TLP:CLEAR

Raport „Parasol Wyborczy - Wybory Prezydenckie 2025”

Ministerstwo Cyfryzacji

Spis Treści

Podsumowanie zarządcze ... 3
Wstęp - kontekst wyborczy i doświadczenia instytucjonalne ... 4
1 Program "Parasol Wyborczy" ... 6
1.1 Cele i zakres działania programu ... 7
1.2 Kontekst bezpieczeństwa narodowego ... 8
1.3 Realizacja programu w praktyce ... 9
1.4 Wyniki wyborów prezydenckich i ocena skuteczności programu ... 10
2 Działania Ministerstwa Cyfryzacji oraz jednostek podległych i nadzorowanych ... 11
2.1 Ministerstwo Cyfryzacji ... 12
2.2 Centralny Ośrodek Informatyki (COI) ... 15
2.1 NASK-PIB ... 17
3 Zaangażowanie krajowych służb kontrwywiadowczych (ABW i SKW) oraz Ministerstwa Spraw Zagranicznych w proces zapewniania bezpieczeństwa wyborczego ... 38
3.1 Agencja Bezpieczeństwa Wewnętrznego (ABW) ... 39
3.2 Służba Kontrwywiadu Wojskowego (SKW) ... 43
3.3 Ministerstwo Spraw Zagranicznych (MSZ) ... 44
4 Technologie anonimizacji w ingerencji wyborczej – analiza wyzwań dla bezpieczeństwa procesów demokratycznych ... 46
5 Wnioski ... 48
Zakończenie ... 52

PODSUMOWANIE ZARZĄDCZE

Raport “Parasol Wyborczy – Wybory Prezydenckie 2025” przedstawia kompleksową analizę działań na rzecz ochrony procesu wyborczego przed zagrożeniami w cyberprzestrzeni, dezinformacją oraz ingerencją zewnętrzną. Wybory w 2025 r. odbyły się w warunkach zwiększonego ryzyka destabilizacji informacyjnej, a ich przebieg stanowił sprawdzian efektywności działań instytucji odpowiedzialnych za bezpieczeństwo państwa i jego obywateli.

“Parasol Wyborczy”, uruchomiony w lutym 2025 r. z inicjatywy Ministerstwa Cyfryzacji (MC) we współpracy z Ministerstwem Spraw Wewnętrznych i Administracji (MSWiA), objął trzy kluczowe obszary: ochronę przed zagrożeniami w cyberprzestrzeni, przeciwdziałanie dezinformacji oraz edukację i współpracę międzyinstytucjonalną. **Raport prezentuje szerokie spektrum działań realizowanych przez kluczowe instytucje: MC, Agencję Bezpieczeństwa Wewnętrznego (ABW), Służbę Kontrwywiadu Wojskowego (SKW), Ministerstwo Spraw Zagranicznych (MSZ), Centralny Ośrodek Informatyki (COI), poszczególne CSIRT-y (zespoły reagowania na incydenty bezpieczeństwa komputerowego) oraz Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (NASK). Połączenie kompetencji tych podmiotów umożliwiło kompleksowe działania zgodnie z wyznaczonymi im ustawowo zakresami zadań.** Wypracowany model współpracy pozwolił na reagowanie w czasie rzeczywistym – m.in. dzięki regularnej komunikacji pomiędzy podmiotami tworzącymi Parasol Wyborczy, uruchomieniu szybkich kanałów komunikacji z komitetami wyborczymi i platformami społecznościowymi oraz systemowi umożliwiającemu obywatelom zgłaszanie dezinformacji poprzez serwis bezpiecznewybory.pl. Szczególną uwagę poświęcono także wykrywaniu i neutralizacji złośliwych kampanii, w tym działań z wykorzystaniem botów oraz fałszywych kont w mediach społecznościowych.

Podkreślenia wymaga praca wykonana przez ABW (m.in. testy systemów teleinformatycznych, szkolenia, wykorzystanie systemu wczesnego ostrzegania o zagrożeniach w sieci ARAKIS-GOV), NASK (m.in. skanowanie podatności systemem ARTEMIS, monitoring wycieków) oraz MC (m.in. działania koordynacyjne Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, centralna ochrona przed atakami DDoS dla administracji publicznej i Wojska Polskiego, we współpracy z COI zapewnianie bezpieczeństwa państwowych systemów oraz aplikacji mObywatel).

Raport podkreśla wyzwania w zakresie przeciwdziałania zagrożeniom cyfrowym – w tym ograniczenia związane z obowiązującymi przepisami prawa i automatyczną detekcją treści noszących znamiona dezinformacji. Wskazuje także na konieczność zapewnienia należytego stosowania unijnego Aktu u usługach cyfrowych (DSA) oraz budowy narodowej odporności cyfrowej poprzez edukację obywateli w zakresie identyfikowania dezinformacji.

Wnioski z realizacji programu “Parasol Wyborczy” potwierdzają, że skuteczna ochrona demokracji w erze cyfrowej wymaga zaawansowanych rozwiązań technologicznych i operacyjnej koordynacji oraz długofalowego podejścia.

WSTĘP - KONTEKST WYBORCZY I DOŚWIADCZENIA INSTYTUCJONALNE

Rok 2025 stanowił szczególnie intensywny okres w kalendarzu wyborczym Rzeczypospolitej Polskiej (RP), będąc kulminacją trzyletniego cyklu demokratycznych procesów wyborczych, które rozpoczęły się w 2023 r. wyborami parlamentarnymi do Sejmu i Senatu. Ta niezwykła koncentracja procesów wyborczych w stosunkowo krótkim okresie - wybory parlamentarne w październiku 2023 r., wybory samorządowe w kwietniu 2024 r., wybory do Parlamentu Europejskiego w czerwcu 2024 r. oraz wybory prezydenckie w maju i czerwcu 2025 r. - spowodowała konieczność zapewnienia większego bezpieczeństwa procesów demokratycznych w cyberprzestrzeni.

Wybory parlamentarne z 15 października 2023 r., charakteryzujące się rekordową frekwencją wynoszącą 74,38% - najwyższą w historii III Rzeczypospolitej - dostarczyły istotnych doświadczeń w zakresie identyfikacji współczesnych zagrożeń o charakterze cyfrowym i dezinformacyjnym. Następnie, wybory samorządowe z 7 kwietnia 2024 r., obejmujące wybory do sejmików województw, rad powiatów i gmin oraz wybory wójtów, burmistrzów i prezydentów miast, pozwoliły na pogłębienie wiedzy na temat skali i charakteru potencjalnych ingerencji zewnętrznych w procesy wyborcze na różnych szczeblach administracji publicznej.

Wybory prezydenckie 2025 r. odbywały się w szczególnie wymagającym otoczeniu krajowym i międzynarodowym, naznaczonym rosnącą skalą cyberataków, intensywnością operacji informacyjnych, dynamicznymi zmianami technologicznymi oraz nasilającą się polaryzacją społeczną. W dobie globalnej rywalizacji strategicznej oraz eskalujących zagrożeń hybrydowych, bezpieczeństwo procesu wyborczego stało się nie tylko kwestią organizacyjną, ale także fundamentalnym elementem odporności państwa. Z tego względu, konieczne było wdrożenie programu, stanowiącego odpowiedź na konkretne zagrożenia identyfikowane w przestrzeni cyfrowej, ale także będącego częścią długofalowej polityki państwa ukierunkowanej na ochronę podstawowych mechanizmów demokracji.

W kontekście przygotowań do wyborów prezydenckich w 2025 r., Ministerstwo Cyfryzacji (MC) podjęło szereg działań profilaktycznych i ochronnych, kierując się uzasadnionymi obawami przed potencjalnymi atakami w cyberprzestrzeni. Działania te były motywowane znaczącym wzrostem napięć geopolitycznych oraz jawnie manifestowaną niechęcią wobec Polski, wynikającą z zaangażowania naszego kraju we wszechstronne wsparcie Ukrainy na płaszczyznach m.in. humanitarnej, politycznej, gospodarczej oraz wojskowej i logistycznej. Polska, będąc kluczowym partnerem Ukrainy w regionie, stała się szczególnym celem działań destabilizacyjnych, co potwierdzają dane wskazujące na gwałtowny wzrost incydentów cyberbezpieczeństwa - obecnie rejestruje się ok. 50 tysięcy zgłoszeń miesięcznie.

Szczególne zagrożenie stanowiły (i stanowią) zaawansowane technicznie grupy APT (Advanced Persistent Threat) oraz podmioty wspierane przez państwa, które Rosja i Białoruś posiadają w swoim arsenale cyberprzestrzeni. Grupy te, w tym znane formacje APT28 (powiązana z rosyjskim wywiadem wojskowym, GU/GRU) oraz APT29 (powiązana z rosyjską Służbą Wywiadu Zagranicznego, SWR), charakteryzują się wysokim potencjałem operacyjno-technicznym oraz zdolnościami wywierania wpływu zarówno w sferze informacyjnej, jak

i poprzez działania o charakterze stwarzającym wymiernie negatywne skutki gospodarcze lub kinetyczne w tym np. na systemy dystrybucji wody i energii elektrycznej.

Ministerstwo Cyfryzacji odnotowało również niepokojący wzrost aktywności grup haktywistycznych, które tworzą rozbudowane społeczności wykorzystujące m.in. infrastrukturę do przeprowadzania ataków DDoS. Przykładem jest prorosyjska grupa NoName057(16), która rekrutuje "wolontariuszy" oferując im wynagrodzenie za udział w atakach na infrastrukturę krytyczną oraz obiekty wrażliwe państw zachodnich. Równolegle obserwujemy intensyfikację działań zorganizowanej przestępczości kryminalnej motywowanej finansowo, w tym grup ransomware, których aktywność wykazuje wzrost w okresach rosnących napięć polityczno-społecznych w państwach zachodnich. Prowadzona przez te grupy działalność przestępcza jest zbieżna z celami strategicznych interesów polityki bezpieczeństwa Rosji, co świadczy o ich pośrednim powiązaniu, prawdopodobnie za pośrednictwem służb specjalnych Federacji Rosyjskiej. Potwierdzają to medialne dane wskazujące, że rosyjskie służby oferują od 3000 do 4000 euro za pracę polegającą na rozpowszechnianiu dezinformacji w okresie przedwyborczym.

