane.**

- 2014 rok był kluczowym momentem, kiedy Polska, podobnie jak inne kraje Europy Środkowo-Wschodniej, zaczęła intensywnie analizować zagrożenia związane z dezinformacją i wpływami obcych państw, zwłaszcza w kontekście agresji Rosji na Ukrainę.

- **Polskie komisje parlamentarne** (wyspecjalizowane komisje): takie jak Komisja do Spraw Służb Specjalnych, Komisja Obrony Narodowej oraz Komisja Administracji i Spraw Wewnętrznych, mają możliwość analizowania działań instytucji krajowych związanych z przeciwdziałaniem FIMI i **powinny to robić regularnie oraz przedstawiać swoje rekomendacje dotyczące polityki państwa w tym obszarze, w tym publikować publicznie dostępne raporty** (obecnie takowych nie ma).

- Kwestie bezpieczeństwa przestrzeni informacyjnej są na stałe związane z wrogimi operacjami ingerencji. **Zdolności kontrwywiadowcze państwa w połączeniu z aktywnościami systemu państwowego i pozarządowego są i będą kluczowe w przeciwdziałaniu operacjom wpływu.**

- Polska aktywnie uczestniczy w międzynarodowych inicjatywach mających na celu walkę z dezinformacją, takich jak działania NATO czy Unii Europejskiej, które obejmują również aspekty prawne dotyczące FIMI.

- Po wybuchu wojny na Ukrainie w 2022 roku, Polska zintensyfikowała działania w zakresie ochrony przestrzeni informacyjnej, w tym organizacyjnie i legislacyjne.

- W nadchodzących latach **Polska będzie musiała stawić czoła nowym i rozwijającym się zagrożeniom informacyjnym**, które obejmują zaawansowane technologie, manipulację wyborami, wyzwania związane z migracją oraz rosnąca skala cyberataków.

- W Polsce, podobnie jak w innych krajach, **wrogie podmioty zaangażowane w Foreign Information Manipulation and Interference (FIMI) wykorzystują wrażliwości typowe, które są charakterystyczne dla polskiego systemu medialnego, politycznego i społecznego.**

- **Konieczne będą zintegrowane i innowacyjne podejścia do ochrony przed operacjami informacyjnymi i psychologicznymi.** Rozbudowa systemu cyberbezpieczeństwa, budowa dedykowanych **zespołów bezpieczeństwa przestrzeni informacyjnej,** a także skuteczne strategie komunikacyjne i współpraca międzynarodowa, aby zabezpieczyć integralność demokracji i stabilność społeczną Polski i krajów Zachodu.

- **Niedostateczna współpraca między instytucjami:** Mimo że w Polsce działają instytucje, które monitorują i walczą z dezinformacją, brakuje efektywnej koordynacji między różnymi podmiotami, w tym rządem, mediami, organizacjami pozarządowymi i platformami społecznościowymi.

- **Wysoki poziom nieufności Polaków do mediów** i instytucji publicznych sprawia, że wrogie podmioty łatwiej wprowadzają „alternatywny obieg (dez)informacji" i własne narracje, które znajdują oddźwięk wśród podatnych na nie odbiorców i są przez nich kolportowane.

- **Istnieją powiązania i zbieżności między wewnętrznymi,** lokalnymi **aktorami a zewnętrznymi podmiotami** prowadzącymi działania związane z Foreign Information Manipulation and Interference (FIMI) przeciwko Polsce.

- Mimo że **wsparcie dla Ukrainy na poziomie politycznym nie jest bezpośrednio zagrożone, spory między polskimi siłami politycznymi mogą wpływać na to, jak temat ten jest przedstawiany w debacie publicznej**. Wrogie podmioty mogą wykorzystywać te spory, aby zaostrzać podziały i podważać konsensus polityczny wokół pomocy Ukrainie.

- **Brak pamięci instytucjonalnej**: niedostateczna kontynuacja działań i strategii związanych z przeciwdziałaniem dezinformacji. Nowe zespoły i instytucje często muszą zaczynać od 0 lub w zbyt małym stopniu korzystają z wcześniejszych doświadczeń i wypracowanego dorobku administracji i poprzedników.

- **Parlament Europejski powinien dążyć do wprowadzenia bardziej kompleksowych (horyzontalnych) regulacji dotyczących walki z dezinformacją**. Oznaczałoby to zakaz rozpowszechniania dezinformacji we wszystkich kontekstach, jeśli stwarza ona zagrożenie dla interesu publicznego, zamiast ograniczania przepisów do konkretnych obszarów (wertykalność).

- **Obecnie różnice w regulacjach dotyczących dezinformacji między państwami członkowskimi UE utrudniają skuteczną koordynację**. Parlament Europejski powinien wspierać harmonizację przepisów, tak aby wszystkie kraje miały wspólne standardy i podejścia w walce z FIMI.

Przeciwdziałanie FIMI w Polsce. 2014 - 2024

Działania analityczne. Polskie instytucje analityczne raportują na temat rosyjskiej propagandy i dezinformacji.

2014

Rosyjska agresja na Ukrainę i aneksja Krymu przez Rosję

Monitorowanie i raportowanie rosyjskiej propagandy w tradycyjnych i elektronicznych środkach przekazu.

2014-2015

Rozbudowa zdolności do detekcji FIMI

Zacieśnienie współpracy międzynarodowej z NATO i UE w zakresie przeciwdziałania dezinformacji.

2016

Rozwój instytucjonalny, pierwsze zmiany legislacyjne

Wprowadzenie dokumentu uwzględniającego zagrożenia związane z wojną informacyjną i dezinformacją.

2017

Koncepcja Obrony Narodowej

Edukacja, budowa odporności społecznej i świadomości dotyczącej zagrożeń informacyjnych.

2017

Strategie i zmiany prawne

Stworzenie ram prawnych do ochrony cyberprzestrzeni w tym przeciwdziałania cyberatakom.

2018

Ustawa o Krajowym Systemie Cyberbezpieczeństwa

Strategia podkreśla konieczność wzmacniania odporności na działania informacyjne, w tym dezinformację.

2020

Strategia Bezpieczeństwa Narodowego, zmiany legislacyjne

Budowa zespołów i instytucji ds przeciwdziałania dezinformacji: NASK, RCB, MSZ, KPRM (pełnomocnik rządu).

2020-2023

Budowa zdolności do przeciwdziałania dezinformacji

Ustanowienie pełnomocnika ds. przeciwdziałania dezinformacji przy MSZ, rozbudowa potencjału MSZ i NASK.

2023-2024

Budowa zdolności do przeciwdziałania dezinformacji

INFO OPS POLSKA

www.infoops.pl | www.iri.org

IRI INTERNATIONAL REPUBLICAN INSTITUTE Advancing Democracy Worldwide

Wprowadzenie

Foreign Information Manipulation and Interference (FIMI), czyli Zagraniczna Manipulacja i Zakłócanie Informacji, to termin używany do opisania działań podejmowanych przez wrogie podmioty zagraniczne, które mają na celu wpływanie na opinię publiczną, procesy polityczne (procesy decyzyjne), czy bezpieczeństwo narodowe poprzez manipulację informacją lub zakłócenia przepływu informacji.

- **Manipulacja informacją:** rozpowszechnianie fałszywych, wprowadzających w błąd lub zmanipulowanych informacji w celu wpłynięcia na percepcję lub decyzje społeczne. Może to obejmować dezinformację (rozpowszechnianie fałszywych informacji lub w zmanipulowanym kontekście tzw. selektywny dobór informacji) oraz propagandę.
- **Zakłócanie procesów informacyjnych:** działania mające na celu zakłócenie dostępu do prawdziwych informacji lub zniekształcenie ich odbioru. Przykładami mogą być cyberataki na media, platformy społecznościowe lub systemy wyborcze oraz podszywanie się pod znane media.
- **Celem FIMI jest** zazwyczaj destabilizacja społeczeństwa, osłabienie zaufania do instytucji demokratycznych, podważenie wyników wyborów, wywołanie niepokojów społecznych lub wpłynięcie na decyzje polityczne danego kraju zgodnie z wolą ośrodka wprowadzającego w błąd.

Pojęcie FIMI jest w istocie zachodnią interpretacją wybranych aspektów środków aktywnych. Sowieckie środki aktywne (ros. активные мероприятия) to termin używany w odniesieniu do szerokiego zakresu działań propagandowych, dezinformacyjnych i operacji wpływu prowadzonych przez Związek Sowiecki w okresie zimnej wojny. Celem tych działań było wpływanie na opinię publiczną i procesy polityczne w krajach zachodnich oraz w innych regionach świata, w celu osłabienia ich rządów, podważenia zaufania do instytucji demokratycznych, a także promowania interesów ZSRS. Zagrożenia FIMI dla bezpieczeństwa Polski ze strony aktorów państwowych w zdecydowanej mierze tyczą się działań aktywnych Federacji Rosyjskiej, Chin i Białorusi. Rosja, kontynuując tradycje sowieckie (tzn. zdolności, wynikające z ciągłości funkcjonowania aparatu bezpieki), stosuje różnorodne środki aktywne przeciwko Polsce, mające na celu destabilizację społeczną, podważanie zaufania do instytucji demokratycznych oraz osłabienie pozycji Polski na arenie międzynarodowej.

Ramy prawne

W Polsce problematyka związana z Foreign Information Manipulation and Interference (FIMI), czyli manipulacją informacyjną i ingerencją z zagranicy, nie ma bezpośredniego włączenia do ram prawnych i regulacyjnych jako zamknięty akt prawny i definicyjny. Są jednak pojedyncze przepisy i regulacje, których umiejętne wykorzystanie pozwala ograniczać potencjał wrogich operacji FIMI. Na uwagę zasługują szczególnie następujące wydarzenia i procesy legislacyjne:

1. Reakcja na wojnę Rosja - Ukraina (2014)

2014 rok był kluczowym momentem, kiedy Polska, podobnie jak inne kraje Europy Środkowo-Wschodniej, zaczęła intensywnie analizować zagrożenia związane z dezinformacją i wpływami obcych państw, zwłaszcza w kontekście agresji Rosji na Ukrainę. Rząd polski oraz instytucje odpowiedzialne za bezpieczeństwo narodowe zaczęły traktować problem dezinformacji jako zagrożenie dla bezpieczeństwa państwa.

2. Nowelizacje Prawa Medialnego i Ustaw o Ochronie Informacji (2016-2017)

W latach 2016-2017 rząd Polski podjął pierwsze kroki w kierunku regulacji mediów w kontekście przeciwdziałania dezinformacji. Zmieniono niektóre przepisy prawa medialnego, a także rozpoczęto dyskusje na temat konieczności ochrony przestrzeni informacyjnej przed zagranicznymi wpływami.

Zostały wprowadzone również zmiany w przepisach dotyczących ochrony informacji niejawnych oraz przeciwdziałania cyber zagrożeniom.

3. Ustawa o Krajowym Systemie Cyberbezpieczeństwa (2018)

W 2018 roku w Polsce wprowadzono Ustawę o Krajowym Systemie Cyberbezpieczeństwa, która odnosi się także do zagrożeń związanych z dezinformacją i wpływami obcych państw w cyberprzestrzeni. Ustawa ta obejmuje między innymi działania mające na celu ochronę infrastruktury krytycznej i przeciwdziałanie cyberatakom, które często są powiązane z kampaniami dezinformacyjnymi.

4. Strategia Bezpieczeństwa Narodowego (2020)

Strategia Bezpieczeństwa Narodowego Polski z 2020 roku zawierała jasne odniesienia do zagrożeń związanych z dezinformacją i wpływami obcych państw. W strategii tej FIMI zostało zidentyfikowane jako jedno z głównych wyzwań dla bezpieczeństwa narodowego. Po raz pierwszy zagrożenie FIMI zyskało osobny rozdział. Wskazano na konieczność wzmacniania odporności społeczeństwa na manipulacje informacyjne oraz poprawy zdolności instytucji państwowych do przeciwdziałania tym zagrożeniom, w kooperacji z organizacjami pozarządowymi.

5. Nowelizacja ustawy o radiofonii i telewizji (2021-2022)

W ramach nowelizacji ustawy o radiofonii i telewizji pojawiły się kwestie związane z kontrolą kapitału zagranicznego w polskich mediach. Ustawa ta nie uniknęła kontrowersji politycznych (przykład1; przykład2) ale stanowiła przykład próby regulacji

wpływów zagranicznych w polskim krajobrazie medialnym, co wpisuje się w szerszy kontekst FIMI przy odpowiednim zaadresowaniu przepisów.

6. Zwiększenie monitoringu mediów społecznościowych

W ciągu ostatnich kilku lat, polskie organy ścigania oraz instytucje odpowiedzialne za bezpieczeństwo narodowe monitorują media społecznościowe w celu wykrywania i przeciwdziałania kampaniom dezinformacyjnym prowadzonym przez zagraniczne podmioty. W szerszym kontekście, kwestie bezpieczeństwa przestrzeni informacyjnej są na stałe związane z wrogimi operacjami ingerencji. Zdolności kontrwywiadowcze państwa uzupełniły zakres zainteresowania o platformy nowych technologii, które są wykorzystywane przez wrogich aktorów do operacji FIMI.

7. Współpraca międzynarodowa

Polska aktywnie uczestniczy w międzynarodowych inicjatywach mających na celu walkę z dezinformacją, takich jak działania NATO czy Unii Europejskiej, które obejmują również aspekty prawne dotyczące FIMI. Na poziomie UE Polska wspierała inicjatywy związane z regulacją platform internetowych (DSA i DMA) oraz tworzeniem mechanizmów szybkiego reagowania na dezinformację (Rapid Alert System).

8. Nowe inicjatywy legislacyjne (od 2022)

Po wybuchu pełnoskalowej wojny na Ukrainie w 2022 roku, Polska zintensyfikowała działania w zakresie ochrony przestrzeni informacyjnej. Trwają prace nad nowymi regulacjami, które mają na celu dalsze wzmocnienie odporności kraju na manipulacje informacyjne i ingerencje z zagranicy. W szczególności:

Art. 130. Kodeksu Karnego dotyczący *Szpiegostwa*, a w szczególności § 9. zostały uzupełnione o zapisy dotyczące działalności dezinformacyjnej: „*Kto, biorąc udział w działalności obcego wywiadu albo działając na jego rzecz, prowadzi dezinformację, polegającą na rozpowszechnianiu nieprawdziwych lub wprowadzających w błąd informacji, mając na celu wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest Rzeczpospolita Polska albo skłonienie organu władzy publicznej Rzeczypospolitej Polskiej, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest Rzeczpospolita Polska, do podjęcia lub zaniechania określonych czynności, podlega karze pozbawienia wolności na czas nie krótszy od lat 8.*”

9. Istniejące prawo, nie dedykowane FIMI ale mogące być wykorzystane do jego zwalczania

Jeżeli chodzi o szkody publiczne wywołane dezinformacją, to aktualnie w Polsce obowiązuje przepis z **art.111 §1 ustawy - kodeks wyborczy**, zwalczający rozpowszechnianie nieprawdziwych informacji w związku z kampanią wyborczą.