W odpowiedzi na te zagrożenia, MC wraz z partnerami wdrożyło program "Parasol Wyborczy", mający na celu ochronę procesu wyborczego przed zagrożeniami w cyberprzestrzeni, wpływami zewnętrznymi i dezinformacją. Uzupełnieniem tego były aktywności edukacyjne, w tym szkolenia dla komitetów wyborczych w zakresie cyberbezpieczeństwa. Działania te są niezbędne w obliczu trwającego cyberkonfliktu z Rosją.

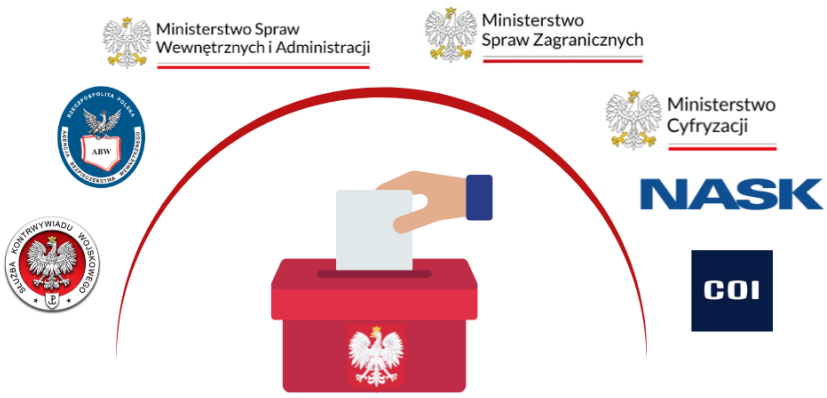
Niniejszy raport dokumentuje zarówno operacyjne aspekty realizacji programu, jak i systemowe wnioski wynikające z jego wdrożenia - z myślą o kolejnych etapach budowy narodowej odporności cyfrowej i informacyjnej.

1 PROGRAM "PARASOL WYBORCZY"

"Parasol Wyborczy" stanowił kompleksowy program ochrony wyborów prezydenckich opracowany przez MC we współpracy z Ministerstwem Spraw Wewnętrznych i Administracji (MSWiA), uruchomiony został w lutym 2025 r. na podstawie akumulacji doświadczeń zebranych podczas poprzednich procesów wyborczych. **Program ten został zaprojektowany jako odpowiedź na zidentyfikowane zagrożenia związane z potencjalną ingerencją zewnętrzną w proces wyborczy, w szczególności ze strony służb rosyjskich, które z pełną premedytacją, ale również z planami operacyjnymi, chciały i miały zamiar wpływać na polską kampanię prezydencką -** powyższe zostało ogłoszone we wspólnym wystąpieniu podczas konferencji prasowej [1] Wicepremiera, Ministra Cyfryzacji i Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa Krzysztofa Gawkowskiego oraz Ministra Spraw Wewnętrznych i Administracji Tomasza Siemoniaka w dniu 28 stycznia 2025 r.

Nazwa programu nawiązywała do funkcji ochronnej jaką miał pełnić program wobec demokratycznego procesu wyborczego w cyberprzestrzeni. Program stanowił element szerszej koncepcji zabezpieczenia demokratycznych procesów państwa polskiego mającej na celu zapewnienie uczciwości i transparentności wyborów prezydenckich, których pierwsza tura odbyła się w dniu 18 maja 2025 r. oraz druga tura 1 czerwca 2025 r.

Utworzenie programu "Parasol Wyborczy" wynikało bezpośrednio z systematycznej analizy doświadczeń wyborczych z lat 2023-2024, które ujawniły narastającą skalę zagrożeń w środowisku cyfrowym oraz dezinformacyjnych. Doświadczenia z wyborów parlamentarnych 2023 r., gdzie po raz pierwszy w tak szerokim zakresie zaobserwowano próby wpływania na proces wyborczy w Polsce poprzez platformy mediów społecznościowych oraz wybory samorządowe 2024 r., które wykazały podatność lokalnych struktur administracyjnych na cyberataki, stały się fundamentem dla opracowania kompleksowego podejścia do ochrony wyborów prezydenckich. Koniecznym było również wzmocnienie współpracy pomiędzy podmiotami tworzącymi Parasol Wyborczy, ze względu na różne obszary określonych ustawowo zakresów działań tych instytucji.

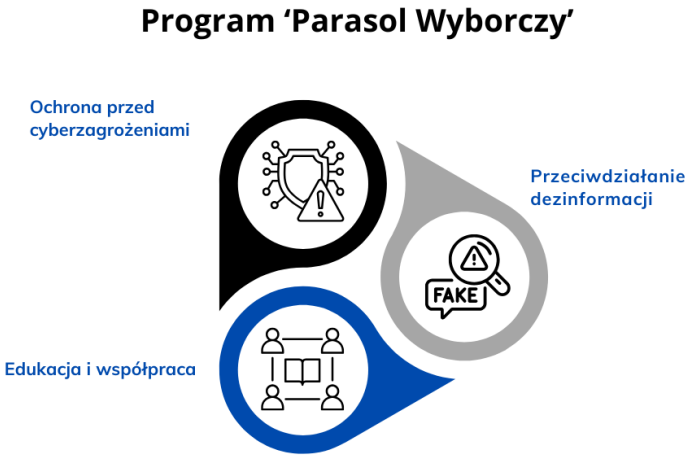


Rysunek 1: Instytucje realizujące program 'Parasol Wyborczy'.

[1] https://www.gov.pl/web/cyfryzacja/program-ochrony-wyborow-przed-cyberzagrozeniami-i-dezinformacja

1.1 CELE I ZAKRES DZIAŁANIA PROGRAMU

Program "Parasol Wyborczy" obejmował działania w trzech kluczowych obszarach zabezpieczenia procesu wyborczego, wypracowanych na podstawie doświadczeń z poprzednich cykli wyborczych, do których zaliczono: ochronę przed cyberzagrożeniami, przeciwdziałanie dezinformacji oraz działalnosc edukacyjną i współpracę.



Rysunek 2: Obszary działań w ramach parasola wyborczego

1. **Ochrona przed cyberzagrożeniami:**
   - wzmocnienie cyberbezpieczeństwa aplikacji krytycznych dla organizacji wyborów;
   - przeprowadzanie analiz podatności na cyberataki przez Agencję Bezpieczeństwa Wewnętrznego (ABW);
   - testy penetracyjne, wzmacnianie, monitorowanie systemów teleinformatycznych związanych z procesem wyborczym (w tym systemów Krajowego Biura Wyborczego, KBW), jak również systemów i rejestrów państwowych oraz cyfrowych usług publicznych (w tym aplikacji mObywatel);
   - odpieranie ataków DDoS dzięki projektowi AntyDDoS, którym MC zapewnia ochronę przed atakami DDoS dla kilkudziesięciu kluczowych instytucji, w tym związanych z procesem wyborczym;
   - bezpłatne narzędzia do diagnozy cyberbezpieczeństwa dla komitetów wyborczych.

2. **Przeciwdziałanie dezinformacji:**
   - monitoring polskiej infosfery, w tym w szczególności platform społecznościowych: X, Facebook, Instagram, TikTok oraz Telegram przez NASK, ABW, SKW, MSZ;
   - wykrywanie i weryfikacja treści dezinformacyjnych publikowanych w internecie;
   - zespół ds. przeciwdziałania zagranicznym operacjom informacyjnym wymierzonym w proces wyborczy przy MSZ powołany przez Prezesa Rady Ministrów;

- regularne spotkania w formule „War room” z przedstawicielami platform społecznościowych oraz służb specjalnych.

3. **Współpraca i edukacja:**
   - Połączone Centrum Operacyjne Cyberbezpieczeństwa;
   - szkolenia cyberbezpieczeństwa dla pracowników KBW i członków Państwowej Komisji Wyborczej (PKW);
   - organizacja szkoleń dla komitetów wyborczych, dziennikarzy oraz osób odpowiedzialnych za organizację wyborów;
   - współpraca z największymi platformami mediów społecznościowych;
   - kampania informacyjna dotycząca rozpoznawania dezinformacji;
   - monitoring naruszeń ciszy wyborczej.

1.2 KONTEKST BEZPIECZEŃSTWA NARODOWEGO

Wdrożenie programu "Parasol Wyborczy" wynikało z analizy zagrożeń przeprowadzonej przez podmioty publiczne odpowiedzialne za bezpieczeństwo państwa w oparciu o obserwacje poczynione podczas kolejnych cykli wyborczych. MC wspólnie z MSWiA (w tym poprzez jednostki podległe i nadzorowane oraz służby specjalne) zdiagnozowały występowanie zorganizowanych akcji, prowokacji, ale również inicjatyw, które miałyby w Polsce zdestabilizować sytuację wyborczą oraz wpłynąć na wzrost poziomu polaryzacji społecznej.

Dane statystyczne opublikowane w Sprawozdaniu Pełnomocnika Rządu ds. Cyberbezpieczeństwa za rok 2024 [2] wskazywały zasadność podjęcia działań, świadcząc o wzroście liczby zgłoszeń i incydentów w zakresie działań w cyberprzestrzeni. W 2024 r. CSIRTy poziomu krajowego sumarycznie zarejestrowały 111 660 incydentów bezpieczeństwa teleinformatycznego, z czego CSIRT NASK zarejestrował 103 449 (wzrost 29% rdr), CSIRT GOV (ABW) 3 991 (spadek 16% rdr), natomiast CSIRT MON 4 220 (spadek 28% rdr). Powyższe zestawienie liczby incydentów, zostało zawarte w tabeli poniżej. Analiza wskaźników wskazuje wyraźny trend wzrostowy rejestrowanych incydentów w skali krajowej (23% rdr).

[2] https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie

CSIRT poziomu krajowego	2023 r.	2024 r	Zmiana procentowa
CSIRT NASK	80 267	103 449	+29%
CSIRT GOV	4 676	3 991	-15%
CSIRT MON	5 841	4 220	-28%
Sumaryczna roczna liczba zarejestrowanych incydentów	90 784	111 660	+23%

Tabela 1: Liczba zarejestrowanych incydentów w CSIRT-ach poziomu krajowego w 2024 r.

1.3 REALIZACJA PROGRAMU W PRAKTYCE

Program "Parasol Wyborczy" zakładał skoordynowane działania poszczególnych instytucji państwowych w ramach nadanych im ustawowo kompetencji, wykorzystujące doświadczenia zgromadzone podczas wyborów parlamentarnych 2023 r. oraz samorządowych 2024 r. i do Parlamentu Europejskiego z tego samego roku.