Ponadto **artykuł 180 ust. 1 Prawa Telekomunikacyjnego** brzmi: *Przedsiębiorca telekomunikacyjny jest obowiązany do niezwłocznego blokowania połączeń telekomunikacyjnych lub przekazów informacji, na żądanie uprawnionych podmiotów,*

jeżeli połączenia te mogą zagrażać obronności, bezpieczeństwu państwa oraz bezpieczeństwu i porządkowi publicznemu, albo do umożliwienia dokonania takiej blokady przez te podmioty. Na bazie tego przepisu ABW (Agencja Bezpieczeństwa Wewnętrznego) po 24.02.2022 r. zablokowała szereg domen będących przekaźnikami rosyjskiej dezinformacji i propagandy.

Funkcjonuje także lista domen zgłaszanych przez ABW na podstawie artykułu 32c ustawy o ABW, zawierająca witryny o charakterze terrorystycznym. Ponadto rząd polski dostosowując polskie prawo do przepisów Unii Europejskiej, które dotyczą przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, przyjął projekt ustawy umożliwiającej szefowi ABW, a nie jak dotychczas sądowi, decydowanie o tym, które treści w internecie mają charakter terrorystyczny. Na mocy decyzji szefa ABW mogą być one usuwane.

Art. 117. Kodeksu Karnego § 3. brzmi: *Kto publicznie nawołuje do wszczęcia wojny napastniczej* ***lub publicznie pochwala wszczęcie lub prowadzenie takiej wojny****, podlega karze pozbawienia wolności od 3 miesięcy do lat 5*. Jest to najpotężniejszy i najbardziej bezpośredni przepis prawny, który wprost uderza w środowiska rezonujące rosyjskie FIMI po 24.02.2022 r., a jednocześnie **najmniej wykorzystane narzędzie prawne**.

Art. 55 Ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu mówi, że zaprzeczanie publicznie i wbrew faktom zbrodniom, o których mowa w art. 1 pkt 1 powyższej ustawy, jest przestępstwem ściganym z urzędu zagrożonym grzywną lub karą pozbawienia wolności do lat 3. Wyrok podawany jest do publicznej wiadomości.

Czynami określonymi w art. 1 pkt 1 ustawy są:

a) popełnione na osobach narodowości polskiej lub obywatelach polskich innych narodowości w okresie od dnia 1 września 1939 r. do dnia 31 lipca 1990 r.:

- zbrodnie nazistowskie,
- zbrodnie komunistyczne,
- inne przestępstwa stanowiące zbrodnie przeciwko pokojowi, ludzkości lub zbrodnie wojenne.

b) inne represje z motywów politycznych, jakich dopuścili się funkcjonariusze polskich organów ścigania lub wymiaru sprawiedliwości albo osoby działające na ich zlecenie, a ujawnione w treści orzeczeń zapadłych na podstawie *ustawy z dnia 23 lutego 1991 r. o uznaniu za nieważne orzeczeń wydanych wobec osób represjonowanych za działalność na rzecz niepodległego bytu Państwa Polskiego*.

Ustawa zabrania negacji wszelkich zbrodni popełnionych przez systemy totalitarne, zarówno w mutacji faszystowskiej, jak komunistycznej. Dotyczy więc **"kłamstwa oświęcimskiego",** jak określane są negacjonizm i rewizjonizm Holocaustu – twierdzenie w języku prawnym przyjmujące, że powszechnie przyjęta interpretacja Holocaustu jest

albo w dużym stopniu przesadzona, albo całkowicie zafałszowana. Ponieważ ustawa zabrania także negacji zbrodni komunizmu, zasadne jest również mówienie o **„kłamstwie katyńskim”**.

Wszystkie powyższe kroki świadczą o tym, że Polska stopniowo budowała ramy prawne i regulacyjne w odpowiedzi na zagrożenia związane z FIMI, dostosowując swoje przepisy do dynamicznie zmieniających się wyzwań w sferze bezpieczeństwa informacyjnego. Niemniej działania w tym obszarze powinny być cały czas rozwijane zarówno pod względem legislacji jak i **egzekucji już istniejących przepisów**.

Instytucje odpowiedzialne za przeciwdziałanie i analizę FIMI

W Polsce przeciwdziałaniem oraz analizą zagrożeń związanych z Foreign Information Manipulation and Interference (FIMI) zajmuje się szereg instytucji i agencji państwowych, które współpracują w ramach różnych struktur rządowych. Oto główne z nich:

1. DPD NASK (Dział Przeciwdziałania Dezinformacji NASK)

NASK (Naukowa i Akademicka Sieć Komputerowa) to instytut badawczy podległy resortowi cyfryzacji. Na początku 2022 r. utworzono w nim dział przeciwdziałania dezinformacji (DPD). Od marca 2024 roku przeszedł duże zmiany i jego uwaga ma być skupiona na zewnętrznych zagrożeniach dla Polski.

Ze względu na zasoby kadrowe i finansowe, którymi dysponuje, na DPD NASK spoczywa największy obowiązek i odpowiedzialność ze wszystkich instytucji cywilnych w Polsce.

2. Agencja Bezpieczeństwa Wewnętrznego (ABW)

Zadania: ABW jest główną agencją odpowiedzialną za ochronę bezpieczeństwa wewnętrznego Polski, w tym przeciwdziałanie zagrożeniom związanym z dezinformacją i manipulacją informacyjną ze strony obcych państw. ABW monitoruje i analizuje działania dezinformacyjne oraz prowadzi operacje mające na celu ich neutralizację.

Współpraca międzynarodowa: ABW współpracuje ze służbami wywiadowczymi i agencjami bezpieczeństwa z państw sojuszniczych, aby skutecznie przeciwdziałać zagrożeniom FIMI na poziomie międzynarodowym.

3. Służba Kontrwywiadu Wojskowego (SKW)

Zadania: SKW odpowiada za ochronę bezpieczeństwa wojskowego Polski, w tym za przeciwdziałanie dezinformacji i manipulacjom informacyjnym, które mogą zagrażać polskim siłom zbrojnym i ich operacjom. SKW monitoruje działania informacyjne skierowane przeciwko polskim interesom wojskowym, zarówno w kraju, jak i za granicą.

4. Ministerstwo Obrony Narodowej (MON)

Zadania: MON, poprzez swoje struktury, takie jak Centrum Operacyjne MON czy dowództwa sił zbrojnych, prowadzi działania mające na celu przeciwdziałanie dezinformacji w przestrzeni medialnej i internetowej. MON koordynuje działania związane z cyberbezpieczeństwem, które obejmują również ochronę przed operacjami FIMI.

Cyberbezpieczeństwo: MON zarządza krajowymi zdolnościami cyberobrony, w tym ochroną przed cyberatakami, które często są powiązane z kampaniami dezinformacyjnymi.

5. Ministerstwo Spraw Wewnętrznych i Administracji (MSWiA)

Zadania: MSWiA, poprzez swoje agendy, w tym Policję i Straż Graniczną, monitoruje i reaguje na zagrożenia związane z dezinformacją, szczególnie w kontekście porządku publicznego i bezpieczeństwa wewnętrznego. MSWiA jest również zaangażowane w edukację i kampanie informacyjne mające na celu zwiększenie świadomości społecznej na temat zagrożeń FIMI.

Bezpieczeństwo informacyjne: MSWiA koordynuje działania w zakresie ochrony infrastruktury krytycznej i bezpieczeństwa informacyjnego na poziomie administracyjnym.

5. Rządowe Centrum Bezpieczeństwa (RCB)

Zadania: RCB jest instytucją odpowiedzialną za koordynację działań rządowych w sytuacjach kryzysowych, w tym tych wynikających z dezinformacji i manipulacji informacyjnej. RCB opracowuje scenariusze reagowania na różne formy zagrożeń, w tym hybrydowe, które mogą obejmować kampanie FIMI. Jawnym dokumentem obejmującym analizę zagrożenia dezinformacją jest Krajowy Plan Zarządzania Kryzysowego (KPZK RCB).

Zarządzanie kryzysowe: RCB współpracuje z innymi instytucjami państwowymi w zakresie monitorowania i analizowania zagrożeń oraz koordynuje działania przeciwdziałające tym zagrożeniom, co może mieć istotne znaczenie przy zarządzaniu incydentami, których efekty mogą negatywnie oddziaływać na środowisko informacyjne (kataklizm, zamach, inne incydenty fizyczne).

6. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC)

Zadania: DKWOC działa w ramach Wojska Polskiego i jest odpowiedzialne za ochronę cyberprzestrzeni Polski, w tym za monitorowanie i neutralizowanie zagrożeń płynących od aktorów państwowych. DKWOC współpracuje z innymi służbami w zakresie wymiany informacji i reagowania na incydenty związane z bezpieczeństwem.

7. Ministerstwo Spraw Zagranicznych (MSZ)

W maju 2024 roku powołano pełnomocnika ministra spraw zagranicznych ds. przeciwdziałania dezinformacji międzynarodowej. Pełnomocnik ma stanąć na czele Działu Komunikacji Strategicznej.

Zadania: Nowy pełnomocnik będzie odpowiedzialny za realizację strategii i koordynację działań w zakresie identyfikacji, monitorowania i zwalczania obcej dezinformacji. Zadaniem pełnomocnika będzie współpraca z międzynarodowymi partnerami oraz organizacjami zajmującymi się problematyką dezinformacji oraz koordynacja współdziałania z krajowymi urzędami i instytucjami, a także organizacjami pozarządowymi w celu wymiany informacji, doświadczeń i najlepszych praktyk. MSZ prowadzi działania dyplomatyczne mające na celu przeciwdziałanie dezinformacji na arenie międzynarodowej, w tym przeciwdziałanie kampaniom FIMI skierowanym przeciwko Polsce. MSZ jest również zaangażowane w informowanie społeczności międzynarodowej o zagrożeniach ze strony obcych państw.

Public diplomacy: MSZ prowadzi aktywną dyplomację publiczną, starając się korygować fałszywe informacje i promować prawdziwy obraz Polski na arenie międzynarodowej, w tym poprzez specjalny program grantowy, który jest dedykowany przeciwdziałaniu dezinformacji międzynarodowej przez organizacje pozarządowe.

8. Krajowa Rada Radiofonii i Telewizji (KRRiT)

Zadania: KRRiT monitoruje polski rynek medialny, dbając o zgodność nadawanych treści z polskim prawem, w tym o przeciwdziałanie dezinformacji i manipulacjom medialnym. KRRiT może również nakładać sankcje na nadawców, którzy naruszają przepisy dotyczące bezpieczeństwa informacyjnego.

Regulacja mediów: KRRiT pracuje nad regulacjami, które mają na celu zwiększenie przejrzystości mediów oraz ograniczenie wpływów zagranicznych na polskie środki przekazu.

10. Urząd Ochrony Danych Osobowych (UODO)

Zadania: UODO monitoruje ochronę danych osobowych, co jest istotne w kontekście przeciwdziałania FIMI, ponieważ operacje typu “hack and leak” często wiążą się z nieuprawnionym wykorzystywaniem danych osobowych. Urząd ten współpracuje z innymi instytucjami w zakresie ochrony prywatności i bezpieczeństwa danych.

11. Instytuty badawcze i think-tanki

W ciągu ostatnich 10 lat w Polsce powstało kilkanaście ośrodków, grup roboczych czy instytucji zajmujących się analizą dezinformacji i FIMI. Niestety nie wszystkie inicjatywy funkcjonują do dziś. Sztandarowymi inicjatywami, ośrodkami i NGO były: „Rosyjska V Kolumna w Polsce”; „Disinfo Digest”; „Centrum Analiz Propagandy i Dezinformacji - CAPD”; „STOP FAKE PL”; analizy dezinformacji w „Centrum Stosunków Międzynarodowych” - CSM; „Laboratorium INFO OPS w Fundacji Bezpieczna Cyberprzestrzeń”; analizy dezinformacji w „Fundacji im. Kazimierza Pułaskiego”; analizy

dezinformacji w „Instytucie Kościuszki”; dziennikarskie śledztwa w sprawie rosyjskiej dezinformacji i propagandy we „Frontstory”; organizacja w całości poświęcona walce z FIMI: „Fundacja INFO OPS Polska”.

Państwowe ośrodki zajmujące się głównie analizą dokumentów strategicznych i doktryn związanych z wojną informacyjną: „Ośrodek Studiów Wschodnich - OSW”; „Polski Instytut Spraw Międzynarodowych - PISM”; „Akademickie Centrum Komunikacji Strategicznej - ACKS”. Instytucje te dostarczają analizy i raporty wspierające rząd w rozumieniu zagrożeń informacyjnych. Istnieją również organizacje pozarządowe zajmujące się dezinformacją i weryfikacją faktów jako zjawiskiem społecznym (nie konkretnie FIMI), z których największą jest „Demagog”. Polska Agencja Prasowa uruchomiła również projekt walki z dezinformacją i fake newsami pod nazwą „Fake Hunter”.

12. Krajowy Zespół ds. Cyberbezpieczeństwa (CERT Polska)

Zadania: CERT Polska jest zespołem reagowania na incydenty komputerowe, działającym w ramach NASK. CERT Polska monitoruje i reaguje na zagrożenia w cyberprzestrzeni, w tym pośrednio na incydenty teleinformatyczne, które mogą być elementem obcych operacji wpływu (fraudy stron internetowych, spoofing, inne oszustwa internetowe).

Każda z powyższych instytucji odgrywa kluczową rolę w ochronie polskiej przestrzeni informacyjnej przed zagrożeniami związanymi z FIMI, działając zarówno w sposób samodzielny, jak i w ramach szerszej współpracy międzyresortowej oraz międzynarodowej.