W zakresie cyberbezpieczeństwa działania poszczególnych instytucji były koordynowane na poziomie strategicznym (Kolegium ds. Cyberbezpieczeństwa i Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa) oraz operacyjnym (Połączone Centrum Operacyjne Cyberbezpieczeństwa [3]). Tematyka dot. uruchomienia programu została poruszona na posiedzeniu Kolegium ds. Cyberbezpieczeństwa w dniu 19.12.2024 r. i obejmowała przedstawienie opinii ABW oraz NASK w sprawie bezpieczeństwa wyborów prezydenckich 2025 r. W terminach późniejszych zagadnienie było systematycznie poruszane w ramach spotkań Połączonego Centrum Operacyjnego Cyberbezpieczeństwa, gdzie były omawiane zagadnienia dot. bezpieczeństwa cyberprzestrzeni na poziomie operacyjnym i technicznym, w tym również z przedstawicielami m.in. KBW, służb specjalnych, policji i CSIRT-ów poziomu krajowego. Prowadzono liczne przedsięwzięcia związane z podnoszeniem odporności infrastruktury związanej procesem wyborczym i zapewniającej nieprzerwane funkcjonowanie systemów i usług państwowych, jak również podnoszeniem kompetencji w zakresie cyberbezpieczeństwa i higieny cyfrowej kluczowych w tym zakresie instytucji.

[3] Połączone Centrum Operacyjne Cyberbezpieczeństwa

W ramach realizacji zadań z zakresu przeciwdziałania dezinformacji powstały m.in. zespoły koordynujące regularną współpracę z największymi platformami mediów społecznościowych, a także Zespół ds. przeciwdziałania zagranicznym operacjom informacyjnym wymierzonym w proces wyborczy działający przy Ministerstwie Spraw Zagranicznych (MSZ) powołany przez Prezesa Rady Ministrów. W ramach cotygodniowych spotkań Zespołu wymieniano się informacjami dotyczącymi zewnętrznego aspektu ingerencji i manipulacji informacją procesie wyborczym. Regularny monitoring sieci realizowany przez Ośrodek Analizy Dezinformacji NASK (OAD NASK) w trakcie kampanii wyborczej wykrywał treści dezinformujące oraz anomalie m.in. w postaci płatnych kampanii na platformie Facebook, których źródła finansowania mogły pochodzić spoza Polski lub nielegalnej agitacji wyborczej realizowanej przez nieuprawnione podmioty. Wykryte treści dezinformujące, które mogły być niezgodne z prawem i kodeksem wyborczym zostały niezwłocznie zgłoszone do ABW w celu prowadzenia dalszych działań sprawdzających zgodnie z właściwością zadań ABW. NASK informował również o wykrytych incydentach również KBW oraz występował do firmy Meta (właściciela platformy Facebook) o usunięcie manipulacyjnych treści.

Podczas realizacji zadań w zakresie Parasola Wyborczego zidentyfikowano m.in. że jedną z barier uniemożliwiających sprawne działanie są niedoskonałości w systemie prawnym w zakresie przeciwdziałania zdarzeniom w cyberprzestrzeni, co zostanie rozwinięte w dalszej części Raportu.

1.4 WYNIKI WYBORÓW PREZYDENCKICH I OCENA SKUTECZNOŚCI PROGRAMU

Wybory prezydenckie 2025 r. odbyły się zgodnie z planem - pierwsza tura miała miejsce 18 maja 2025 r., zaś druga tura została przeprowadzona 1 czerwca 2025 r.. Frekwencja w skali całego kraju wyniosła 71,63 procent, co stanowiło najwyższą frekwencję od 1990 r. w historii wyborów prezydenckich.

Program "Parasol Wyborczy" stanowił kluczowy element strategii państwa polskiego w zakresie ochrony demokratycznych procesów wyborczych przed współczesnymi zagrożeniami cyfrowymi i mającymi znamiona dezinformacji, będąc bezpośrednim rezultatem systematycznej akumulacji doświadczeń instytucjonalnych z trzech kolejnych cykli wyborczych przeprowadzonych w latach 2023-2025. Skuteczność programu została potwierdzona zarówno przez wykrycie i próby neutralizacji ingerencji zewnętrznej, jak również przez ogólnie spokojny przebieg procesu wyborczego i wysoką frekwencję wyborczą.

2 DZIAŁANIA MINISTERSTWA CYFRYZACJI ORAZ JEDNOSTEK PODLEGŁYCH I NADZOROWANYCH

W kontekście zapewniania odporności państwa na zagrożenia cyfrowe w okresie kampanii wyborczej, istotną rolę odgrywa **MC jako instytucja odpowiedzialna za koordynację polityki państwa w obszarze transformacji cyfrowej, bezpieczeństwa informacji oraz infrastruktury teleinformatycznej**. Współdziałając z podmiotami nadzorowanymi – w szczególności Centralnym Ośrodkiem Informatyki (COI) oraz NASK – resort realizuje zadania o charakterze zarówno strategicznym, jak i operacyjnym, ukierunkowane na ochronę procesów wyborczych przed zakłóceniami cyfrowymi takimi jak cyberataki, dezinformacja oraz ingerencja zewnętrzna w cyberprzestrzeni.

Rysunek 3: Ministerstwo Cyfryzacji oraz jednostki podległe i nadzorowane

Działania podejmowane przez MC i jednostki nadzorowane obejmują m.in. monitorowanie przestrzeni informacyjnej, przeciwdziałanie incydentom teleinformatycznym oraz prowadzenie działań edukacyjnych i prewencyjnych w zakresie cyberbezpieczeństwa. Szczególny nacisk położono na współpracę z operatorami usług kluczowych, administracją publiczną oraz sektorem prywatnym w celu zapewnienia ciągłości działania systemów teleinformatycznych wykorzystywanych w procesie wyborczym.

Celem niniejszego podrozdziału jest przedstawienie zakresu, charakterystyki oraz skuteczności działań realizowanych przez MC, COI i NASK w ramach systemowego zabezpieczenia procesu wyborczego, ze szczególnym uwzględnieniem aspektów technicznych, organizacyjnych oraz informacyjnych.

2.1 MINISTERSTWO CYFRYZACJI

Minister Cyfryzacji jest jednocześnie Pełnomocnikiem Rządu do Spraw Cyberbezpieczeństwa, a Departament Cyberbezpieczeństwa MC zapewnia jego wsparcie i obsługę. Pod auspicjami Pełnomocnika działa Połączone Centrum Operacyjne Cyberbezpieczeństwa, w ramach którego koordynowane są działania instytucji zapewniających cyberbezpieczeństwo na poziomie krajowym. Już na kilka miesięcy wcześniej tematyka wyborów była jednym z głównym obszarów działań Połączonego Centrum Operacyjnego Cyberbezpieczeństwa, który funkcjonuje w trybie niejawnym. Umożliwiło to należytą koordynację działań i zarządzanie procesem zapewniania cyberbezpieczeństwa wyborów.

Rysunek 4: Kampania informacyjna "Z mObywatelem wybory są łatwiejsze"

MC w ramach projektu AntyDDoS zapewnia centralnie ochronę przed atakami DDoS dla kilkudziesięciu kluczowych instytucji publicznych. Chronione są m.in. serwisy bezpośrednio związane z wyborami. Warto podkreślić, że resort cyfryzacji rozpościera tarczę przeciwko atakom DDoS nad ponad 80 podmiotami, w tym także nad Siłami Zbrojnymi RP.

Kluczowe dla przeciwdziałania cyberzagrożeniom miał system rozpoznawania zagrożeń w cyberprzestrzeni (Cyber Threat Intelligence, CTI), pozyskany na potrzeby własne (MC i COI) oraz siedmiu innych instytucji zapewniających bezpieczeństwo teleinformatyczne na poziomie krajowym. Umożliwiło to m.in. poszukiwanie informacji o atakach i wyciekach oraz aktywności grup hakerskich.

Ponadto MC poprzez działania własne i dotacje dla jednostek nadzorowanych zapewnia funkcjonowanie kluczowych inicjatyw dla cyberbezpieczeństwa na poziomie krajowym, w tym w zakresie bezpieczeństwa wyborów (m.in. bezpiecznedane.gov.pl, bezpiecznewybory.pl, bezpieczny komunikator, system łączności niejawnej SKR-Z).

W zakresie budowania świadomości społecznej MC uruchomiło kampanie informacyjną pod hasłem: „Wybory z mObywatelem są łatwiejsze” miała ona na celu pokazanie, jak aplikacja mObywatel może wspierać obywateli w trakcie wyborów prezydenckich. Przekaz kampanii koncentrował się na praktycznych funkcjach aplikacji, takich jak mDowód, który umożliwia potwierdzenie tożsamości w lokalu wyborczym, a także dostęp do informacji o miejscu głosowania i możliwość jego zmiany. Działania te stanowiły kontynuację szerszej kampanii „mObywatel ma łatwiej”.

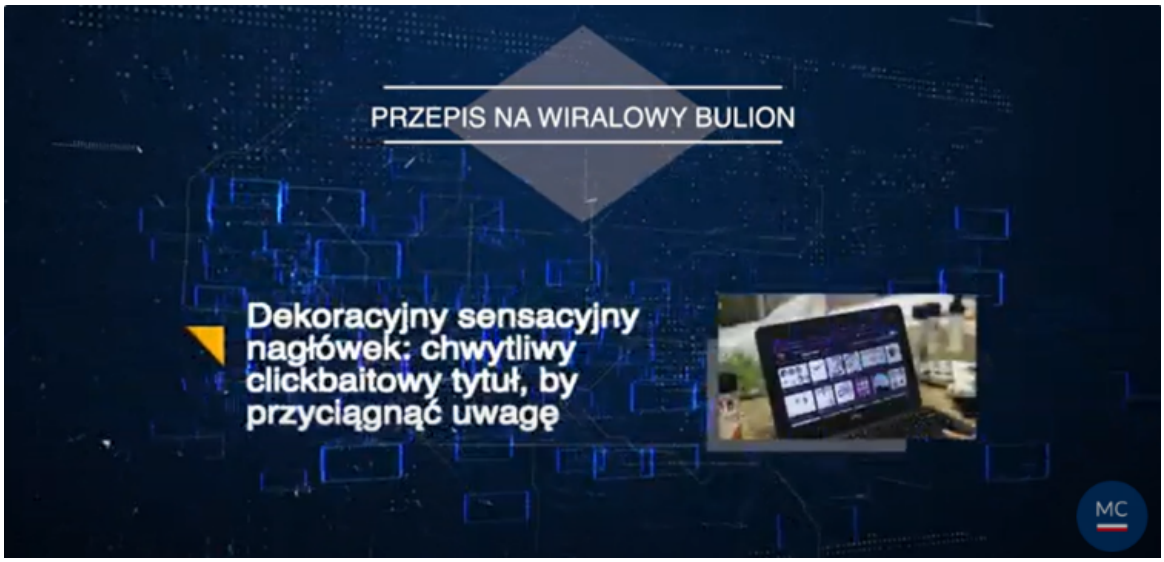
Dodatkowo MC wraz z NASK zrealizowało kampanie informacyjno-edukacyjne w zakresie przeciwdziałania dezinformacji:

1. Kampania internetowa, radiowa i telewizyjna – Trolle –22.04-16.05.25.

Rysunek 5: Kampania informacyjna TROLE

Rysunek 6: Kampania informacyjna TROLE

2. Kampania edukacyjna "Przepis na dezinformację", emitowania w dniach 13.05-05.06 (z wyłączeniem ciszy wyborczej i wyborów) na stacjach TVP 1, TVP 2 i TVP Seriale.



Rysunek 7: Kampania edukacyjno- informacyjna „Przepis na dezinformację”

Rysunek 8: Kampania edukacyjno- informacyjna „Przepis na dezinformację”

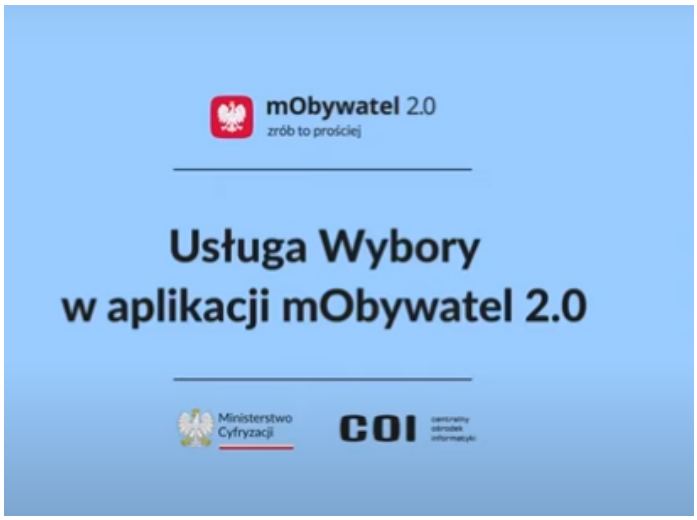
Istotnym obszarem działań MC są liczne formy szkoleń cyberbezpieczeństwa. W ramach projektu SecureV, którego celem są szkolenia cyberbezpieczeństwa dla najważniejszych osób w państwie, objęto nimi także przedstawicieli KBW i organów wyborczych.

Jednym z działań MC wspólnie z MSZ było uszczelnienie możliwości rejestracji internetowej w spisie wyborców za granicą, co potencjalnie uniemożliwiło adwersarzom podjęcie próby masowej zmiany miejsca głosowania nieświadomych tego uprawnionych wyborców.

2.2 CENTRALNY OŚRODEK INFORMATYKI (COI)

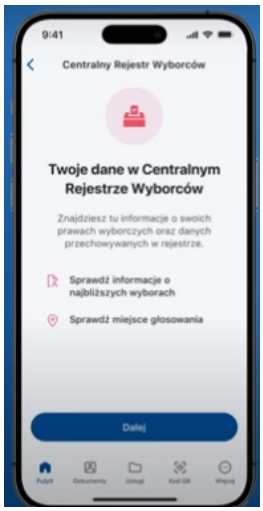
Realizacja działań przez COI w ramach programu „Parasol Wyborczy"

Centralny Ośrodek Informatyki zapewnienia wysoki poziom cyberbezpieczeństwa utrzymywanych systemów i rejestrów państwowych oraz usług cyfrowych (m.in. kluczowych dla wyborów takich jak PESEL, Węzeł Krajowy, mObywatel), w tym poprzez monitorowanie w trybie 24/7 przez zespół cyberbezpieczeństwa, stałe podnoszenie zdolności do reagowania na incydenty, ścisłą współpracę z CSIRT GOV (ABW) i CSIRT NASK oraz poprzez wdrażanie nowych rozwiązań technicznych, proceduralnych i systemowych, jak również przeprowadzanie cyklicznych testów ciągłości działania oraz włączenie aspektów cyberbezpieczeństwa na jak najwcześniejszym etapie rozwoju i utrzymania.



Rysunek 9: Usługa Wybory w aplikacji mObywatel 2.0

W ramach przygotowań do wyborów COI prowadził szereg spotkań z KBW, których celem było zapewnienie optymalnych i bezpiecznych metod potwierdzania tożsamości wyborców z wykorzystaniem aplikacji mObywatel. Spotkania te pozwoliły na wypracowanie rozwiązań, które uwzględniają potrzeby i ograniczenia techniczne związane z procesem wyborczym.



Rysunek 10: Centralny Rejestr Wyborców w mObywatel 2.0

Ponadto COI opracował specjalne kody QR, które zostały rozdystrybuowane do wszystkich Komisji Wyborczych w kraju. Dzięki nim Komisje Wyborcze mogły w prosty i szybki sposób zweryfikować autentyczność aplikacji mObywatel i potwierdzić tożsamość osoby głosującej. PKW w Uchwale w sprawie wytycznych dla obwodowych komisji wyborczych w wyborach Prezydenta RP w 2025 r. opisało sposób potwierdzania tożsamości wyborcy na podstawie aplikacji mObywatel: Uchwała nr 165/2025 Państwowej Komisji Wyborczej z dnia 23 kwietnia 2025 r. w sprawie wytycznych dla obwodowych komisji wyborczych dotyczących zadań i trybu przygotowania oraz przeprowadzenia głosowania w obwodach głosowania utworzonych w kraju w wyborach Prezydenta Rzeczypospolitej Polskiej zarządzonych na dzień 18 maja 2025 r.

„Komisja może potwierdzić tożsamość wyborcy także na podstawie aplikacji mObywatel. W tym celu wyborca powinien: a) zalogować się do aplikacji mObywatel na swoim telefonie (aplikacja powinna być zaktualizowana do wersji 4.56.0 lub nowszej), b) wybrać w prawym dolnym rogu na ekranie głównym przycisk Kod QR, c) nacisnąć przycisk Zeskanuj kod QR. Aplikacja poprosi o wyrażenie zgody na użycie aparatu fotograficznego w celu zeskanowania kodu QR. Następnie członek komisji okazuje wyborcy

otrzymaną przez komisję kartkę z kodem QR, który wyborca musi zeskanować swoim telefonem. Po zeskanowaniu kodu na telefonie wyborcy powinien wyświetlić się ekran z potwierdzeniem jego danych. Na tej podstawie członek komisji potwierdza tożsamość wyborcy[4]*."*

Wykonano analizę zagrożeń w cyberprzestrzeni, mogących stanowić potencjalne niebezpieczeństwa dla procesu wyborczego i na tej podstawie przeprowadzono działania doskonalące w obszarze monitorowania zdarzeń, reagowania na incydenty bezpieczeństwa przez zespół Security Operations Center (SOC). Przeszkolono również w tym zakresie personel COI.

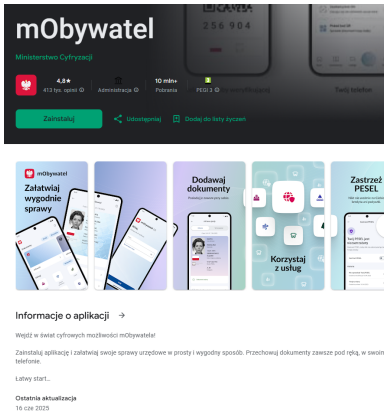
W ramach działań informacyjnych, skierowanych do użytkowników aplikacji mObywatel podejmowano następujące działania:

– wysyłano wiadomości push przypominające o konieczności aktualizacji aplikacji do najnowszej wersji;

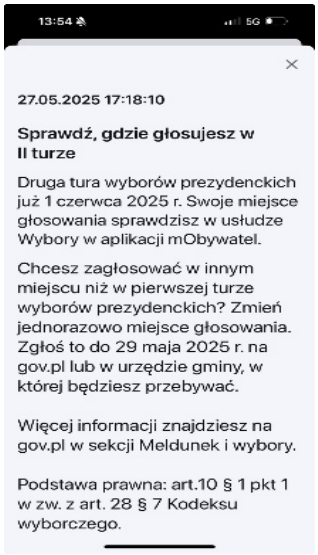
– użytkownicy byli na bieżąco informowani o usłudze „Wybory" w aplikacji, umożliwiającej sprawdzenie przysługujących im praw wyborczych, najbliższych wyborach (terminie i rodzaju wyborów), miejsca głosowania (numerze obwodu i adresie siedziby obwodowej komisji wyborczej). Usługa została wyposażona także w funkcję umożliwiającą dodanie terminu wyborów do kalendarza w telefonie.

Dane udostępniane w usłudze pochodzą bezpośrednio z Centralnego Rejestru Wyborców (CRW). W rejestrze zawarte są dane o wszystkich wyborcach – zarówno obywatelach polskich, jak i cudzoziemcach uprawnionych do głosowania w Polsce. Dzięki aplikacji mObywatel wyborcy mogą wziąć udział w głosowaniu w sposób wygodny, nowoczesny i bezpieczny. Co więcej mDowód pozwala zostawić tradycyjny dokument tożsamości w domu, a usługa Wybory ułatwia udział w głosowaniu, dzięki wielu dedykowanym funkcjonalnościom.

Rysunek 11: Funkcjonalności w usłudze „Wybory" w aplikacji mObywatel 2.0



Rysunek 12: Aplikacja mObywatel 2.0 do pobrania



Rysunek 13: Wiadomość PUSH - weryfikacja miejsca głosowania

[4] Źródło: https://wybory.gov.pl/prezydent2025/statics/PKW_UCHWALY/uploaded_files/1745430357_wytyczne-obwodowe-w-kraju-prezydent-2025-904.pdfUCHWAŁA NR 165/2025 PAŃSTWOWEJ KOMISJI WYBORCZEJ z dnia 23 kwietnia 2025 r. w sprawie wytycznych dla obwodowych komisji wyborczych dotyczących zadań i trybu przygotowania oraz przeprowadzenia głosowania w obwodach głosowania utworzonych w kraju w wyborach Prezydenta Rzeczypospolitej Polskiej zarządzonych na dzień 18 maja 2025 r.