Ewolucja i dynamika analizowania, raportowania i przeciwdziałania FIMI

Ewolucja i dynamika analizowania, raportowania oraz przeciwdziałania Foreign Information Manipulation and Interference (FIMI) w Polsce od 2014 roku odzwierciedla rosnącą świadomość zagrożeń związanych z dezinformacją oraz potrzebę odpowiedzi na coraz bardziej zaawansowane i złożone działania wpływu ze strony państw trzecich, w szczególności Rosji.

1. Początkowa faza (2014-2016): Świadomość zagrożeń i pierwsze reakcje

Kontekst geopolityczny

- **Rosyjska wojna przeciwko Ukrainie** (2014) i aneksja Krymu przez Rosję zwiększyły obawy w Polsce dotyczące działań dezinformacyjnych i manipulacyjnych prowadzonych przez Rosję w Europie Środkowo-Wschodniej. Rosja intensywnie korzystała z narzędzi propagandowych, by uzasadnić swoje działania na Ukrainie, co rozwijało świadomość w Polsce na temat potencjalnych zagrożeń.

Pierwsze działania

- **Analizy think-tanków**: Polskie instytucje analityczne (opisane w poprzednim rozdziale „Instytuty badawcze i think-tanki"), zaczęły intensywniej badać i raportować na temat rosyjskiej propagandy i dezinformacji w regionie. Powstały również pierwsze organizacje weryfikujące informacje.
- **Monitorowanie mediów**: Rozpoczęły się pierwsze systematyczne działania monitorowania środowiska informacyjnego i wpływu rosyjskiej propagandy, przekazów skierowanych do polskiego społeczeństwa, a także badania i analizy narracji propagandowych.

2. Faza konsolidacji (2016-2018): Rozwój instytucjonalny i strategiczny

Wzmocnienie instytucjonalne

- **Nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa**: W 2018 roku przyjęto ustawę, która stworzyła ramy prawne do ochrony cyberprzestrzeni Polski, w tym przeciwdziałania cyberatakom i dezinformacji. Utworzenie sieci CSIRT (Computer Security Incident Response Teams) było istotne w kontekście obrony przed operacjami FIMI poprzez usystematyzowanie i uporządkowania procesów obsługi incydentów w cyberprzestrzeni, cyberataków, które mogą być elementem operacji wpływu.

Strategie i polityki

- **Koncepcja Obrony Narodowej** (2017): Dokument ten uwzględnia zagrożenia związane z wojną informacyjną i dezinformacją, wskazując na potrzebę budowania odporności państwa na takie ataki.
- **Zacieśnienie współpracy międzynarodowej**: Polska zintensyfikowała współpracę z NATO i UE w zakresie przeciwdziałania dezinformacji, co przełożyło się na udział w projektach wspólnego monitorowania i analizowania operacji wpływu.

3. Faza zaawansowanej reakcji (2018-2020): Rozwój narzędzi i zaangażowanie społeczne

Strategia Bezpieczeństwa Narodowego (2020)

- **Uwzględnienie zagrożeń hybrydowych**: Strategia ta podkreślała konieczność wzmacniania odporności na działania informacyjne, w tym dezinformację, co było odpowiedzią na narastające zagrożenia ze strony Rosji.
- **Edukacja i świadomość społeczna**: Wzrosło zaangażowanie państwa w kampanie informacyjne i edukacyjne skierowane do społeczeństwa, mające na celu zwiększenie odporności na dezinformację.

4. Faza intensywnej walki (2020-2023): Systematyzacja i cyfryzacja działań

Nowe narzędzia i technologie

- **Rozwój narzędzi analitycznych**: Polska wprowadziła bardziej zaawansowane technologie monitorowania i analizy danych, które pozwalają na szybsze wykrywanie i analizowanie kampanii dezinformacyjnych.
- **Platformy współpracy**: Rozwój platform współpracy międzyinstytucjonalnej, w tym z sektorem prywatnym i organizacjami międzynarodowymi, poprawił koordynację działań.

Nowe instytucje i inicjatywy

- **Rządowe Centrum Bezpieczeństwa (RCB):** Rozwinięcie funkcji RCB w zakresie reagowania na kryzysy informacyjne oraz wprowadzenie systemu wczesnego ostrzegania (publicznie dostępny komponent - #Disinfo Radar) przed kampaniami dezinformacyjnymi (2021 - 2024).
- **Powołanie Pełnomocnika Rządu do spraw Bezpieczeństwa Przestrzeni Informacyjnej** (2022 - 2023), którego obszar odpowiedzialności to koordynacja, analiza i przeciwdziałania dezinformacji na poziomie państwowym, międzyresortowym.

- Utworzenie specjalistycznego kursu w **Eksperckim Centrum Szkolenia Cyberbezpieczeństwa MON** na kierunku INFO OPS oraz uruchomienie

dedykowanych projektów na uczelniach wojskowych, w tym utworzenie kierunku studiów “Bezpieczeństwo informacyjne i cyberbezpieczeństwo” dla studentów cywilnych w Akademii Sztuki Wojennej.

- **Powołanie specjalistycznej komórki ds. walki z dezinformacja międzynarodową w Ministerstwie Spraw Zagranicznych** (od 2023). W 2024 roku komórka została przekształcona w departament i wzmocniona pod względem kadrowym i organizacyjnym.

- **Powołanie DPD w NASK (2022)** i rozbudowa zespołu Działu Przeciwdziałania Dezinformacji w NASK (od 2024).

Inicjatywy społeczne i edukacyjne

Kampanie informacyjne: W Polsce prowadzone były kampanie mające na celu edukację społeczeństwa w zakresie rozpoznawania dezinformacji i fałszywych narracji. Kampania Sztabu Generalnego Wojska Polskiego “#PSYCHOodporni to #DEZINFOodporni” to aktualnie (2024 - obecnie) jedyna trwająca kampania informacyjno-edukacyjna (przykład).

- **Kampanie i inicjatywy, wybrane przykłady:**

    - Kampania „Nie daj się nabrać, sprawdź zanim uwierzysz” (Ministerstwo Cyfryzacji):
    - Program NASK "Włącz Weryfikację" (od lutego 2022 do kwietnia 2024 roku).
    - “Odpowiedzialni za Słowo" (Fundacja Panoptykon - NGO)
    - #StopFakeNews (Polska Policja)
    - Disinfo Radar (2022 - 2024 Rządowe Centrum Bezpieczeństwa)
    - Kampania "Stop Fake News" (2020): Podczas pandemii COVID-19 Ministerstwo Zdrowia
    - "Znajdź właściwe źródło" (2021 Ministerstwo Zdrowia)

- **Stacje telewizyjne i programy poświęcone zwalczaniu dezinformacji i budowaniu świadomości:**

    - Biełsat TV (ang. Bielsat TV) - stacja telewizyjna nadająca w języku białoruskim, rosyjskim i ukraińskim. Biełsat zapewnia Białorusinom dostęp do niezależnych informacji o sytuacji w ich kraju i w krajach byłego ZSRR: 2007 – trwa nadal;
    - TVP Info: „Demaskatorzy”: czerwiec 2023 - grudzień 2023;
    - TVP Info: „Sprawdzamy”: czerwiec 2024 – trwa nadal;
    - TVP Świat: „Anatomia dezinformacji”: wrzesień 2024 – trwa nadal.

- **Wsparcie dla organizacji pozarządowych**: Ministerstwo Spraw Zagranicznych stworzyło projekt grantowy dla NGOs (od 2023) na rzecz przeciwdziałania dezinformacji międzynarodowej (przykład z 2024 roku).

Ewolucja i dynamika działań Polski w zakresie FIMI od 2014 roku pokazuje, że kraj ten stara się reagować na rosnące zagrożenia poprzez rozwój instytucjonalny, legislacyjny i technologiczny. Przyszłe wyzwania związane z dezinformacją będą wymagały dalszej adaptacji i innowacyjnych rozwiązań w tej dziedzinie.

Rola parlamentu w radzeniu sobie z FIMI

Polski parlament, składający się z sejmu i senatu, odgrywa istotną rolę w przeciwdziałaniu Foreign Information Manipulation and Interference (FIMI) poprzez swoje funkcje legislacyjne, nadzorcze oraz polityczne. Oto kluczowe obszary, w których parlament (i jego członkowie) może i powinien odgrywać rolę:

1. Funkcja legislacyjna

Uchwalanie prawa: Polski parlament jest odpowiedzialny za uchwalanie ustaw, które regulują kwestie związane z bezpieczeństwem informacyjnym, cyberbezpieczeństwem oraz ochroną przed zagrożeniami dezinformacyjnymi. To parlament tworzy ramy prawne umożliwiające działanie służbom, instytucjom i agencjom zajmującym się przeciwdziałaniem FIMI.

Nowelizacje prawa: W reakcji na nowe zagrożenia, parlament może wprowadzać nowelizacje istniejących ustaw, dostosowując je do dynamicznie zmieniającego się środowiska informacyjnego oraz technologicznego.

2. Funkcja nadzorcza

Kontrola nad działaniami rządu: Parlament sprawuje nadzór nad działaniami rządu, w tym nad agencjami i służbami zajmującymi się bezpieczeństwem informacyjnym i przeciwdziałaniem dezinformacji. Może to obejmować organizowanie przesłuchań, sesji informacyjnych oraz debat, w których omawiane są działania rządu i efektywność prowadzonych przez niego inicjatyw.

Komisje parlamentarne: Specjalistyczne komisje, takie jak Komisja ds. Służb Specjalnych, Komisja Obrony Narodowej, czy Komisja Administracji i Spraw Wewnętrznych, mają możliwość analizowania działań instytucji krajowych związanych z przeciwdziałaniem FIMI, mogą także przedstawiać swoje rekomendacje dotyczące polityki państwa w tej dziedzinie.

3. Funkcja polityczna

Debata publiczna: Parlament jest forum dla debaty publicznej na temat zagrożeń związanych z FIMI. Przedstawiciele różnych partii politycznych dyskutują o sposobach ochrony polskiej przestrzeni informacyjnej, co może prowadzić do formułowania strategii i polityk państwa.

Wspieranie świadomości społecznej: Poprzez swoje działania, posłowie i senatorowie mogą podnosić świadomość społeczeństwa na temat zagrożeń związanych

z dezinformacją, manipulacjami informacyjnymi i wpływami obcych państw, co ma kluczowe znaczenie w budowaniu odporności społecznej na takie zagrożenia.

4. Zatwierdzanie budżetu

Finansowanie działań: Parlament odgrywa kluczową rolę w zatwierdzaniu budżetu państwa, w tym środków przeznaczonych na działania związane z bezpieczeństwem informacyjnym i cyberbezpieczeństwem. Dzięki temu może wpływać na poziom finansowania instytucji odpowiedzialnych za przeciwdziałanie FIMI.

5. Inicjatywy międzynarodowe

Współpraca międzynarodowa: Poprzez uczestnictwo w międzynarodowych organizacjach parlamentarnych i współpracę z parlamentami innych krajów, polscy parlamentarzyści mogą wspierać i inicjować międzynarodowe działania na rzecz przeciwdziałania dezinformacji i manipulacjom informacyjnym.

6. Odpowiedzialność polityczna

Debaty i interpelacje: Posłowie i senatorowie mogą zadawać pytania rządowi oraz inicjować debaty dotyczące działań związanych z ochroną Polski przed FIMI, co daje społeczeństwu wgląd w działania podejmowane w tej sferze.

7. Inicjatywy edukacyjne

Projekty edukacyjne i społeczne: Parlament może wspierać lub inicjować projekty edukacyjne skierowane do społeczeństwa, mające na celu podniesienie świadomości na temat dezinformacji i zagrożeń związanych z manipulacjami informacyjnymi.

8. Inicjatywy dot. analizy wpływu FIMI na życie społeczne, polityczne i ekonomiczne w Polsce

W ostatnich dwóch latach zostały powołane do życia dwie **następujące po sobie** komisje.

1. Państwowa Komisja do spraw badania wpływów rosyjskich na bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej w latach 2007-2022 (nie funkcjonuje).
2. Państwowa Komisja do spraw badania wpływów rosyjskich i białoruskich w latach 2004-2024 - została powołana na mocy zarządzenia premiera (aktualnie funkcjonująca).

Wszystkie te działania pozycjonują polski parlament jako kluczowego aktora w kształtowaniu polityki i strategii państwa w zakresie ochrony przed zagrożeniami związanymi z FIMI, zarówno na poziomie krajowym, jak i międzynarodowym. Jednocześnie należy ocenić, że powyższe możliwości nie są wykorzystywane na wystarczającym poziomie, a polscy parlamentarzyści nie są zbyt zaangażowani w działania w tym obszarze. Walka z FIMI w parlamencie wciąż postrzegana jest w powszechnej świadomości co najwyżej jako walka z fake newsami, co sprawia, że jest nieskuteczna.

Najważniejsze obszary i narracje po stronie wrogich aktorów

Oto niektóre z najważniejszych działań FIMI, jakie Rosja stosuje przeciwko Polsce:

- Manipulowanie obrazem rosyjskiej agresji na Ukrainę i przedstawianie go jako rzekomej wojny obronnej Rosji przeciwko Zachodowi/NATO;
- Presja psychologiczna przez zastraszanie – szantaż bronią nuklearną;
- Szantaż kryzysem energetycznym;
- Kampanie propagandowe uderzające w wizerunek Wojska Polskiego i polskiej polityki obronnej;
- Manipulowanie historią II wojny światowej;
- Propaganda antynatowska i antyamerykańska;
- Dezinformacja związana z COVID-19;
- Podsycanie napięć społecznych i politycznych;
- Kampanie dezinformacyjne wymierzone w Ukrainę;
- Ataki na polskie media i dziennikarzy;
- Wykorzystywanie kryzysu migracyjnego (mechanizm przymusowej migracji zastosowany przez Rosję i Białoruś przeciwko Polsce i krajom bałtyckim);
- Ataki na polski wizerunek międzynarodowy;
- Wspieranie skrajnej prawicy i lewicy (polaryzacja);
- Podsycanie antyimigranckich nastrojów;
- Wspieranie ruchów antysystemowych.