2.1 NASK-PIB

DZIAŁANIA CSIRT NASK W OBSZARZE BEZPIECZEŃSTWA WYBORÓW PREZYDENCKICH 2025 R.

Działania profilaktyczne i prewencyjne

Zespół CSIRT NASK w ramach wyborów prezydenckich przygotował plan działań, które miały usprawniać wykrywanie i niwelowanie zagrożeń oraz udoskonalić komunikację między kluczowymi podmiotami zaangażowanymi w proces okołowyborczy. Poniżej zostały opisane najważniejsze aktywności:

Skanowanie domen i sieci komitetów wyborczych przy użyciu narzędzia ARTEMIS oraz moje.cert.pl

Skanowanie bezpieczeństwa było prowadzone dwutorowo. Oprócz skanowań prowadzonych z własnej inicjatywy, CSIRT NASK zaprosił komitety wyborcze do skorzystania portalu moje.cert.pl, aby mogły uruchomić skanowanie wszystkich swoich domen i sieci, nie tylko tych zidentyfikowanych przez zespół CSIRT NASK. W ramach prowadzonych skanowań sprawdzono 591 domen i 16998 subdomen, co pozwoliło zidentyfikować 3256 podatności błędnych konfiguracji, w tym 121 wiążących się z wysokim ryzykiem. Skanowanie obejmowało różne typy podatności, zarówno te umożliwiające atakującemu zmianę treści strony czy doprowadzenie do jej niedostępności, jak też brak wdrożonych mechanizmów zabezpieczających przed wysyłaniem fałszywych e-maili z danej domeny.

Szybki kanał kontaktu z komitetami wyborczymi

W celu zapewnienia sprawnej wymiany informacji na bezpiecznym komunikatorze udostępnianym przez MC założono dedykowane, trójstronne kanały szybkiego kontaktu z 8 chętnymi zarejestrowanymi komitetami wyborczymi kandydatów na prezydenta RP. W każdym z nich uczestniczyli członkowie zespołu OAD działającego w ramach NASK, eksperci CSIRT NASK oraz przedstawiciele komitetu. Kanały wykorzystywano do przesyłania komunikatów o zagrożeniach, najczęściej związanych z działaniami dezinformacyjnymi oraz informowaniu o działaniach podejmowanych przez NASK, a także do promowania wykorzystania serwisu moje.cert.pl wśród kandydatów i związanych z nimi partii politycznych do podniesienia poziomu cyberbezpieczeństwa.

Działania prewencyjne

Od początku kampanii wyborczej, a także w dniach poprzedzających CSIRT NASK monitorował nowo rejestrowane domeny, media społecznościowe, zgłoszenia (napływające poprzez e-mail, formularz, aplikację mObywatel, przekazywane na numer 8080 w postaci wiadomości SMS) pod kątem potencjalnych oszustw wykorzystujących wizerunek partii politycznych, poszczególnych

kandydatów lub instytucji związanych z procesem wyborczym.

CSIRT NASK pozostawał również w ścisłym kontakcie z innymi CSIRT'ami poziomu krajowego oraz sektorowymi zespołami cyberbezpieczeństwa (CSIRT CeZ, CSIRT KNF), organami ścigania, a także OAD NASK.

Monitoring wycieków

CSIRT NASK na bieżąco monitoruje dostępne źródła pod kątem wycieków danych uwierzytelniających polskich internautów lub publikacji innych danych pozyskanych w wyniku włamań do polskich podmiotów. W okresie kampanii wyborczej szczególną uwagę położono na monitorowanie zdarzeń zawierających słowa kluczowe związane z partiami politycznymi i poszczególnymi kandydatami, w celu możliwie szybkiego reagowania na incydenty, które mogłyby mieć wpływ na trwające wybory.

17 marca 2025 r. CSIRT NASK uzyskał informację o publikacji danych członków partii Nowa Nadzieja. Zostały one wykradzione przez serwis służący do okresowego opłacania składek członkowskich i zawierały informacje takie tak imię, nazwisko, numer PESEL, adres mailowy oraz przypisaną komórkę organizacyjną partii. Łącznie w wycieku znalazły się dane ok. 2500 osób. Informacja o zdarzeniu została bezzwłocznie przekazana za pośrednictwem kanału szybkiego kontaktu do Komitetu Wyborczego Kandydata tej partii w wyborach. Nie udało się uzyskać informacji technicznych w zakresie wektora ataku lub infrastruktury wykorzystywanej przez atakujących. Równolegle CSIRT NASK skontaktował się z administratorem serwisu, na którym opublikowano dane, dzięki czemu oryginalne linki zostały zablokowane. Niestety, w kolejnych miesiącach dane ponownie były zamieszczane w różnych serwisach przez adwersarzy, którzy zdążyli pobrać zawartość oryginalnej publikacji.

Reklamy fałszywych platform inwestycyjnych wykorzystujących wizerunki kandydatów

W okresie przedwyborczym CSIRT NASK w dalszym ciągu obserwował kampanie reklamowe fałszywych platform inwestycyjnych, w tym te wykorzystujące wizerunki kandydatów. Domeny zawierające takie reklamy były na bieżąco umieszczane na Liście Ostrzeżeń CERT Polska, a hostingodawcy rzeczonych domen otrzymywali stosowną informację o zagrożeniu.

W przypadku informacji o pojawieniu się takich reklam w mediach społecznościowych, informacje o nich były niezwłocznie przekazywane do Ośrodka Analizy Dezinformacji.

Działania CSIRT NASK podczas I tury wyborów

CSIRT NASK zarejestrował następującą liczbę zgłoszeń powiązanych z I turą wyborów:

- 144 zgłoszenia dot. fałszywych SMSów;
- incydent dot. domeny bezpartyjnisamorzadowcy.pl - infekcja strony, kontakt z administratorem;
- incydent dot. domeny robertbiedron.pl - umieszczenie niepożądanej treści na stronie;
- 115 zgłoszeń dotyczących łamania ciszy wyborczej - przekazane do organów ścigania oraz do CSIRT GOV (ABW);
- 3 zgłoszenia dotyczące nieprawidłowościach w komisjach - przekazane do organów ścigania oraz do CSIRT GOV (ABW).

PRZYKŁADY ZIDENTYFIKOWANYCH KAMPANII

Opis incydentu dot. fałszywej kampanii SMSowej

14 maja w godzinach wieczornych rozpoczęła się fałszywa kampania SMS-owa, w ramach której sprawcy rozsyłali spreparowane wiadomości, rzekomo stanowiące element kampanii wyborczej prowadzonej przez Platformę Obywatelską. Nazajutrz 15 maja CSIRT NASK otrzymał zgłoszenie w tej sprawie od jednego z komitetów wyborczych za pośrednictwem kanału szybkiego kontaktu w komunikatorze oraz uzyskał potwierdzenie od KWKP Rafała Trzaskowskiego, że wiadomości są fałszywe i nie były wysyłane w ramach prowadzonej kampanii. W ramach prowadzonych działań został utworzony wzorzec wiadomości umożliwiający operatorom telekomunikacyjnym ich blokowanie.

Zwiekszylismy zasilek pogrzebowy do 7 tys. POlacy zasluguja na godne ostatnie POzegnanie. Glosuj na Trzaskowskiego. Platforma.org
wiekszylismy zasilek pogrzebowy do 7 tys. POlacy zasluguja na godne ostatnie POzegnanie. Glosuj na Trzaskowskiego. Platforma.org
Spelniamy obietnice. Zlikwidowalismy kolejki w przychodniach. Glosuj na Trzaskowskiego. Platforma.org
Europa jest nasza przyszloscia. Dlatego wprowadzimy EURO. Marzenia staja sie rzeczywistoscia. Glosuj na Trzaskowskiego. Platforma.org

Rysunek 14: Przykładowe treści złośliwych wiadomości SMS

Część wiadomości została wysłana przy wykorzystaniu nadpisów:

Platforma
RITISHPROV

Rysunek 15: Przykład nadpisu wiadomości

Podobną aktywność CSIRT NASK obserwował przed wyborami parlamentarnymi w 2023 r. Podczas tamtej kampanii szkodliwe SMS-y wykorzystywały wizerunek będącej wówczas u władzy partii Prawo i Sprawiedliwość. Tematyka SMSów częściowo się pokrywa - wówczas jednym z wykorzystywanych szablonów było:

GlosujNaPiS!Przywrocilismy seniorom prawo do godnej starosci i zrobimy tez pogrzeby emerytow za darmo

Rysunek 16: Przykładowa treść złośliwych wiadomości SMS z poprzedniej kampanii wyborczej

Warto zauważyć, że w 2023 r. rozesłanie SMS-ów było poprzedzone kampanią spamową, m.in. wykorzystującą spoofing adresu nadawcy i podszywającą się pod domeny Prawa i Sprawiedliwości. Wiadomości mailowe zawierały wówczas motywy, które powtórzyły się potem w SMS-ach. Kampania mailowa z 2023 r. została powiązana z aktywnością grupy UNC1151/GhostWriter, zaangażowanej w wymierzone w Polskę działania dezinformacyjne i operacje szpiegowskie.

Opis ataków DDoS:

Prorosyjska grupa hacktywistyczna NoName057(16) w ramach projektu DDoSia w trakcie wyborów prezydenckich uruchamiała ataki na polskie podmioty w dniach 16. maja i 18. maja 2025 r. 16. maja 2025 r. wśród 19 atakowanych polskich stron były strony partii lub komitetów wyborczych: Polskie Stronnictwo Ludowe, Bezpartyjni Samorządowcy, Lewica, Platforma Obywatelska, Trzecia Droga, Kukiz 15. 18. maja 2025 r. wśród 39 atakowanych polskich stron były strony partii Polskiego Stronnictwa Ludowego oraz Platformy Obywatelskiej. Należy podkreślić, że wśród znanych celów wskazanych powyżej ataków DDoS nie było witryn wykorzystywanych przez kandydatów na urząd Prezydenta Polski (atakowane były natomiast np. witryny komitetów wyborczych założone na potrzeby kampanii w 2023 r.).