Wybrane ataki na infrastrukturę cyfrową:

- Atak na infrastrukturę rządową (czerwiec 2021) [przykład].
- Ataki na polskie media i firmy (2022) [przykład 1 i 2].
- Atak na sektor zdrowia (2022) [przykład].
- Atak na systemy infrastruktury krytycznej (2023) [przykład 1 i 2].
- Kampanie phishingowe przeciwko urzędnikom i przedsiębiorcom (2022-2023) [przykład].
- Ataki na sektor transportu kolejowego (2023) [przykład].
- Atak na Polską Agencję Prasową (maj 2024) [przykład].
- Atak hakerów na polską instytucję POLADA - Polska Agencja Antydopingowa (sierpień 2024). Hakerzy wspierani przez służby wrogiego państwa wykradli i opublikowali dane wrażliwe polskich sportowców, łącznie prawie 250 gigabajtów. Atak ten miał stanowić punkt wyjścia do ataków na inne instytucje państwowe [przykład].

Rozwinięcie wskazanych obszarów wrogiej aktywności FIMI znajduję się w załączniku nr 1.

Główne luki wykorzystywane przez wrogie podmioty FIMI

W Polsce, podobnie jak w innych krajach, wrogie podmioty zaangażowane w Foreign Information Manipulation and Interference (FIMI) mogą wykorzystywać specyficzne luki, które są charakterystyczne dla polskiego systemu medialnego, politycznego
i społecznego. Główne luki, które mogą być eksploatowane w Polsce, to:

Polaryzacja polityczna

- **Silne podziały polityczne:** w Polsce istnieje wysoki poziom polaryzacji politycznej, co stanowi dogodny grunt dla szerzenia dezinformacji. Wrogie podmioty mogą wykorzystywać te podziały i emocje, publikując fałszywe informacje, które zaostrzają konflikt pomiędzy różnymi grupami politycznymi i społecznymi.
- Polaryzacja polityczna tyczy się także stosunku danych ugrupowań (a za nimi grup społecznych) do współpracy międzynarodowej i udziału Polski w różnych organizacjach międzynarodowych. Manipuluje się przy tym obrazem obowiązków, powinności, korzyści już istniejących i możliwych do osiągnięcia w czasie przyszłym. A także tym, jakby Polska wyglądała bez obecności w niektórych formatach, np. NATO czy UE.
- **Narracje antyunijne i antyzachodnie:** wrogie podmioty promują narracje krytykujące Unię Europejską, NATO oraz szeroko pojęty Zachód, podważając zaufanie do instytucji międzynarodowych i próbując wpłynąć na postawy społeczne wobec współpracy międzynarodowej**.**

Słabości systemu medialnego

- **Zależność mediów od polityki:** w Polsce część mediów jest związana z określonymi siłami politycznymi, co podgrzewa atmosferę polaryzacji i buduję podziały społeczne a nie więzi. Dezinformacja może być rozpowszechniana, gdy media faworyzujące konkretną narrację polityczną nie weryfikują wystarczająco treści lub celowo nagłaśniają kontrowersyjne tematy.
- **Brak zaufania do mediów:** wysoki poziom nieufności Polaków do mediów i instytucji publicznych sprawia, że wrogie podmioty łatwiej wprowadzają „alternatywny obieg (dez)informacji" i własne narracje, które znajdują oddźwięk wśród podatnych na nie odbiorców i są przez nich kolportowane.

Media społecznościowe i nawyki informacyjne społeczeństwa

- **Szybkie rozpowszechnianie niezweryfikowanych informacji:** w Polsce media społecznościowe, takie jak Facebook, Twitter/X czy TikTok, są głównym kanałem dezinformacji. Specyficzne ekosystemy wprowadzania dezinformacji tworzone są za to na telegramie. Wrogie podmioty mogą manipulować algorytmami tych platform, aby fałszywe treści były szybciej rozprzestrzeniane i miały większy zasięg.

- **Brak efektywnej moderacji treści:** Brak skutecznej moderacji treści w języku polskim na międzynarodowych platformach społecznościowych pozwala na szerzenie dezinformacji bez szybkiej interwencji. Fałszywe informacje mogą krążyć długo, zanim zostaną zidentyfikowane i usunięte.

Narracje związane z bezpieczeństwem

- **Dezinformacja obrazem konfliktu w Ukrainie:** Odwrócona logika pojęć to częsty zabieg manipulacyjny stosowany przez władze na Kremlu. Ma on na celu uprzedzenie oskarżenia i przypisanie własnego działania stronie przeciwnej. W optyce propagandy Kremla to Zachód i Ukraina odpowiedzialne za wojnę, jej przebieg oraz ofiary. Jest to dezinformacja o odpowiedzialności Zachodu i Ukrainy za wojnę, którą rosyjski system propagandy kontynuuje kształtowanie fałszywego obrazu napaści Rosji na Ukrainę.
- **Narracje antyukraińskie:** wrogie podmioty wykorzystują napięcia pomiędzy Polską
  a Ukrainą, bazując na historycznych zaszłościach i współczesnych problemach, aby osłabić solidarność przed rosyjskim neoimperializmem w regionie.
- **Modernizacja i rozbudowa Wojska Polskiego** przedstawiana jest przez wrogie podmioty w fałszywym świetle. Dezinformacja polega na wtłaczaniu opinii publicznej fałszywego przekazu, jakoby Polska szykowała się do działań ofensywnych, wymierzonych w swoich wschodnich sąsiadów jak Białoruś, Rosja czy nawet Ukraina.

Brak edukacji medialnej

- **Niska świadomość w zakresie dezinformacji:** W Polsce, mimo rosnącej świadomości problemu, edukacja medialna nie jest jeszcze wystarczająco powszechna. Społeczeństwo często ma trudności z rozpoznawaniem fałszywych informacji
  i rozróżnianiem wiarygodnych źródeł od manipulacji, co ułatwia wrogim podmiotom szerzenie dezinformacji.
- **Brak narzędzi do weryfikacji informacji:** Chociaż istnieją organizacje fact-checkingowe, ich zasięg nie obejmuje całego społeczeństwa, co pozostawia przestrzeń dla wrogich narracji. Warto podkreślić również, że realne możliwości fact-checking wobec przeciwdziałania FIMI są znacząco ograniczone i nieadekwatne.

Wykorzystanie kryzysów społecznych i gospodarczych

- **Kryzysy gospodarcze i inflacja:** W sytuacji kryzysu gospodarczego, np. wysokiej inflacji czy problemów związanych z rynkiem pracy, wrogie podmioty mogą manipulować faktami, szerząc dezinformację, która zwiększa niepokój społeczny i wywołuje panikę.
- **Pandemia COVID-19:** W czasie pandemii w Polsce rozpowszechniano wiele fałszywych narracji na temat szczepionek, wirusa oraz rządowych restrykcji, co

było aktywnie wykorzystywane przez wrogie podmioty w celu podważenia zaufania do służby zdrowia i instytucji państwowych.

Kwestie migracyjne

- **Dezinformacja na temat uchodźców, migrantów** i brak rozróżnienia jednych i drugich. W szczególności tyczy się to agresji reżimu Aleksandra Łukaszenki (szerzej państwa związkowego Rosji i Białorusi), poniżej progu wojny (hybrid threats/warfare), której celem jest wykreowanie kryzysu humanitarnego aby następnie poprzez obsługę informacyjną (INFO OPS) oraz presję psychologiczną (PSY OPS) osiągać cele i korzyści polityczne, a także finansowe.
- **Kwestie migracyjne** i problemy z nimi związane są wykorzystywane przez rosyjską propagandę do budowy obrazu „upadającej Europy i zgniłego Zachodu". Służy temu hiperbolizacja i fałszywe informacje dotyczące migracji, uchodźców oraz potencjalnych zagrożeń z tym związanych.

Brak spójnej reakcji instytucji

- **Niedostateczna współpraca między instytucjami:** Mimo że w Polsce działają instytucje, które monitorują i walczą z dezinformacją, brakuje efektywnej koordynacji między różnymi podmiotami, w tym rządem, mediami, organizacjami pozarządowymi i platformami społecznościowymi.

Narracje antyamerykańskie

- **Podważanie relacji Polska-USA:** Wrogie podmioty stale próbują podważać współpracę Polski ze Stanami Zjednoczonymi, w szczególności w zakresie bezpieczeństwa i współpracy wojskowej, sugerując, że Polska staje się zależna od USA w sposób, który może jej zaszkodzić.

Użycie historycznych zaszłości

- **Manipulowanie trudną historią:** Wrogie podmioty mogą wykorzystywać historyczne zaszłości, takie jak relacje polsko-rosyjskie czy polsko-ukraińskie, do szerzenia dezinformacji, próbując wzbudzić antagonizmy między Polakami a sąsiadami, co prowadzi do podziałów w regionie.

Powiązania i zbieżności między aktorami FIMI a podmiotami wewnętrznymi

Istnieją powiązania i zbieżności między wewnętrznymi, lokalnymi aktorami a zewnętrznymi podmiotami prowadzącymi działania związane z Foreign Information Manipulation and Interference (FIMI) przeciwko Polsce. W szczególności widać to w kontekście współpracy, świadomej lub nieświadomej, między grupami wewnętrznymi a aktorami zewnętrznymi, którzy dążą do osłabienia stabilności politycznej, społecznej i gospodarczej Polski.

1. Wspólnota interesów

- **Wspólne cele**: Niektóre grupy wewnętrzne w Polsce, w tym ekstremistyczne ruchy polityczne lub organizacje, które mogą działać na marginesie sceny politycznej, mogą mieć cele zbieżne z celami zewnętrznych aktorów. Na przykład, grupy skrajnie prawicowe czy skrajnie lewicowe mogą być zainteresowane destabilizacją systemu politycznego, co jest zgodne z celami FIMI prowadzonymi przez takie państwa jak Rosja.
- **Propagowanie podziałów społecznych**: Zewnętrzni aktorzy FIMI często dążą do pogłębiania podziałów społecznych, co może być korzystne dla niektórych lokalnych grup, które również dążą do polaryzacji społeczeństwa. Takie grupy mogą nieświadomie stawać się narzędziem w rękach zewnętrznych aktorów, realizując ich agendę.

2. Narzędzia i metody współpracy

- **Kampanie dezinformacyjne**: Często lokalne grupy lub media powielają narracje, które są inspirowane lub wręcz pochodzą od zewnętrznych aktorów FIMI. Narracje te mogą być związane z krytyką NATO, UE, migracji, czy też mniejszości narodowych i etnicznych. Zewnętrzni aktorzy FIMI wykorzystują te tematy do wzmacniania podziałów w Polsce.
- **Wykorzystywanie mediów społecznościowych**: Zewnętrzni aktorzy, zwłaszcza Rosja, są znani z wykorzystywania mediów społecznościowych do rozpowszechniania dezinformacji. Lokalni aktorzy, w tym ekstremistyczne grupy, mogą korzystać z tych samych platform do szerzenia podobnych treści, co zwiększa ich zasięg i skuteczność.
- **Finansowanie i wsparcie**: Choć trudno o bezpośrednie dowody, istnieją przesłanki, że niektóre lokalne organizacje mogą otrzymywać wsparcie, bezpośrednie lub pośrednie, od zewnętrznych aktorów. Przykładem mogą być fundusze pochodzące od podmiotów powiązanych z rosyjskimi interesami, które trafiają do organizacji lub mediów promujących narracje zgodne z rosyjską propagandą.

3. Manipulacja informacjami i narracjami

- **Wykorzystanie lokalnych problemów**: Zewnętrzni aktorzy FIMI często wykorzystują istniejące w Polsce problemy społeczne lub polityczne, aby nasilić napięcia. Lokalni aktorzy, zwłaszcza ci, którzy mają radykalne poglądy, mogą wykorzystywać te same narracje, aby zyskać poparcie lub wzmocnić swoje wpływy.
- **Fałszywe konta i boty**: Zewnętrzni aktorzy FIMI, zwłaszcza z Rosji, często korzystają z fałszywych kont i botów w mediach społecznościowych, aby wzmocnić lokalne narracje. Te same narracje są następnie podchwytywane przez lokalnych aktorów, co tworzy iluzję szerokiego poparcia dla pewnych poglądów / dezinformacji.

4. Ekstremizmy i radykalizacja

- **Skrajna prawica i lewica**: Grupy skrajnie prawicowe i lewicowe, środowiska antysystemowe w Polsce mogą być inspirowane lub bezpośrednio wspierane przez zewnętrznych aktorów.
- **Narracje antyzachodnie**: Lokalni aktorzy, którzy promują antyzachodnie narracje, często zbieżne z propagandą rosyjską, mogą nieświadomie (lub świadomie) wspierać cele FIMI. Takie narracje mogą być związane z krytyką NATO, Unii Europejskiej, czy Stanów Zjednoczonych lub zniechęcania do stawiania oporu rosyjskiej polityce agresji.

5. Przykłady konkretnych przypadków

- **Narracje antyszczepionkowe**: Podczas pandemii COVID-19, zewnętrzni aktorzy FIMI, w szczególności Rosja, intensyfikowali kampanie dezinformacyjne na temat szczepionek. W Polsce lokalne grupy antyszczepionkowe często powielały te same fałszywe informacje, co wskazuje na zbieżność interesów.
- **Dezinformacja dotycząca konfliktu na Ukrainie**: Rosja intensywnie propaguje fałszywe informacje na temat wojny na Ukrainie, a niektóre polskie media lub organizacje bliskie skrajnej prawicy lub lewicy powielają te narracje, co sugeruje współzależność między lokalnymi a zewnętrznymi aktorami.

Podsumowanie

- **Złożoność powiązań**: Powiązania między wewnętrznymi a zewnętrznymi aktorami prowadzącymi FIMI przeciwko Polsce są skomplikowane i często subtelne. Mogą obejmować wspólne cele, korzystanie z tych samych narzędzi i metod, a także bezpośrednie lub pośrednie wsparcie finansowe i organizacyjne.
- **Znaczenie monitorowania**: Kluczowe jest monitorowanie tych powiązań, aby lepiej rozumieć, w jaki sposób zewnętrzne operacje informacyjne mogą

wpływać na wewnętrzne procesy polityczne i społeczne w Polsce. Zidentyfikowanie i przeciwdziałanie tym powiązaniom wymaga współpracy różnych instytucji państwowych, organizacji pozarządowych, sektora prywatnego oraz społeczeństwa obywatelskiego.

Czy wsparcie dla Ukrainy jest zagrożone na poziomie krajowym i społecznym?