Do dotkniętych podmiotów rozesłano ostrzeżenia dotyczące planowanych ataków, zawierające informację na temat rekomendowanych metod obrony przed tym zagrożeniem. CSIRT NASK podjął również próby kontaktu telefonicznego celem upewnienia się, że podmioty ostrzeżenia otrzymały. W przypadku niepowodzenia, podejmowano próby przekazania informacji za pośrednictwem komitetu wyborczego kandydata popieranego przez partię, której witryna była celem ataku.

Z uwagi na przedłużającą się niedostępność jednego z serwisów wykorzystywanego przez partię polityczną, CSIRT NASK nawiązał bezpośredni kontakt z administratorem serwisu w celu udzielenia niezbędnego wsparcia. W trakcie działań uzyskano informację, że dostęp do witryny został ograniczony decyzją administratora. Zaatakowany podmiot przekazał też do CSIRT NASK logi sieciowe z ataku, co pozwoliło na zebranie informacji na temat charakterystyki złośliwego ruchu. W przypadku drugiej z zaatakowanych witryn należących do partii politycznej, udało się nawiązać kontakt telefoniczny z administratorem, który przekazał informację, że działania zostaną podjęte dopiero po weekendzie wyborczym.

Incydent dot. umieszczenia niepożądanej treści na stronie robertbiedron.pl

18. maja 2025 r. CSIRT NASK uzyskał informację o włamaniu na stronę europosła Roberta Biedronia i zamieszczeniu na niej treści przez atakującego. Informacja o włamaniu została przekazana do KWKP Magdaleny Biejat. W odpowiedzi otrzymano potwierdzenie przekazania wiadomości do administratora strony i podjęcia przez niego działań.

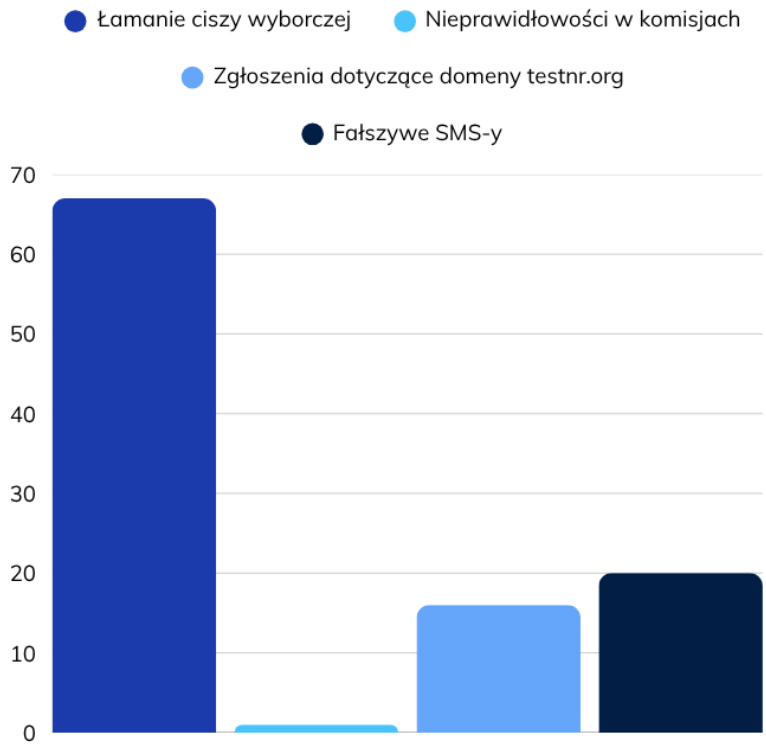
Działania CSIRT NASK podczas II tury wyborów:

CSIRT NASK zarejestrował następującą liczbę zgłoszeń powiązanych z II turą wyborów:

- 67 zgłoszeń dotyczących łamania ciszy wyborczej - przekazane do organów ścigania oraz do CSIRT GOV (ABW);
- 1 zgłoszenie dotyczące nieprawidłowości w komisjach - przekazane do organów ścigania oraz do CSIRT GOV (ABW);
- 110 zgłoszeń dotyczących domeny testnr.org (Ruch Kontroli Wyborów) – przekazane do

organów ścigania oraz do CSIRT GOV (ABW)[5];

– 15 zgłoszeń dot. fałszywych SMSów.



Rysunek 17: Zestawienie CSIRT NASK dot. zarejestrowanej liczby zgłoszeń powiązanych z II turą wyborów

28. maja 2025 r. CSIRT NASK ponownie odnotował zgłoszenia SMS o treści wskazującej na prawdopodobne podszycie pod materiał wyborczy od jednego z komitetów. Poprzez kanał szybkiego kontaktu szybko potwierdzono, że SMS-y są fałszywe i nie stanowią elementu prowadzonej kampanii wyborczej, w związku z czym bezzwłocznie przygotowano wzorce umożliwiające operatorom telekomunikacyjnym ich blokowanie.

Powiedz "nie" Potworowi I Sutenerowi. Cala Polska naprzod!
Powiedz "nie" Potworowi I Sut*nerowi. Cala Polska naprzod!
@P@o@w@i@e@d@z@ @"@n@i@e@"@ @P@o@t@w@o@r@o@w@i@ @I@
@S@u@t@e@n@e@r@o@w@i@.@ @C@a@l@a@ @P@o@l@s@k@a@ @n@a@p@r@z@o@d@!
Cala Polska naprzod! Nie dla Potwora i Sutenera. Wybieraj Rafala

Rysunek 18: Prawdopodobne podszycie pod materiał wyborczy

Działania NASK w ramach Ogólnopolskiej Sieci Edukacyjnej (OSE)

[5] Zgłoszenia dotyczące aplikacji związanej z organizacją "Ruch Kontroli Wyborów". Aplikacja służyła do rzekomej weryfikacji ponownego wykorzystania zaświadczenia o prawie do głosowania. Zgłaszający zarzucali wyłudzenie danych osobowych, wpływanie na członków komisji wyborczych oraz przebieg wyborów.

Ważnym aspektem zabezpieczenia przez NASK wyborów również tym razem była Ogólnopolska Sieć Edukacyjna (OSE). Jest to rządowy program zapewniający szkołom w całej Polsce dostęp do szybkiego, bezpłatnego i bezpiecznego internetu. Program został zaprojektowany przez MC i realizowany jest przy współpracy z NASK.

Podczas wyborów zapewniono sprawne i bezprzerwowe działanie sieci we wszystkich punktach wyborczych zlokalizowanych w szkołach, za pośrednictwem zorganizowanych przez MC wraz z NASK szybkich łączy internetowych, umożliwiając komisjom wyborczym sprawną realizacje zadań. Zespoły NASK przygotowały specjalne dyżury oraz postawiły w stan gotowości operacyjnej wszystkich kluczowych dostawców rozwiązań sieciowych i węzłów bezpieczeństwa.

W trakcie pierwszej tury wyborów odnotowano tylko jedno zgłoszenie ze szkoły, w której mieścił się lokal wyborczy. Zgłaszany problem dotyczył awarii zasilania w lokalizacji, a nie awarii łącza OSE. NASK przeprowadził diagnostykę urządzeń brzegowych oraz zapewnił wsparcie operatora łącza dostępowego do lokalizacji. Klient potwierdził poprawne działanie usług i wskazał przyczynę awarii (opuszczone bezpieczniki).

W trakcie drugiej tury wyborów odnotowano kilka zdarzeń niemających wpływu na dostępność usług w szkołach, w tym 3 ataki DDoS na sieć OSE. Najpoważniejszy z nich o godzinie 17:31 na poziomie 161 Gbps (wykryty i zmitygowany przez system ochrony AntyDDoS). Nie odnotowano innych zgłoszeń z lokali wyborczych.

Działania Ośrodka Analizy Dezinformacji NASK (OAD NASK)

Wybory parlamentarne i samorządowe oraz wybory do Parlamentu Europejskiego w 2024 r. pokazały rosnącą skalę dezinformacji i znaczenie budowania odporności społeczeństwa na to zjawisko. Fałszywe i wprowadzające w błąd treści mogą podważać zaufanie do uczciwości procesu wyborczego, obniżać poziom zaufania do administracji państwowej, uderzać w demokratyczne podstawy państwa czy kształtować negatywny obraz Polski na arenie międzynarodowej. Sprzyja to pogłębianiu podziałów społecznych, wzmacnianiu poczucia zagrożenia oraz utrwalaniu postaw nieufności i wrogości wobec innych, co może prowadzić do osłabienia spójności społecznej. Dezinformacyjne treści mogą być też wymierzone w konkretnych kandydatów i wpływać na decyzje wyborców.

W dobie rosnącej roli mediów społecznościowych, przy coraz większej skali fałszywych, wprowadzających w błąd lub niezweryfikowanych treści tworzonych i rozpowszechnianych zarówno przez aktorów wewnętrznych, jak i zewnętrznych niezwykle istotne jest edukowanie i podnoszenie świadomości społeczeństwa w kwestii dezinformacji.