Choć wsparcie dla Ukrainy na poziomie politycznym w Polsce pozostaje stabilne, wsparcie społeczne może być zagrożone ze względu na kilka kluczowych czynników:

- **Kampanie dezinformacyjne** są jednym z głównych narzędzi, które osłabiają wsparcie społeczne dla Ukrainy. Wrogie podmioty, takie jak Rosja, aktywnie szerzą fałszywe informacje, które mają na celu wzbudzanie niechęci wobec Ukrainy oraz destabilizację relacji polsko-ukraińskich.
- **Polaryzacja polityczna:** mimo że wsparcie dla Ukrainy na poziomie politycznym nie jest bezpośrednio zagrożone, spory między polskimi siłami politycznymi mogą wpływać na to, jak temat ten jest przedstawiany w debacie publicznej. Wrogie podmioty mogą wykorzystywać te spory, aby zaostrzać podziały i podważać konsensus polityczny wokół pomocy Ukrainie.
- **Brak efektywnej komunikacji i współpracy w rozwiązywaniu trudnych tematów** (np. kwestii historycznych, gospodarczych, czy związanych z rolnictwem) otwiera przestrzeń dla dezinformacji. Wrogie grupy mogą zagospodarować sporne tematy, co dodatkowo komplikuje percepcję wsparcia społecznego dla Ukrainy w Polsce.
- Z czasem społeczeństwo może wykazywać **zmęczenie wsparciem dla Ukrainy**, zwłaszcza w obliczu problemów wewnętrznych, takich jak inflacja, kryzys energetyczny, czy inne trudności gospodarcze. Dezinformacja może wykorzystywać te problemy, podsycając poczucie, że Polska powinna bardziej skoncentrować się na własnych problemach, zamiast angażować się w pomoc dla Ukrainy.

Aby utrzymać wysokie poparcie społeczne, konieczne są skuteczniejsze działania w zakresie **edukacji medialnej**, zwiększenie odporności społeczeństwa na manipulacje oraz bardziej spójna **strategia komunikacyjna** między Polską a Ukrainą.

Nowe zagrożenia informacyjne w przyszłości w perspektywie najbliższych 2-5 lat – wybory, AI, cyberbezpieczeństwo ?

W nadchodzących latach Polska będzie musiała stawić czoła nowym i rozwijającym się zagrożeniom informacyjnym, które obejmują zaawansowane technologie, manipulację wyborami, wyzwania związane z migracją oraz rosnące ryzyko cyberataków. Konieczne będą zintegrowane i innowacyjne podejścia do ochrony przed operacjami informacyjnymi i psychologicznymi. Rozbudowa systemu cyberbezpieczeństwa, budowa dedykowanych zespołów bezpieczeństwa przestrzeni informacyjnej a także skuteczne strategie komunikacyjne i współpraca międzynarodowa, aby zabezpieczyć integralność demokracji i stabilność społeczną Polski i krajów Zachodu.

Patrząc w przyszłość, Polska będzie musiała stawić czoła kilku istotnym zagrożeniom informacyjnym, które mogą znacząco wpłynąć na stabilność kraju w perspektywie najbliższych 2-5 lat. Oto główne z nich:

- **Manipulacje wyborcze**: Wybory prezydenckie w Polsce i USA będą celem intensywnych kampanii dezinformacyjnych. Fałszywe informacje o nieprawidłowościach wyborczych, próby podważenia wyników wyborów i zniechęcanie do głosowania mogą być stosowane w celu podważenia legitymacji demokratycznych procesów.
- **Działania (dez)informacyjne związane z relokacją migrantów do Polski**. Obszar ten na pewno będzie wykorzystywany przez wrogie podmioty i polskie instytucje państwowe powinny zawczasu być na to przygotowane.
- **Sianie dezinformacji do krajów Globalnego Południa**: Rozprzestrzenianie dezinformacji do krajów Globalnego Południa na temat Polski i budowa fałszywego obrazu Polski może prowadzić do wzrostu napięć oraz zakłócać interesy RP w regionie oraz nastawiać wrogo migrantów jeszcze przed przybyciem do Polski czy szerzej Europy.
- **Deepfake i Deepporn**: Technologia deepfake może być wykorzystywana do tworzenia realistycznych, ale fałszywych materiałów wideo i audio, co może prowadzić do poważnych nadużyć i kompromitacji publicznych osób. Deepporn, czyli fałszywe materiały pornograficzne, mogą być używane do szantażu lub kompromitacji.
- **Zautomatyzowane bootnety**: Rozwój bardziej zaawansowanych bootnetów, które mogą generować i rozpowszechniać dezinformację w wielu językach, z lepszym tłumaczeniem i bardziej spersonalizowanymi treściami.
- **Masowe generowanie treści przez AI**: Zautomatyzowane systemy generowania treści mogą być wykorzystywane do produkcji i rozpowszechniania dużych ilości dezinformacji, co sprawi, że rozpoznawanie fałszywych informacji będzie trudniejsze.
- **Spoofing**: Techniki takie jak spoofing głosu, numerów telefonów i wizerunku mogą być używane do przeprowadzania oszustw, szantażu i manipulacji, co może wpływać na prywatność i bezpieczeństwo osób publicznych i prywatnych.

- **Ataki na zasoby danych i kompromitacja systemów**: Operacje takie jak „ghostwriter” czy działania typu hack and leak mogą obejmować ataki na dane osobowe i kompromitację komunikacji, co może prowadzić do wykorzystania tych danych w celu szerzenia dezinformacji i wpływania na opinię publiczną.
- **Podziały społeczne**: Wrogie podmioty będą intensyfikować polaryzację społeczną, zwłaszcza poprzez wykorzystywanie kwestii takich jak migracja, bezpieczeństwo, czy kwestie historyczne, aby pogłębiać podziały i wprowadzać chaos w społeczeństwie.
- **Osłabienie sojuszy międzynarodowych**: Wrogie podmioty będą kontynuować kampanie dezinformacyjne mające na celu osłabienie sojuszy międzynarodowych, takich jak NATO, poprzez tworzenie fałszywych narracji dotyczących zdolności obronnych i współpracy wojskowej.
- **Kontynuacja i możliwa eskalacja działań na granicy Polsko – Białoruskiej.**
- **Zwiększona aktywność wywiadowcza.** Więcej szpiegów typu Pablo Gonzalez na europejskich salonach, mających za zadanie zinfiltrować, wprowadzać podziały i zdyskredytować środowiska opiniotwórcze, w tym dziennikarskie.
- **Zwiększona aktywność informacyjno - psychologiczna Rosji, Białorusi i Chin,** w tym przy zastosowaniu środków aktywnych, wywiadu i działań specjalnych.

Jakich rozwiązań obecnie brakuje na poziomie prawnym, instytucjonalnym, społecznym i międzynarodowym w Polsce?

W Polsce brakuje rozwiązań w zakresie prawodawstwa, strategii instytucjonalnej, edukacji i współpracy społecznej oraz koordynacji międzynarodowej w walce z dezinformacją i zagrożeniami FIMI. Kluczowe jest opracowanie i wdrożenie skutecznych przepisów prawnych, poprawa koordynacji między rządem a NGO, zwiększenie inwestycji w zwalczanie dezinformacji oraz rozwijanie edukacji medialnej. Zintegrowane podejście na poziomie krajowym i międzynarodowym jest niezbędne do skutecznej obrony przed rosnącymi zagrożeniami informacyjnymi. Główne obszary wymagające pilnego zagospodarowania to:

1. **Niedostateczny cel instytucjonalny**
   Wymagane jest ujednolicenie i rozbudowa strategii instytucjonalnej i rządowej w zakresie zwalczania dezinformacji. Konieczne jest opracowanie i wdrożenie długoterminowej strategii przeciwdziałania FIMI na poziomie międzyresortowym.
2. **Brak pamięci instytucjonalnej**
   Niedostateczna kontynuacja działań i strategii związanych z przeciwdziałaniem dezinformacji. Nowe zespoły i instytucje często w zbyt małym stopniu korzystają z wcześniejszych doświadczeń i wypracowanego dorobku administracji i poprzedników.
3. **Szkolenia i kwalifikacje kadr**
   System szkoleń wykwalifikowanych kadr zajmujących się analizą i przeciwdziałaniem dezinformacji wymaga usystematyzowania, rozbudowy i ujednolicenia.
4. **Brak standaryzacji siatki pojęciowej i TTP (techniki, taktyki, procedury)**
   Niedostateczne ujednolicenie standardów i procedur w zakresie zwalczania dezinformacji.
5. **Strategia komunikacji (Stratcom)**
   Wyzwania dla bezpieczeństwa środowiska informacyjnego wymagają doskonalenia komunikacji między rządem a obywatelami w zakresie zagrożeń dezinformacyjnych. Społeczeństwo powinno być systematycznie informowane o sposobach rozpoznawania i reagowania na fałszywe informacje. Stratcom powinien również realizować szeroko rozumianą koordynację działań informacyjnych państwa, jak również przeciwdziałania dezinformacji w kraju i za granicą.
6. **Współdziałanie z organizacjami pozarządowymi**
   Współpraca między państwem a NGO's zajmującymi się edukacją medialną i przeciwdziałaniem dezinformacji powinna być zintensyfikowana i skoordynowana w celu podnoszenia efektywności.
7. **Działania edukacyjne**
   Konieczne jest zwiększenie wysiłków w zakresie edukacji medialnej, szczególnie w szkołach oraz poprzez kampanie informacyjne prowadzone przez różne instytucje państwa zgodnie z ich obszarem odpowiedzialności (np. zdrowie, bezpieczeństwo, polityka międzynarodowa, bezpieczeństwo wewnętrzne).

8. **Legislacja dotycząca FIMI**
   Wymagane jest rozwinięcie przepisów prawnych dotyczących zwalczania dezinformacji i manipulacji informacyjnej. Istniejące przepisy często nie są dostosowane do specyfiki współczesnych zagrożeń, takich jak deepfake czy zautomatyzowane kampanie dezinformacyjne, środki aktywne, operacje informacyjne czy psychologiczne.
9. **Niedostateczne wykorzystywanie istniejących przepisów**
   Istniejące przepisy są często niedostatecznie wykorzystywane lub stosowane w ograniczony sposób. Przykładem może być niska efektywność w stosowaniu prawa wobec dezinformacji związanej z wojną napastniczą czy z działalnością antyszczepionkową.
10. **Brak regulacji dotyczących walki z dezinformacją**:
    Brakuje skutecznych regulacji w zakresie monitorowania i zwalczania fałszywych informacji w mediach. Wprowadzenie przepisów regulujących działania mediów w kontekście dezinformacji, na wzór regulacji w bankowości (AML – wewnętrzne działy kontroli), mogłoby poprawić sytuację.
11. **Niskie nakłady finansowe**
    W Polsce, podobnie jak w innych krajach, istnieje potrzeba zwiększenia nakładów finansowych na walkę z dezinformacją i FIMI. Kluczowe są większe inwestycje w technologie, badania i rozwój oraz wsparcie dla odpowiednich instytucji sektora państwowego i pozarządowego.

W jaki sposób parlament krajowy i Parlament Europejski powinny lepiej zająć się kwestią FIMI?

Aby skuteczniej zwalczać zagrożenia związane z FIMI, zarówno parlament krajowy, jak i Parlament Europejski powinny wprowadzić bardziej spójne i horyzontalne regulacje, które uwzględniają współpracę z sektorem prywatnym, NGO i instytucjami międzynarodowymi, takimi jak NATO. Kluczowe są również lepsze mechanizmy monitorowania, zwiększenie szkoleń oraz skuteczne sankcje wobec podmiotów szerzących dezinformację. Działania w szczególności powinny obejmować:

1. **Planowanie i wizja**

Parlament krajowy powinien wymagać od rządu stworzenia jasnej, długoterminowej strategii przeciwdziałania FIMI. Działania te powinny obejmować wszystkie poziomy władzy, od premiera po prezydenta, z jasno określonymi celami, budżetem i ewaluacją działań.

2. **Ewaluacja i rozliczalność instytucji**

Konieczne jest wdrożenie mechanizmów monitorowania skuteczności działań instytucji publicznych. Parlament powinien regularnie oceniać, czy odpowiednie instytucje dostarczają wyniki w walce z dezinformacją.

3. **Przeciwdziałanie fragmentaryzacji wiedzy**

Parlament powinien wspierać inicjatywy mające na celu lepszą koordynację działań między instytucjami państwowymi. Działania te powinny skupiać się na dzieleniu się wiedzą, unikaniu duplikacji zadań i tworzeniu centralnego ośrodka zarządzającego walką z dezinformacją.

4. **Współpraca z sektorem prywatnym i NGO**

Współpraca między rządem, sektorem prywatnym (zwłaszcza mediami) i organizacjami pozarządowymi powinna być kluczowa. Parlament może promować inicjatywy legislacyjne, które zachęcają do tego rodzaju współpracy, np. poprzez wspólne programy edukacyjne czy badawcze.

5. **Szkolenia i rozwój kadr**

Parlament powinien dążyć do zwiększenia inwestycji w szkolenie kadr, w tym pracowników sektora publicznego i prywatnego, w zakresie rozpoznawania i zwalczania FIMI. Współpraca z NATO mogłaby przynieść szczególną korzyść, zwłaszcza w zakresie szkoleń dotyczących rosyjskich, białoruskich i chińskich metod dezinformacji.

Na poziomie Unii Europejskiej: wzmocnienie przepisów i koordynacji

1. **Horyzontalna regulacja dezinformacji**

Parlament Europejski powinien dążyć do wprowadzenia bardziej kompleksowych (horyzontalnych) regulacji dotyczących walki z dezinformacją, jak to ma miejsce na Malcie. Oznaczałoby to zakaz rozpowszechniania dezinformacji we wszystkich kontekstach, jeśli stwarza ona zagrożenie dla interesu publicznego, zamiast ograniczania przepisów do konkretnych obszarów (wertykalność), jak np. COVID-19.

2. **Ujednolicenie przepisów w UE**

Obecnie różnice w regulacjach dotyczących dezinformacji między państwami członkowskimi UE utrudniają skuteczną koordynację. Parlament Europejski powinien wspierać harmonizację przepisów, tak aby wszystkie kraje miały wspólne standardy i podejścia w walce z FIMI.

3. **Monitorowanie szczelności sankcji**

Parlament Europejski powinien wzmacniać mechanizmy monitorowania skuteczności sankcji wobec mediów dezinformacyjnych, takich jak RT czy Sputnik. RAS (Rapid Alert System) powinien być bardziej efektywny, a państwa członkowskie powinny cyklicznie raportować o działaniach podejmowanych w zakresie zamykania luk, które pozwalają na rozprzestrzenianie rosyjskiej propagandy.

4. **Możliwość składania zażaleń na propagandę w innych krajach**

Powinien powstać formalny mechanizm, umożliwiający krajom członkowskim zgłaszanie przypadków naruszania sankcji lub propagandy dezinformacyjnej w innych krajach UE, z możliwością wyciągania konsekwencji. Przykładami mogą być działania RT w Niemczech czy Hiszpanii.

Obowiązki w zakresie przeciwdziałania dezinformacji

1. **Compliance w mediach**:

Podobnie jak banki są zobowiązane do przeciwdziałania praniu brudnych pieniędzy, media powinny mieć obowiązek posiadania wewnętrznych działów ds. przeciwdziałania dezinformacji. Parlament Europejski mógłby wprowadzić przepisy, które wymagają od mediów stosowania mechanizmów zabezpieczających przed rozpowszechnianiem fałszywych informacji – a w przypadku ich braku, nakładać kary.

2. **Kary za rozpowszechnianie dezinformacji**

Media, które nie stosują odpowiednich zabezpieczeń lub celowo szerzą dezinformację, powinny być poddane wysokim karom finansowym, co będzie działało odstraszająco.

Lepsza wymiana doświadczeń i szkoleń

1. **Współpraca UE-NATO**

Parlament Europejski i NATO powinny zacieśnić współpracę w zakresie wymiany wiedzy i szkoleń dotyczących FIMI. NATO ma bogate doświadczenie w analizowaniu metod stosowanych przez Rosję, Białoruś czy Chiny. UE powinna korzystać z tego potencjału, aby szkolić swoje kadry w zakresie przeciwdziałania zagrożeniom informacyjnym.

Budowanie zdolności obronnych:

1. **Wzmacnianie zdolności krajów UE**

Parlament Europejski powinien wspierać inwestycje w infrastrukturę i technologie służące do monitorowania i zwalczania dezinformacji, zwłaszcza w krajach bardziej narażonych na zagrożenia FIMI. Inicjatywy takie mogłyby być współfinansowane przez fundusze UE.

Konkluzje

Polska jest celem działań związanych z Foreign Information Manipulation and Interference (FIMI), szczególnie ze strony Rosji, Białorusi i Chin. Głównym celem tych operacji jest destabilizacja społeczeństwa, osłabienie zaufania do instytucji demokratycznych, wywołanie niepokojów społecznych i podważenie międzynarodowej pozycji Polski.

Polska zareagowała na zagrożenie FIMI wprowadzając nowe regulacje prawne, np. w zakresie cyberbezpieczeństwa, nowelizując prawo medialne i wspierając międzynarodowe inicjatywy w ramach NATO i UE. Instytucje takie jak ABW, MON, MSWiA oraz NASK odgrywają kluczową rolę w przeciwdziałaniu dezinformacji, a niedawno powołano nowe instytucje odpowiedzialne za monitorowanie i przeciwdziałanie zagrożeniom informacyjnym.

Mimo tych kroków, w Polsce wciąż istnieje wiele luk, które wrogie podmioty FIMI mogą wykorzystać. Głównymi wyzwaniami są m.in. polaryzacja polityczna, słabości systemu medialnego, brak edukacji medialnej oraz niedostateczna współpraca instytucji i organizacji pozarządowych w zakresie zwalczania dezinformacji.

Załącznik: odnośnik do rozdziału 8: pogłębione spektrum obszarów aktywności aktorów FIMI w polskiej infosferze

Rosja, kontynuując tradycje sowieckie (tzn. zdolności, wynikające z ciągłości funkcjonowania aparatu bezpieki), stosuje różnorodne środki aktywne przeciwko Polsce, mające na celu destabilizację społeczną, podważanie zaufania do instytucji demokratycznych oraz osłabienie pozycji Polski na arenie międzynarodowej. Wykorzystuje do tego następujące działania:

1. Dezinformacja i propaganda

- **Kampanie dezinformacyjne:** Rosja prowadzi intensywne kampanie dezinformacyjne, mające na celu wprowadzenie zamieszania i polaryzację społeczeństwa oraz tworzenie błędnej oceny sytuacji w szerokim spektrum działań propagandowych i manipulacyjnych.

W ostatnich latach Rosja prowadziła szereg działań propagandowych wymierzonych w Polskę, mających na celu destabilizację społeczną, podważanie zaufania do instytucji demokratycznych, manipulowanie historią oraz osłabienie pozycji Polski na arenie międzynarodowej. Oto kilka kluczowych przykładów:

- **Manipulowanie historią II wojny światowej**

Narracje obwiniające Polskę: Rosja regularnie podejmowała próby przekształcania narracji historycznych dotyczących II wojny światowej, szczególnie w kontekście wybuchu wojny oraz paktu Ribbentrop-Mołotow. Rosyjskie władze i media wielokrotnie oskarżały Polskę o współodpowiedzialność za wybuch wojny, twierdząc, że Polska rzekomo współpracowała z nazistowskimi Niemcami.

Kwestia wyzwolenia Polski: Rosyjska propaganda podkreślała rolę Armii Czerwonej jako wyzwolicieli Polski, ignorując przy tym zbrodnie sowieckie, takie jak zbrodnia katyńska, deportacje Polaków na Syberię oraz okupację wschodnich terenów Polski po wojnie.

- **Propaganda antynatowska i antyamerykańska**

Krytyka obecności wojsk USA i NATO w Polsce: Rosyjskie media i oficjele regularnie krytykowali obecność wojsk NATO i USA w Polsce, przedstawiając to jako zagrożenie dla bezpieczeństwa regionu. Często promowane były narracje sugerujące, że Polska jest marionetką Zachodu, działającą na szkodę swojego bezpieczeństwa narodowego.

Podsycanie antyamerykanizmu: Rosyjska propaganda próbowała wzmacniać nastroje antyamerykańskie w Polsce, sugerując, że Stany Zjednoczone wykorzystują Polskę jako narzędzie do prowadzenia swoich interesów w Europie, kosztem bezpieczeństwa i suwerenności kraju.

- **Dezinformacja związana z COVID-19**

Teorie spiskowe: Rosja promowała teorie spiskowe dotyczące pandemii COVID-19, w tym fałszywe informacje o rzekomym zagrożeniu związanym ze szczepieniami. Celem było wywołanie nieufności wobec polskiego rządu oraz instytucji medycznych i międzynarodowych.

Narracje antyzachodnie: Rosyjskie media promowały przekaz, że Polska i inne kraje zachodnie nie radzą sobie z pandemią, podkreślając rzekomą wyższość modelu zarządzania kryzysowego w Rosji.

- **Podsycanie napięć społecznych i politycznych**

Wykorzystywanie mediów społecznościowych: Rosja angażowała się w kampanie dezinformacyjne na platformach społecznościowych, aby podsycać podziały społeczne i polityczne w Polsce. W tym celu promowano skrajne narracje zarówno z lewej, jak i prawej strony sceny politycznej.

Manipulacja w kwestiach obyczajowych: Rosyjska propaganda próbowała wpływać na polskie społeczeństwo poprzez promowanie kontrowersyjnych tematów obyczajowych, takich jak prawa osób LGBT+, migracja, czy kwestie religijne, w celu wywołania napięć społecznych.

- **Kampanie dezinformacyjne związane z Ukrainą**

Fałszywe informacje o uchodźcach: Rosja rozpowszechniała fałszywe informacje na temat ukraińskich uchodźców w Polsce, sugerując, że stanowią oni zagrożenie dla bezpieczeństwa i gospodarki kraju. Narracje te miały na celu wywołanie niechęci Polaków wobec Ukraińców i destabilizację relacji polsko-ukraińskich.

Sugerowanie konfliktów polsko-ukraińskich: Rosyjskie media wielokrotnie sugerowały, że Polska ma ukryte ambicje terytorialne wobec zachodniej Ukrainy, co miało na celu wywołanie nieufności między Polską a Ukrainą oraz osłabienie sojuszu między tymi krajami.

- **Ataki na polskie media i dziennikarzy**

Dyskredytacja niezależnych mediów: Rosyjskie kampanie propagandowe często atakowały polskie media niezależne, starając się podważyć ich wiarygodność i osłabić ich wpływ na opinię publiczną. Często celem były media krytyczne wobec Rosji lub ujawniające działania rosyjskiego wywiadu.

Promowanie prorosyjskich mediów: Rosja wspierała rozwój i działalność prorosyjskich mediów w Polsce, które miały na celu propagowanie narracji korzystnych dla Kremla.

- **Wykorzystywanie kryzysu migracyjnego (mechanizm przymusowej migracji zastosowany przez Rosję i Białoruś przeciwko Polsce i krajom bałtyckim).**

Narracje antyimigranckie: Podczas kryzysu na granicy polsko-białoruskiej, który został sprowokowany przez Białoruś (blisko związaną z Rosją), rosyjska propaganda starała się

wykorzystać sytuację do wywołania strachu i podziałów w polskim społeczeństwie. Wykorzystywano w tym celu media społecznościowe i kanały propagandowe do szerzenia dezinformacji na temat migrantów i rzekomej brutalności czy wręcz mordów na granicy popełnianych przez polskich funkcjonariuszy, działań polskiego rządu.

- **Ataki na polski wizerunek międzynarodowy**

Dyskredytowanie Polski w Unii Europejskiej: Rosyjska propaganda często starała się podważać wiarygodność Polski jako partnera w Unii Europejskiej, sugerując, że Polska łamie prawa człowieka lub jest państwem nieprzyjaznym wobec swoich sąsiadów.

  - W Polsce Rosja próbowała podsycać antyeuropejskie nastroje w celu osłabienia więzi między Polską a Unią Europejską oraz prowokować napięcia między Polską a innymi państwami członkowskimi.
  - Polska od wielu lat jest przedstawiana w rosyjskiej i białoruskiej propagandzie jako niestabilne, agresywne państwo odpowiedzialne za degradację międzynarodowego systemu bezpieczeństwa. W tym celu wykorzystuje się nie tylko dezinformację historyczną sugerującą współudział Polski w wywołaniu II wojny światowej, ale także współczesne narracje dezinformacyjne, które przedstawiają Polskę jako państwo przygotowujące się do ataku na Rosję lub Białoruś, lub jako nieludzkie, gdzie wykorzystuje tematy dezinformacyjne poprzez kampanie dezinformacyjne dotyczące przemocy (a nawet morderstw) polskich urzędników wobec nielegalnych imigrantów w oparciu o mechanizm przymusowej migracji stosowany przeciwko Polsce [więcej tutaj].
  - Rosyjska propaganda przedstawia Polskę jako państwo dążące do zniszczenia Białorusi [więcej tutaj].
  - Historyczne kłamstwa i współczesna propaganda - Kreml dezinformuje o polskim imperializmie [więcej tutaj].
  - Wybrane aspekty propagandy Aleksandra Łukaszenki na podstawie wywiadu dla Rossiya-1 w kontekście obecnej kampanii propagandowej prowadzonej przez Rosjan w sieciach społecznościowych [więcej tutaj].
  - W Polsce i krajach bałtyckich rosyjskie ośrodki propagandowe regularnie przypisują rusofobię jako główną motywację do przeciwstawiania się rosyjskiemu neoimperializmowi. Od 2014 roku rusofobia przestała być terminem używanym wyłącznie do opisu zjawisk ksenofobicznych, a stała się narzędziem budowania przekazu propagandowego. Termin rusofobia coraz częściej pojawia się w publikacjach głównych mediów wspierających dystrybucję rosyjskiej propagandy i na stałe wpisał się w kanon rosyjskiej propagandy. na stałe do kanonu rosyjskiej publicystyki propagandowej [więcej tutaj].

Podsumowanie: działania propagandowe Rosji przeciwko Polsce mają na celu destabilizację wewnętrzną, osłabienie pozycji międzynarodowej oraz wpływanie na decyzje polityczne. W odpowiedzi na te działania Polska i jej partnerzy podejmują działania w celu wzmocnienia odporności na dezinformację, edukacji społeczeństwa

oraz rozwijania współpracy międzynarodowej w zakresie bezpieczeństwa informacyjnego.

2. Wspieranie ekstremizmów i podziały społeczne

Podsycanie konfliktów wewnętrznych: Rosja aktywnie wspiera narracje, które mogą prowadzić do polaryzacji społeczeństwa polskiego, na przykład poprzez prowokacje i inspirowanie skrajnych ugrupowań politycznych, zarówno z prawej, jak i lewej strony sceny politycznej.

Działania na rzecz radykalizacji: Wykorzystywanie mediów społecznościowych do promowania skrajnych ideologii i wzmacniania istniejących napięć, np. w kwestiach związanych z migracją.

Rosja w ostatnich latach podejmowała działania mające na celu wspieranie i promowanie ekstremizmów w Polsce, zarówno na skrajnej prawicy, jak i na skrajnej lewicy. Działania te miały na celu destabilizację społeczną, pogłębianie podziałów politycznych oraz osłabianie zaufania do instytucji demokratycznych. Oto niektóre z przykładów:

- **Wspieranie skrajnej prawicy**

Narracje nacjonalistyczne: Rosja promowała nacjonalistyczne i ksenofobiczne narracje, często skierowane przeciwko mniejszościom narodowym, imigrantom, czy społecznościom LGBT+. Celem było wywołanie podziałów w społeczeństwie oraz wzmacnianie skrajnych postaw wśród Polaków.

Dezinformacja i propaganda antyukraińska: Rosja starała się wspierać skrajne grupy prawicowe poprzez rozpowszechnianie dezinformacji antyukraińskiej, która miała na celu podsycanie wrogości wobec ukraińskich migrantów w Polsce. Narracje te były szczególnie silne w kontekście konfliktu na wschodzie Ukrainy i kryzysu migracyjnego związanego z wojną.

Narracje antysemickie: Rosyjskie media i kanały propagandowe czasami podsycały antysemickie sentymenty, próbując wpłynąć na grupy nacjonalistyczne i ekstremistyczne w Polsce, które mogłyby wykorzystywać te narracje do mobilizacji swoich zwolenników.

- **Wspieranie skrajnej lewicy**

Promowanie antykapitalizmu i antyglobalizmu: Rosja starała się również oddziaływać na skrajną lewicę, promując narracje antykapitalistyczne i antyglobalistyczne. W tym celu Rosja wspierała grupy i inicjatywy, które przeciwstawiały się globalizacji, neoliberalizmowi, a także instytucjom takim jak Unia Europejska czy NATO, przedstawiając je jako narzędzia opresji.