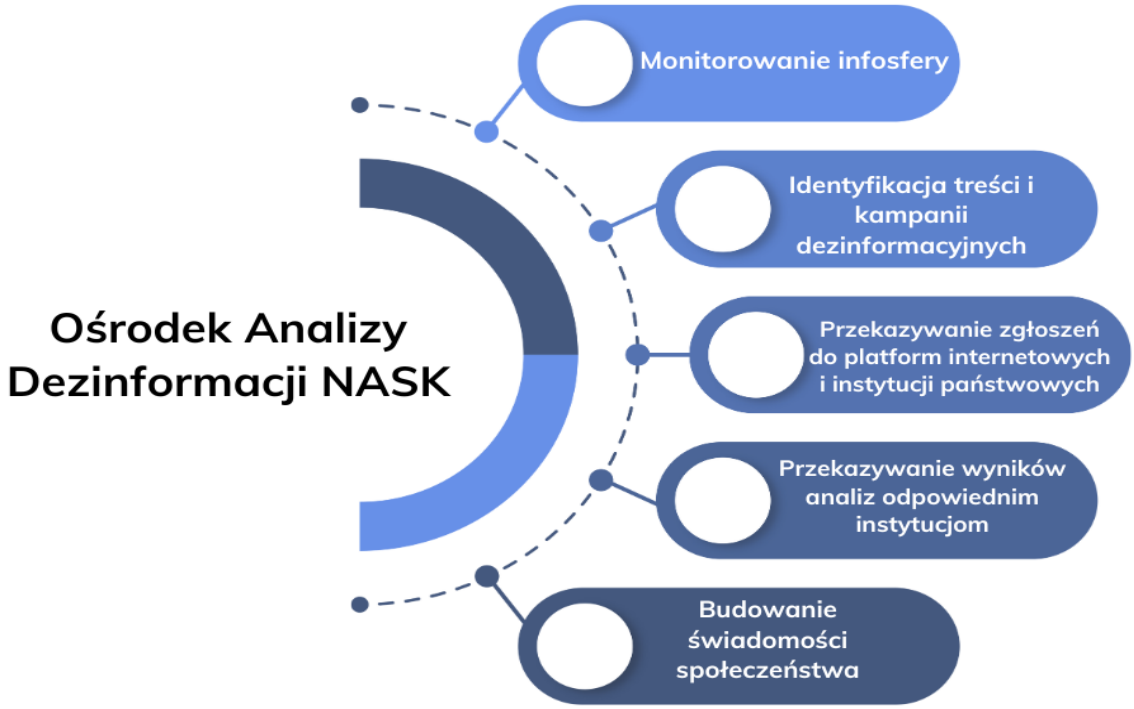
Mając na uwadze ochronę procesu wyborczego - na podstawie zadań zleconych przez Ministra Cyfryzacji oraz w perspektywie wyborów prezydenckich w 2025 r. - już od stycznia 2025 r. w NASK podjęto szereg działań na rzecz monitorowania infosfery podczas kampanii i procesu wyborczego. Komórką odpowiedzialną za to zadanie był OAD NASK.

Rola NASK OAD

Do zadań NASK PIB należy realizacja projektów związanych z zapewnieniem bezpieczeństwa Internetu, a także działalność badawczo-rozwojowa w zakresie opracowywania rozwiązań

zwiększających wydajność, niezawodność i bezpieczeństwo sieci teleinformatycznych oraz innych złożonych systemów sieciowych. Instytut angażuje się również w prace naukowe i rozwój rozwiązań technologicznych wykorzystywanych przez instytucje publiczne, firmy prywatne i obywateli.

Natomiast działający w ramach NASK OAD prowadzi stały monitoring infosfery oraz opracowuje analizy dotyczące rozpowszechniania i identyfikacji treści dezinformacyjnych oraz kampanii dezinformacyjnych (operacji wpływu). Do kluczowych zadań w tym obszarze zaliczyć należy: identyfikowanie treści szkodliwych, przekazywanie zgłoszeń do platform internetowych lub instytucji państwowych, analizę narracji dezinformacyjnych bądź szerszych kampanii dezinformacyjnych, przekazywanie wyników analiz odpowiednim instytucjom oraz budowanie świadomości społeczeństwa w zakresie możliwych zagrożeń.



Rysunek 19: Zadania Ośrodka Analizy Dezinformacji

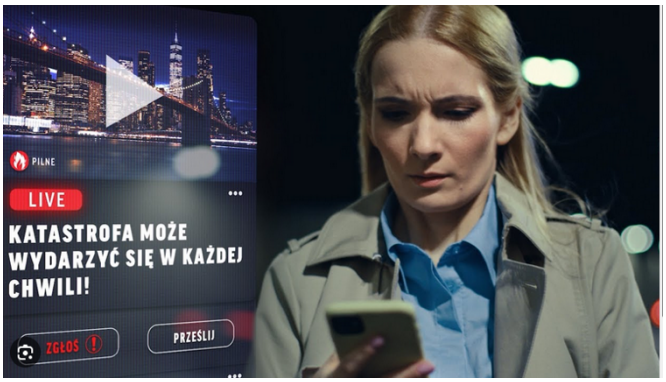
Zadania te wykonywane są w oparciu o analizę jawnych źródeł informacji, treści dezinformacyjnych zidentyfikowanych przez analityków w ramach monitoringu przestrzeni informacyjnej i zgłoszeń zewnętrznych pochodzących od użytkowników lub innych instytucji. Stałym monitoringiem analityków OAD NASK objęto ponad 3 tys. domen i profili/kont (w tym m.in. X, Facebook, Instagram Threads, TikTok, YouTube, LinkedIn, Bluesky, Wykop, Telegram).

W przypadku stwierdzenia wystąpienia incydentu dezinformacji treści raportowane są za pomocą ustalonych z administracjami platform systemów zgłoszeniowych. Najpoważniejsze naruszenia eskalowane są bezpośrednio poprzez dedykowane punkty kontaktowe. Oprócz ww. podejmowana jest także standardowa procedura zgłaszania incydentów z poziomu

operacyjnych kont użytkowników.

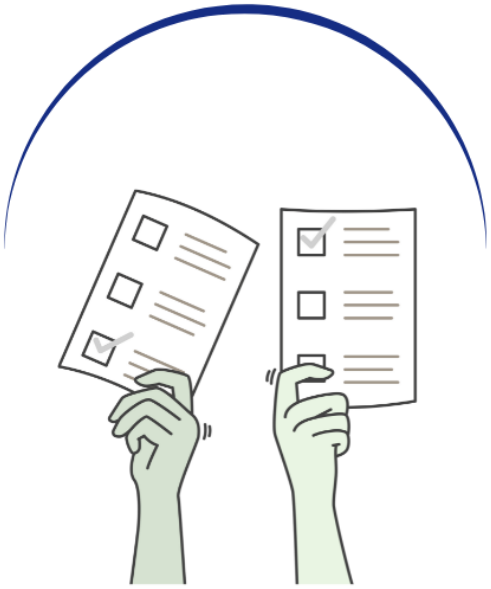
W ramach realizowanych działań MC powierzyło NASK zadanie pt. „Osłona informacyjna kampanii wyborczej 2025 r.", które stanowiło jeden z elementów międzyresortowego projektu „Parasol Wyborczy". W ramach zadania NASK realizował szereg działań, w tym:

- utrzymanie oraz prowadzenie serwisu bezpiecznewybory.pl jako kompendium wiedzy o procesie wyborczym. W ramach tych działań opracowano łącznie ponad 50 publikacji o charakterze informacyjno-edukacyjnym dotyczących kampanii wyborczej i wyborów (część z nich zamieszczono także na stronie głównej nask.pl);
- przyjmowanie (za pośrednictwem strony bezpiecznewybory.pl i adresu mailowego: dezinformacja@nask.pl) oraz weryfikacja zgłoszeń od obywateli dotyczących wystąpienia przypadków dezinformacji w infosferze; odpowiadanie na zgłoszenia i przekazywanie ich do administracji odpowiednich platform społecznościowych i/lub odpowiednich instytucji;
- stały monitoring infosfery pod kątem ryzyka ingerencji wewnętrznych (Domestic Information Manipulation and Interference) i zewnętrznych (FIMI - Foreign Information Manipulation and Interference);
- przeprowadzenie szkoleń i warsztatów dla Komitetów Wyborczych kandydatów na prezydenta, przedstawicieli administracji publicznej i jednostek samorządowych oraz pracowników ambasad RP w celu rozwijania umiejętności skutecznej identyfikacji oraz właściwej reakcji na dezinformację wyborczą; organizacja otwartych spotkań oraz szkoleń z udziałem dziennikarzy, przedstawicieli organizacji pozarządowych, oraz influencerów w celu edukowania i podnoszenia świadomości w zakresie zagrożeń wyborczych (łącznie odbyło się 11 otwartych spotkań, szkoleń i warsztatów). Spotkania te miały na celu rozwijanie umiejętności skutecznej identyfikacji oraz właściwej reakcji na dezinformację wyborczą. Wydarzenia przyjmowały formę wykładów z możliwością zadawania pytań, a ich tematem była edukacja na temat technik i zagrożeń dezinformacyjnych, a nie ocena poglądów politycznych uczestników;
- stała współpraca z partnerami i organizacjami zagranicznymi w zakresie wymiany informacji, spotkania robocze pod kątem analizy dezinformacji przedwyborczej i wniosków płynących z doświadczeń innych państw;
- produkcja i emisja kampanii informacyjno-edukacyjnej w formie spotów w telewizji, radiu, internecie, podnoszących poziom wiedzy na temat zjawiska dezinformacji pod hasłem: „Nie pozwól sobie odebrać głosu!". Kampania została uruchomiona w kwietniu i miała na celu przeciwdziałanie dezinformacji w okresie poprzedzającym wybory prezydenckie. Jej głównym przesłaniem było zachęcenie obywateli do świadomego udziału w głosowaniu i uodpornienie ich na manipulacje, które mogły zniechęcać do udziału w wyborach. W kampanii zwracano uwagę, że rezygnacja z głosu pod wpływem fake newsów, presji czy emocji to również forma utraty wpływu na



Rysunek 20: Kadr ze spotu kampanii edukacyjnej „Nie pozwól sobie odebrać głosu"

rzeczywistość. Przekaz kampanii był rozpowszechniany w mediach społecznościowych i internecie, głównie w formie krótkich spotów wideo.



Rysunek 21: Osłona informacyjna kampanii wyborczej 2025 r.

Analiza danych statystycznych dot. monitoringu przestrzeni informacyjnej obsługi zgłoszeń

W ramach działań OAD NASK, prowadzono stały monitoring infosfery pod kątem aktualnych i potencjalnych narracji dezinformacyjnych, przyjmowano i odpowiadano na zgłoszenia przypadków dezinformacji pochodzące od obywateli, a także przekazywano do platform treści dezinformacyjne oraz zgłaszano policji przypadki naruszeń ciszy wyborczej.

W okresie od 1 stycznia 2025 r. do 2 czerwca 2025 r. w ramach pracy Zespołu Szybkiego Reagowania i Wykrywania Dezinformacji obsłużono ok. 27,5 tys. zgłoszeń potencjalnych incydentów (dotyczących różnych kwestii dezinformacyjnych, wyborczych lub profili/kont). Spośród nich ok. 23,7 tys. zostało uznanych za zasadne i przekazane do dalszej obsługi. Procedowane zgłoszenia obejmowały m.in. przypadki dezinformacji, naruszenia ciszy wyborczej, aż 16 tys. z nich dotyczyło kont zidentyfikowanych w ramach wewnętrznego monitoringu OAD NASK jako nieautentyczne, działające w sposób skoordynowany (CIB Coordinated Inauthentic Behavior).