Manipulacja w kwestiach społecznych: Rosyjskie działania dezinformacyjne obejmowały również kwestie społeczne, takie jak prawa pracownicze, dostęp do opieki zdrowotnej czy kryzys mieszkaniowy. Poprzez wspieranie radykalnych ruchów

lewicowych, Rosja próbowała wzbudzać niezadowolenie społeczne i wprowadzać zamieszanie polityczne.

- **Podsycanie antyimigranckich nastrojów**

Dezinformacja dotycząca kryzysu migracyjnego: Rosja aktywnie promowała fałszywe informacje na temat migrantów, ich rzekomego cierpienia na granicy, zwłaszcza w kontekście sterowanego przez białoruskie służby kryzysu migracyjnego na granicy polsko-białoruskiej. Celem było podsycanie lęków, empatii i dzielenie polskiego społeczeństwa wokół tematyki uchodźców oraz wywoływanie napięć między Polską a jej sąsiadami, w tym prowadzenie działań dyskredytujących Polskę na arenie międzynarodowej.

Wykorzystywanie skrajnych ruchów do destabilizacji: Rosyjskie kanały propagandowe często wspierały antyimigranckie narracje skrajnej prawicy, sugerując, że Polska jest zalewana przez nielegalnych imigrantów, co ma rzekomo zagrażać bezpieczeństwu narodowemu i tożsamości kulturowej kraju.

- **Wspieranie ruchów antysystemowych**

Propagowanie teorii spiskowych: Rosja wspierała rozwój teorii spiskowych, które miały na celu podważenie zaufania do instytucji rządowych i międzynarodowych. Przykładem może być rozpowszechnianie teorii dotyczących rzekomych manipulacji wyborczych, spisków elit politycznych, czy fałszywych informacji na temat szczepień i pandemii COVID-19.

Wspieranie ruchów antyrządowych: Rosyjskie media i trolle internetowe często wspierały ruchy antyrządowe, próbując wywołać destabilizację polityczną i społeczną w Polsce. Narracje te były kierowane zarówno do skrajnej prawicy, jak i lewicy, w zależności od kontekstu.

- **Podsycanie konfliktów społecznych i politycznych**

Wykorzystywanie protestów społecznych: Rosja próbowała wykorzystywać protesty społeczne w Polsce, takie jak protesty przeciwko rządowi czy ruchy społeczne związane z prawami kobiet, aby podsycać podziały i wzmacniać radykalne nastroje. Narracje propagowane przez Rosję często miały na celu eskalację konfliktów i zwiększenie polaryzacji w społeczeństwie.

Infiltracja i wspieranie skrajnych ugrupowań: Rosja mogła również próbować infiltracji skrajnych ugrupowań politycznych, aby wzmacniać ich pozycję i wpływać na działania w Polsce. Wspieranie takich grup może obejmować zarówno pomoc materialną, jak i propagandową.

Podsumowanie: działania te są częścią szerszej strategii Rosji mającej na celu destabilizację krajów, które uznaje za potencjalne zagrożenie dla swoich interesów, oraz osłabienie ich wewnętrznej spójności i pozycji na arenie międzynarodowej. W odpowiedzi na te zagrożenia Polska i jej partnerzy podejmują działania mające na celu wzmacnianie odporności na ekstremizmy i dezinformację, a także edukację

społeczeństwa w zakresie rozpoznawania i przeciwdziałania manipulacjom informacyjnym.

3. Cyberataki

Ataki na infrastrukturę cyfrową: Rosyjskie grupy hakerskie, często powiązane z państwem, przeprowadzają ataki na polskie instytucje rządowe, media, oraz infrastrukturę krytyczną. Celem tych ataków jest nie tylko kradzież informacji, ale także destabilizacja instytucji.

Rozpowszechnianie złośliwego oprogramowania: Wykorzystywanie ransomware oraz innych rodzajów złośliwego oprogramowania w celu zakłócenia pracy polskich firm i instytucji.

W ostatnich dwóch latach Polska była celem kilku istotnych cyberataków, które miały na celu zakłócenie działania instytucji rządowych, infrastruktur krytycznych, a także prywatnych firm. Poniżej przedstawiam niektóre z najważniejszych cyberataków:

- **Atak na infrastrukturę rządową** (czerwiec 2021). Cel: Instytucje rządowe i politycy.

Opis: W czerwcu 2021 roku polski rząd potwierdził, że doszło do serii cyberataków na konta mailowe polskich polityków, w tym na konto ministra Michała Dworczyka, szefa Kancelarii Prezesa Rady Ministrów. Atak ten polegał na przejęciu konta i upublicznieniu zawartości prywatnej korespondencji. Podejrzewa się, że za atakami stały grupy hakerskie związane z Rosją, takie jak UNC1151, które miały na celu destabilizację polskiej sceny politycznej i wywołanie zamieszania społecznego.

Skutki: Upublicznienie prywatnych i służbowych wiadomości oraz podważenie zaufania do bezpieczeństwa systemów komunikacyjnych polskiego rządu.

- **Ataki na polskie media i firmy** (2022-23). Cel: Media, firmy prywatne oraz instytucje finansowe.

Opis: W marcu 2022 r. grupa Killnet, do której należą inne nieustrukturyzowane grupy hakerów sympatyzujące z Rosją, przeprowadziła atak DDoS na stronę internetową polskiego Sądu Najwyższego. Ofiarami ataków grupy padły również strony internetowe ośmiu polskich lotnisk, Narodowego Banku Polskiego (NBP) i innych podmiotów rządowych, a także firm prywatnych (w tym Castorama, Orange i mBank).

W kwietniu 2022 r. rosyjska grupa hakerska Killnet próbowała zakłócić działalność Zakładów Chemicznych Police, należących do Grupy Azoty w celu spowodowania eksplozji w zakładach chemicznych. Chociaż szkody zostały opanowane, atak podkreśla ciągłe zagrożenie dla Grupy Azoty, drugiego co do wielkości producenta nawozów w UE i innych kluczowych branż. W październiku 2022 r. poważny cyberatak naraził na szwank systemy Krajowej Rady Komorniczej.

W 2023 r. doszło do kilku ataków na polskie media i firmy (Niezależna.pl, Wpolityce.pl, Rp.pl, Se.pl, Wyborcza.pl, Polityka.pl, Wprost.pl, Ceneo.pl) mających na celu zakłócenie ich działalności i kradzież danych. Przykładem może być atak na serwery jednego z największych polskich portali informacyjnych. W przypadku firm ataki często przybierały formę ransomware, gdzie hakerzy blokowali dostęp do firmowych systemów, żądając okupu za ich odblokowanie.

Skutki: Utrudnienia w działalności firm, utrata danych, a także konieczność poniesienia znacznych kosztów związanych z odbudową systemów i ochroną przed przyszłymi atakami.

- **Atak na sektor zdrowia** (2022), Cel: Służba zdrowia, w tym szpitale.

Opis: W 2022 roku przeprowadzono cyberatak na kilka polskich szpitali, który spowodował czasowe paraliże ich systemów komputerowych. Atak miał charakter ransomware, co skutkowało zablokowaniem dostępu do kluczowych systemów medycznych, co z kolei wpłynęło na funkcjonowanie placówek i opóźnienia w świadczeniu usług zdrowotnych.

Skutki: Utrudnienia w działaniu szpitali, opóźnienia w leczeniu pacjentów oraz konieczność podjęcia działań naprawczych.

- **Atak na systemy infrastruktury krytycznej** (2023), Cel: Infrastruktura energetyczna i transportowa.

Opis: W 2023 roku odnotowano kilka prób ataków na infrastrukturę krytyczną w Polsce, w tym na sieci energetyczne i systemy transportowe. Jednym z poważniejszych przypadków była próba zakłócenia działania sieci energetycznej, która jednak została skutecznie zneutralizowana przez polskie służby cyberbezpieczeństwa.

Skutki: Choć atak został udaremniony, incydent ten podkreślił zagrożenia związane z cyberatakami na infrastrukturę krytyczną i wymusił zwiększenie nakładów na cyberobronę w tych sektorach.

- **Kampanie phishingowe przeciwko urzędnikom i przedsiębiorcom** (2022-2023) Cel: Urzędnicy, przedsiębiorcy i instytucje finansowe.

Opis: W ciągu ostatnich dwóch lat odnotowano wzrost liczby kampanii phishingowych wymierzonych w polskich urzędników, przedsiębiorców oraz instytucje finansowe. Kampanie te miały na celu wyłudzanie danych uwierzytelniających, które mogłyby być później wykorzystane do bardziej zaawansowanych ataków, takich jak kradzież tożsamości czy ataki na systemy bankowe.

Skutki: Straty finansowe oraz zwiększenie obaw dotyczących bezpieczeństwa wśród użytkowników instytucji finansowych.

- **Ataki na sektor transportu kolejowego** (2023) Cel: Sieć kolejowa.

Opis: W 2023 roku odnotowano cyberataki na polską infrastrukturę kolejową, które miały na celu zakłócenie systemów sterowania ruchem kolejowym. Choć ataki nie

spowodowały większych szkód, podkreśliły one znaczenie zabezpieczeń w sektorze transportu.

Skutki: Podjęcie dodatkowych środków bezpieczeństwa oraz wzmożona kontrola i audyt systemów IT w sektorze transportowym.

Podsumowanie: te cyberataki są częścią szerszej strategii mającej na celu osłabienie Polski i innych krajów w regionie. Skutki tych ataków podkreślają potrzebę ciągłego wzmacniania obrony cybernetycznej oraz współpracy międzynarodowej w zakresie bezpieczeństwa cybernetycznego.

4. Infiltracja polityczna i gospodarcza

Rosja podejmowała różnorodne działania mające na celu infiltrację polityczną i gospodarczą w Polsce. Działania te były skoncentrowane na osłabieniu polskiej suwerenności, wpływaniu na decyzje polityczne, oraz destabilizowaniu polskiej gospodarki i systemu politycznego.

- **Infiltracja polityczna**

Wspieranie prorosyjskich polityków i partii: Rosja starała się wspierać lub nawiązywać kontakty z politykami oraz ugrupowaniami politycznymi w Polsce, które były skłonne prezentować stanowiska prorosyjskie lub eurosceptyczne. Poprzez takie kontakty Moskwa mogła próbować wpływać na decyzje polityczne w Polsce oraz osłabiać proeuropejskie i proatlantyckie nastawienie polskiego rządu.

Finansowanie i wsparcie dla grup ekstremistycznych: Rosja mogła również wspierać radykalne ugrupowania polityczne, które sprzyjały destabilizacji politycznej w Polsce. Wspieranie takich grup miało na celu wprowadzanie chaosu i podziałów na scenie politycznej, co mogło osłabić zdolność polskiego rządu do skutecznego zarządzania krajem.

Propaganda i dezinformacja: Rosja aktywnie prowadziła kampanie dezinformacyjne, które miały na celu manipulowanie opinią publiczną i wpływanie na wyniki wyborów oraz kształtowanie polityki wewnętrznej i zagranicznej Polski. Często wykorzystywano tu media społecznościowe, fałszywe strony internetowe oraz prorosyjskie media działające w Polsce.

- **Infiltracja gospodarcza**

Współpraca gospodarcza z firmami powiązanymi z Rosją: Rosja starała się zacieśniać współpracę gospodarczą z polskimi firmami, szczególnie w sektorach strategicznych, takich jak energetyka, przemysł metalurgiczny, czy sektor finansowy. Poprzez inwestycje, przejęcia lub zakładanie wspólnych przedsiębiorstw, Rosja mogła próbować wywierać wpływ na polski rynek i gospodarkę.

Energetyka jako narzędzie wpływu: Rosja wielokrotnie wykorzystywała dostawy energii, szczególnie gazu ziemnego, jako narzędzie nacisku na Polskę. Poprzez kontrolę nad

dostawami oraz ceny energii, Rosja starała się uzależnić Polskę od swoich surowców energetycznych i tym samym wpływać na politykę energetyczną kraju.

Wykorzystywanie rosyjskich firm jako przykrywek: Niektóre rosyjskie firmy działające w Polsce mogły być wykorzystywane jako przykrywki do działań wywiadowczych lub do korumpowania polskich urzędników i biznesmenów. Tego rodzaju działania mogły obejmować zarówno bezpośrednie działania szpiegowskie, jak i próby zdobycia strategicznych informacji lub wpływu na kluczowe decyzje gospodarcze.

- **Wpływanie na opinię publiczną i elity**

Kreowanie prorosyjskich think tanków i organizacji: Rosja wspierała tworzenie i działalność think tanków, organizacji pozarządowych oraz fundacji, które promowały prorosyjskie narracje i politykę [przykład]. Poprzez te organizacje, Rosja mogła wpływać na polskie elity polityczne i intelektualne, starając się kształtować debatę publiczną w kierunku korzystnym dla swoich interesów.

Zachęcanie do współpracy gospodarczej na dużą skalę: Rosyjscy biznesmeni oraz oligarchowie często starali się nawiązywać współpracę z polskimi przedsiębiorcami i politykami, oferując korzystne umowy lub inwestycje, które miałyby na celu zwiększenie rosyjskiego wpływu w polskiej gospodarce. Takie działania mogły prowadzić do uzależnienia niektórych sektorów polskiej gospodarki od rosyjskiego kapitału.

- **Działania wywiadowcze i szpiegowskie**

Zbieranie informacji strategicznych: Rosyjskie służby wywiadowcze aktywnie zbierały informacje na temat polskich elit politycznych, gospodarczych oraz wojskowych. Tego typu działania miały na celu zdobycie informacji, które mogłyby być wykorzystane do wywierania presji lub szantażu.

Infiltracja instytucji państwowych: Rosja mogła próbować infiltracji polskich instytucji państwowych, aby zdobyć dostęp do poufnych informacji lub wpłynąć na kluczowe decyzje polityczne. Działania te obejmowały zarówno klasyczne metody szpiegowskie, jak i bardziej subtelne formy wpływu, takie jak korumpowanie urzędników.

- **Podsycanie konfliktów regionalnych i etnicznych**

Wykorzystywanie historycznych resentymentów: Rosja mogła próbować podsycać historyczne resentymenty, zwłaszcza w kontekście stosunków polsko-ukraińskich czy polsko-litewskich, aby osłabić pozycję Polski w regionie oraz skomplikować jej relacje z sąsiadami.

Podżeganie do separatyzmu: W przeszłości Rosja próbowała wspierać separatyzm i działania ruchów, które mogłyby osłabić spójność terytorialną Polski lub wprowadzić destabilizację w regionach przygranicznych [przykłady 1 i 2].

Podsumowanie: działania te pokazują, że Rosja konsekwentnie dążyła do osłabienia pozycji Polski zarówno na arenie międzynarodowej, jak i wewnętrznej, wykorzystując szeroką gamę narzędzi, od działań gospodarczych po polityczne i wywiadowcze.

W odpowiedzi na te zagrożenia Polska podejmuje działania mające na celu zwiększenie odporności na zewnętrzne wpływy oraz wzmacnianie współpracy z partnerami międzynarodowymi w zakresie bezpieczeństwa.

5. Rosyjskie i Chińskie operacje wpływu w sferze kultury i edukacji

Rosja i Chiny prowadziły różnorodne operacje wpływu w sferze kultury i edukacji w Polsce, mające na celu promowanie swoich narracji, zwiększanie wpływów politycznych oraz osłabianie więzi Polski z Zachodem. Działania te były częścią szerszych strategii obu krajów mających na celu wywieranie wpływu na opinię publiczną, elity intelektualne oraz młodzież w Polsce.

Operacje wpływu Rosji

Propaganda historyczna i manipulacja pamięci, Kultywowanie fałszywego obrazu rzekomej wspólnej historii: Rosja wspierała organizację wydarzeń kulturalnych i edukacyjnych, które miały na celu promowanie wspólnej, rzekomo pozytywnej historii relacji polsko-rosyjskich, często marginalizując czy wręcz negując negatywne aspekty historii, takie jak okupacja sowiecka czy zbrodnie stalinowskie.

Manipulacja edukacją i kulturą: Wpływanie na polskie środowiska akademickie i kulturalne poprzez propagowanie prorosyjskich narracji oraz próbę budowania prorosyjskiego wizerunku wśród intelektualistów i artystów [przykład].

Sponsoring prorosyjskich inicjatyw: Wspieranie organizacji i wydarzeń, które promują pozytywny wizerunek Rosji w Polsce [przykład].

- **Wsparcie dla prorosyjskich organizacji kulturalnych**

Działalność prorosyjskich stowarzyszeń: Rosja wspierała działalność różnych organizacji i stowarzyszeń kulturalnych w Polsce (Russkij Mir, Rosyjskie Centrum Nauki i Kultury w Warszawie, „Rosyjskie Domy" w Warszawie i Gdańsku), które promowały rosyjską kulturę, język oraz historię. Tego typu organizacje mogły działać jako narzędzia wpływu, szerząc prorosyjskie narracje i starając się kształtować pozytywny wizerunek Rosji wśród Polaków [na przykład: Rossotrudniczestwo - objęte sankcjami].

Propagowanie rosyjskiego języka i kultury: Poprzez finansowanie i organizowanie kursów języka rosyjskiego, wydarzeń kulturalnych oraz współpracy akademickiej, Rosja starała się promować swoją kulturę i wartości w Polsce, szczególnie wśród młodzieży i studentów.

- **Manipulacja edukacją**

Współpraca akademicka i wymiany studenckie: Rosja starała się rozwijać współpracę akademicką z polskimi uczelniami, oferując programy wymiany studenckiej oraz stypendia dla polskich studentów. Celem było promowanie prorosyjskich narracji oraz kształtowanie przyszłych polskich elit, które mogłyby być bardziej przychylne Moskwie.

Infiltracja programów edukacyjnych: Rosyjskie instytucje próbowały wpływać na programy nauczania w Polsce, szczególnie w dziedzinach historii i stosunków międzynarodowych, aby promować rosyjski punkt widzenia.

- **Fundacja Russkij Mir**

Fundacja „Russkij Mir" została założona w 2007 roku z inicjatywy prezydenta Rosji Władimira Putina oraz patriarchy Moskwy i Wszechrusi Aleksego II. Celem fundacji było promowanie rosyjskiej kultury, języka oraz wartości na całym świecie, w tym również w Polsce. Fundacja działała jako narzędzie „miękkiej siły" (soft power) Rosji, mające na celu budowanie prorosyjskiego wizerunku i wpływów w innych krajach.

W Polsce „Russkij Mir" rozwijał swoją działalność poprzez zakładanie centrów kultury, organizowanie kursów języka rosyjskiego oraz wspieranie różnorodnych inicjatyw kulturalnych, głównie na Uniwersytetach. Władzami Fundacji „Russkij Mir" byli rosyjscy urzędnicy państwowi oraz osoby blisko związane z rosyjskim rządem. Działalność fundacji budziła kontrowersje i obawy o propagandowy charakter jej działań, które mogły służyć promowaniu rosyjskich interesów geopolitycznych oraz wpływaniu na opinię publiczną w Polsce. W związku z napięciami na linii Polska-Rosja, działalność fundacji była często postrzegana jako element szerszej strategii „miękkiej siły" Rosji, mającej na celu destabilizację krajów sąsiadujących z Rosją oraz wzmacnianie prorosyjskich sentymentów wśród lokalnej ludności.

Operacje wpływu Chin

- **Instytuty Konfucjusza**

Promowanie języka i kultury chińskiej: Chiny aktywnie rozwijały sieć Instytutów Konfucjusza w Polsce, które miały na celu promowanie języka chińskiego oraz chińskiej kultury. Instytuty te są często postrzegane jako narzędzia "miękkiej siły" Pekinu, mające na celu kształtowanie pozytywnego wizerunku Chin oraz promowanie chińskich wartości i narracji.

Zachęcanie do studiów w Chinach: Chiny oferowały liczne stypendia i programy wymiany dla polskich studentów, zachęcając ich do studiowania w Chinach. Takie programy miały na celu nie tylko edukację, ale także kształtowanie przyszłych elit przychylnych chińskim interesom.

- **Współpraca edukacyjna i naukowa**

Partnerstwa między uczelniami: Chiny rozwijały partnerstwa z polskimi uczelniami, oferując współpracę w dziedzinie nauki i technologii. Tego typu partnerstwa mogły być wykorzystywane do wpływania na badania i programy edukacyjne, promując chińskie podejście do nauki i technologii.

Programy wymiany akademickiej: Chiny organizowały programy [np. Warsaw-Beijing Forum] wymiany dla polskich akademików, naukowców i studentów, oferując im

możliwości prowadzenia badań i nauki w Chinach. Celem było nie tylko edukowanie, ale także kształtowanie światopoglądu i przekonań przyszłych liderów nauki i polityki.

- **Propaganda kulturalna**

Wydarzenia kulturalne i festiwale: Chiny organizowały w Polsce liczne wydarzenia kulturalne, takie jak festiwale filmowe, wystawy sztuki czy koncerty, które miały na celu promowanie chińskiej kultury oraz budowanie pozytywnego wizerunku Chin.

Współpraca z mediami: Chiny nawiązywały współpracę z polskimi mediami, oferując im dostęp do chińskich treści kulturalnych i edukacyjnych. W niektórych przypadkach mogło to prowadzić do promowania prorządowych narracji Pekinu w polskiej przestrzeni medialnej.

- **Szpiegostwo i presja technologiczna**

Chiny wdrażają wywiad gospodarczy i technologiczny przy użyciu szerokiego spektrum narzędzi. Jedną z technik jest zakulisowe wprowadzanie informacji ekonomicznych pochodzących i działających na rzecz Chińskich podmiotów gospodarczych. Przykładem dobrze ilustrującym tego typu technikę wywiadowczą jest zatrzymanie w Polsce pod zarzutami szpiegostwa dyrektora chińskiego konglomeratu technologicznego (Huawei) [więcej tutaj i tutaj]. Potencjał nadużywania chińskich firm i technologii do operacji wywiadowczych jest wysoki ze względu na chiński system prawny i bliskie relacje między rządem, służbami a przedsiębiorstwami. Agresywny marketing chińskich technologii przez chińskie korporacje dodatkowo zaostrza to ryzyko, ponieważ zwiększa możliwości infiltracji infrastruktury krytycznej za pomocą systemów, którym nie można ufać [przykład 1 i 2].

Podsumowanie: operacje wpływu Rosji i Chin w Polsce w sferze kultury i edukacji były częścią szerszych strategii obu krajów mających na celu wywieranie wpływu na społeczeństwo, elity intelektualne oraz decyzje polityczne. Poprzez działania te Rosja i Chiny starały się kształtować opinię publiczną i promować swoje interesy, często wykorzystując narzędzia "miękkiej siły", takie jak kultura, język, edukacja i współpraca naukowa.

6. Manipulacja mediów

Rosja i Chiny w ostatnich latach prowadziły szeroko zakrojone kampanie manipulacyjne w mediach, które miały na celu wpływanie na polską opinię publiczną, destabilizowanie społeczeństwa, a także promowanie własnych interesów politycznych i gospodarczych. Działania te obejmowały szeroki wachlarz metod, od klasycznej propagandy, przez dezinformację, po subtelne formy manipulacji treściami medialnymi. Oto przegląd takich działań.

Tworzenie i wspieranie prorosyjskich mediów: Rosja inwestuje w media, które promują prorosyjskie narracje w Polsce, a także używa kanałów międzynarodowych, takich jak RT (Russia Today) i Sputnik, aby szerzyć swoje wersje wydarzeń.

Ataki na niezależne media: Próby dyskredytowania i osłabiania niezależnych mediów w Polsce, które krytycznie odnoszą się do polityki Kremla.

Rosyjska manipulacja mediów

- **Dezinformacja i fałszywe wiadomości**

Kampanie dezinformacyjne: Rosja aktywnie wykorzystywała media społecznościowe, blogi oraz portale informacyjne do rozpowszechniania fałszywych wiadomości i teorii spiskowych, które miały na celu destabilizowanie polskiego społeczeństwa. Przykłady obejmują fałszywe informacje na temat kryzysu migracyjnego, pandemii COVID-19 czy polityki zagranicznej Polski [przykład].

Narracje antyukraińskie: Rosja prowadziła intensywną kampanię dezinformacyjną skierowaną przeciwko ukraińskiej społeczności w Polsce oraz przeciwko polsko-ukraińskim relacjom. Narracje te często koncentrowały się na podsycaniu historycznych resentymentów i wzbudzaniu nieufności wobec ukraińskich imigrantów [przykład].

- **Propaganda prorosyjska**

Działalność prorosyjskich mediów w Polsce: Rosja wspierała i promowała media, które prezentowały prorosyjskie stanowisko, w tym portale informacyjne i blogi [rosyjskie modus operandi]. Tego rodzaju media często publikowały treści zgodne z linią propagandową Kremla, przedstawiające Rosję w pozytywnym świetle i krytykujące działania NATO, UE oraz polskiego rządu.

Wzmacnianie skrajnych postaw: Rosyjskie media manipulowały przekazami, które miały na celu wzmacnianie skrajnych postaw w Polsce, w tym eurosceptycyzmu, nacjonalizmu oraz wrogości wobec Stanów Zjednoczonych i Zachodu. Tego rodzaju narracje były często promowane w kontekście wyborów, protestów społecznych czy debat politycznych.

- **Ataki na polskie instytucje**

Podważanie zaufania do rządu: Rosyjskie kampanie dezinformacyjne często koncentrowały się na podważaniu zaufania do polskich instytucji państwowych, w tym rządu, wojska oraz służb specjalnych. Przykłady obejmują rozpowszechnianie fałszywych informacji na temat rzekomych skandali korupcyjnych, nieudolności władz czy rzekomej uległości wobec USA.

Ataki na procesy wyborcze: W okresach wyborczych Rosja prowadziła kampanie dezinformacyjne, mające na celu wywoływanie chaosu informacyjnego i podważanie wiarygodności procesów wyborczych w Polsce. Tego typu działania mogły obejmować rozpowszechnianie fałszywych informacji na temat fałszerstw wyborczych lub manipulowania wynikami.

Chińska manipulacja mediów

- **Kreowanie pozytywnego wizerunku Chin**

Propaganda sukcesu: Chińskie media oraz powiązane z Pekinem instytucje aktywnie promowały narracje [przykład] przedstawiające Chiny jako kraj sukcesu gospodarczego i technologicznego, oferujący atrakcyjną alternatywę dla modelu zachodniego. Tego rodzaju treści były często promowane w polskich mediach poprzez artykuły sponsorowane, wywiady czy reportaże.

Współpraca z polskimi mediami: Chiny starały się nawiązywać współpracę z polskimi mediami, oferując im dostęp do chińskich treści i materiałów, które promowały chińską kulturę, politykę oraz gospodarkę. Współpraca ta często obejmowała wymianę dziennikarzy, wspólne projekty medialne oraz wsparcie finansowe.

- **Cenzura i kontrola narracji**

Manipulacja informacjami na temat Chin: Chiny aktywnie starały się kontrolować narracje dotyczące swojego kraju w polskich mediach [przykład], wywierając presję na redakcje i dziennikarzy, aby unikały krytycznych treści dotyczących np. sytuacji w Xinjiangu, Hongkongu czy kwestii praw człowieka. W niektórych przypadkach mogło dochodzić do prób cenzurowania lub usuwania niekorzystnych dla Chin artykułów.

Ograniczanie dostępu do niezależnych źródeł informacji: Chiny starały się ograniczać dostęp polskich mediów i opinii publicznej do niezależnych informacji na temat sytuacji w Chinach, promując jedynie treści zgodne z oficjalną linią partii komunistycznej.

- **Promocja chińskich projektów geopolitycznych**

Inicjatywa Pasa i Szlaku: Chiny intensywnie promowały w Polsce inicjatywę Pasa i Szlaku [przykład], przedstawiając ją jako korzystny dla Polski projekt współpracy gospodarczej i infrastrukturalnej. W tym celu Pekin wykorzystywał zarówno media tradycyjne, jak i cyfrowe, aby przekonywać opinię publiczną i decydentów do wsparcia chińskich inwestycji.

Soft power i wpływ kulturowy: Chiny starały się wykorzystywać narzędzia "miękkiej siły", takie jak kultura i edukacja, aby budować pozytywny wizerunek Chin w Polsce. Przykłady obejmują organizację wydarzeń kulturalnych, promocję języka chińskiego oraz działalność Instytutów Konfucjusza, które miały na celu szerzenie chińskiej kultury i narracji.

- KONIEC -

Autorzy: Maksym Sijer, Wojciech Pokora
info@infoops.pl