Rysunek 22: Dane dot. monitoringu przestrzeni informacyjnej i obsługi zgłoszeń

Spośród 5105 zgłoszeń zewnętrznych (przekazanych przez obywateli bądź instytucje) związanych z wyborami ok. 2,9 tys. zostało uznanych za zasadne i przekazane do dalszej obsługi. 2785 z nich dotyczyło treści udostępnianych za pośrednictwem platform społecznościowych i zostało przekazane do administracji platform. Spośród zgłoszeń wewnętrznych (będących wynikiem wewnętrznego monitoringu OAD) 1051 było związanych z wyborami.

Łącznie 3836 (2785 zewnętrznych i 1051 wewnętrznych) zgłoszeń zasadnych przekazano do administracji mediów społecznościowych i/lub instytucji. Zgłoszenia zawierały głównie: fałszywe lub manipulacyjne treści, przypadki podszywania się pod kandydatów lub komitety wyborcze; materiały wygenerowane za pośrednictwem narzędzi sztucznej inteligencji (AI), m.in. scam z wykorzystaniem wizerunków polityków rzekomo namawiających do inwestycji, w rzeczywistości będących oszustwem. Dodatkowo pracownicy OAD brali udział w procesie przywracania kont niektórych sztabów wyborczych.

Naruszenie ciszy wyborczej lub próby jej obejścia

W ramach swoich zakresów odpowiedzialności OAD NASK monitorował również łamanie ciszy wyborczej podczas obu tur wyborów prezydenckich w 2025 r. Zasady dotyczące ciszy wyborczej ujęto w art. 107. Kodeksu wyborczego: „*W dniu wyborów oraz wciągu 24 godzin poprzedzających ten dzień, zabronione jest prowadzenie agitacji wyborczej, w tym organizowanie zgromadzeń, pochodów i manifestacji, wygłaszanie przemówień oraz rozpowszechnianie materiałów wyborczych*" (art. 107 § 1.); „*Zabronione jest również prowadzenie działalności wyborczej w lokalu wyborczym oraz w budynku, w którym lokal wyborczy się znajduje*" (art. 107 § 2.).

W większości wypadków zgłoszenia kierowane do OAD NASK w czasie ciszy wyborczej w trakcie pierwszej i drugiej tury wyborów dotyczyły łamania lub prób jej obejścia np. poprzez publikację zdjęć kart do głosowania z zaznaczonym nazwiskiem wybranego kandydata. Na platformie X obserwowano hasztagi oraz materiały wygenerowane przy pomocy narzędzi

sztucznej inteligencji, które miały w sposób pośredni wspierać wybranych kandydatów. W mediach społecznościowych używane były hasztagi, grafiki wygenerowane przy pomocy narzędzi sztucznej inteligencji, określenia i emotikony jednoznacznie kojarzące się z wybranym politykiem. Wszystkie zgłoszenia przekazywano do właściwych platform i/lub instytucji.

Pierwsza tura wyborów - dane

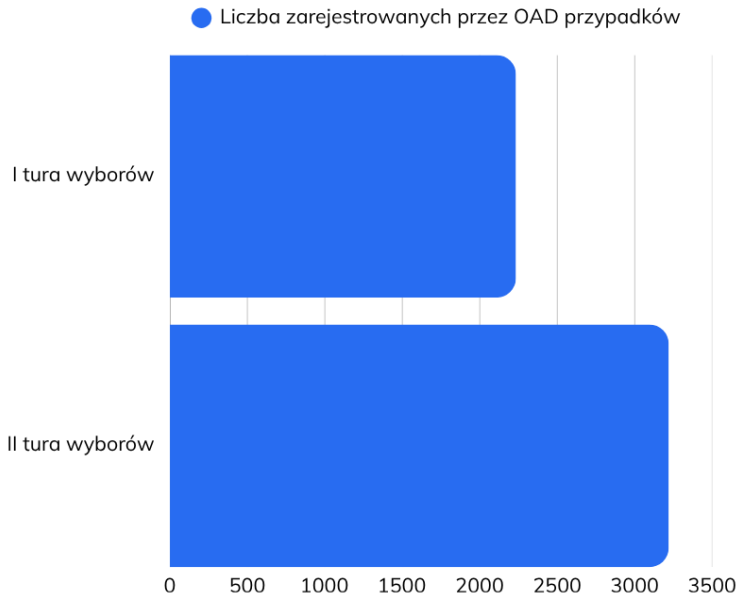
W dniach 16-18 maja 2025 r. w OAD NASK zarejestrowano 2233 przypadki związane z wyborami. Łącznie obywatele lub instytucje zgłosili 2022 treści, natomiast pozostałych 211 zgłoszeń wewnętrznych to efekt stałego monitoringu polskiej przestrzeni informacyjnej.

Łącznie 1325 przypadków (1114 zewnętrznych i 211 wewnętrznych) uznano za zasadne i przekazano do administracji odpowiednich platform mediów społecznościowych. Sprawy naruszeń ciszy wyborczej przekazywano również do Centralnego Biura Zwalczania Cyberprzestępczości (CBZC). Wśród raportowanych przypadków znalazło się także ok. 115 zgłoszeń dotyczących reklam w bibliotece Mety, które mogły być aktywne do 17 maja 2025 r.

Druga tura wyborów prezydenckich - dane

Do OAD NASK w okresie od 30 maja do 2 czerwca 2025 r. wpłynęło łącznie 3219 zgłoszeń wyborczych. 3071 przypadków zostało zgłoszonych przez obywateli i inne instytucje, podczas gdy pozostałe 148 pozycji zostało zidentyfikowanych dzięki ciągłemu monitorowaniu polskiej sfery informacyjnej prowadzonemu przez zespół analityczny.

Łącznie 1382 przypadków (1234 zewnętrznych i 148 wewnętrznych) spośród podanych powyżej zostało ocenionych jako zasadne i przekazanych do administracji odpowiednich platform społecznościowych. Przypadki dotyczące naruszeń ciszy wyborczej przekazano równolegle do CBZC.



Rysunek 23: II tura wyborów prezydenckich

Analiza narracji wykorzystywanych w dezinformacji w okresie wyborczym

Badanie i analiza dezinformacji w infosferze są prowadzone przez OAD NASK wg. taksonomii DISARM Framework[6], która jest metodologią analizowania, mapowania oraz przeciwdziałania kampaniom dezinformacyjnym, polegającą na opisywaniu procesów tworzenia operacji i ułatwianiu skoordynowanych odpowiedzi.

W okresie kampanii wyborczej zidentyfikowano szereg tematów wykorzystywanych do działań dezinformacyjnych. W szczególności wyróżnić należy:

- wizerunek kandydata: zdolność do pełnienia funkcji, obraźliwe lub nieodpowiednie zachowanie, działanie w cudzym interesie, skorumpowanie;
- popularność kandydata: skala poparcia, kontrowersyjne poparcie;
- uczciwość wyborów: oszustwa wyborcze, nieprawidłowości wyborcze, głosowanie osób niebędących obywatelami, podważanie wyników wyborów, przekupywanie wyborców;
- obietnice wyborcze kandydata: skrajne stanowiska, zmniejszenie bezpieczeństwa, zakończenie popularnych programów, odrzucenie tradycji;
- teorie spiskowe: kontrola informacji, zbliżające się zamieszki/wojna domowa, anulowane wybory.

Powyższe tematy stanowią najczęściej występujące wątki dezinformacyjne obserwowane również podczas kampanii wyborczych w Polsce. Struktura i cele rozpowszechniania dezinformacyjnych treści często bowiem pozostają podobne, podczas gdy konkretne narracje dostosowane są do bieżących wydarzeń, uwarunkowań politycznych oraz aktualnych napięć społecznych.

Od początku 2025 r. w kontekście narracji wyborczych najczęściej obserwowano narracje dezinformacyjne odwołujące się do wizerunku kandydatów, uczciwości wyborów oraz prezentujące teorie spiskowe. Poniżej przedstawiono najczęstsze narracje związane z wyborami prezydenckimi w Polsce:

- możliwe zastosowanie „wariantu rumuńskiego" polegające na unieważnieniu wyborów i aresztowaniu kandydatów niewygodnych dla obecnej władzy; w ramach tej narracji sugerowano m.in., że ABW kontaktuje się z rumuńskimi służbami w celu unieważnienia wyborów w Polsce (narracje antypaństwowe);
- możliwa ingerencja Unii Europejskiej w wybory prezydenckie w Polsce, m.in. przedstawianie „Europejskiej Tarczy Demokracji" stworzonej przez UE jako narzędzia wpływania na wynik wyborów (narracje antyunijne);
- wysokie ryzyko sfałszowania wyniku wyborów, np. poprzez wielokrotne głosowanie na podstawie zaświadczeń o prawie do głosowania lub udział komisji w celowym unieważnianiu lub zmienianiu głosów; w ramach tej narracji sugerowano m.in. konieczność zabrania do lokalu wyborczego świeczki, aby „zapobiec potencjalnemu fałszowaniu głosowania";
- podkreślanie rzekomego wpływu obywateli Ukrainy na wybory, m.in. sugerowanie, że zaczną masowo otrzymywać polskie obywatelstwo i prawa wyborcze (narracje antyukraińskie);

[6] Źródło: https://www.disarm.foundation/framework

- przedstawianie wybranych kandydatów jako niestabilnych psychicznie lub uzależnionych od substancji psychoaktywnych;
- tezy wskazujące na możliwość przeprowadzenia zamachu terrorystycznego podczas wyborów;
- fałszywe treści o przesunięciu lub zmianie terminu wyborów.

Wśród regularnie powracających narracji należy dodatkowo wskazać na dezinformację dotyczącą migracji oraz ochrony granic, które częstokroć pojawiały się również w kontekście wyborczym.

Na podstawie analizy powyższych narracji można zauważyć, że dezinformacja wyborcza służyła przede wszystkim budowaniu metanarracji podważającej fundamenty procesów demokratycznych. Narracje te - obejmujące oskarżenia o fałszerstwa wyborcze, manipulacje wynikami, ingerencje zewnętrzne oraz teorie spiskowe dotyczące zamachów i anulowania wyborów - miały na celu wzbudzenie poczucia zagrożenia, chaosu i niepewności. Ich powtarzalność i emocjonalny charakter prowadzić mogą do erozji zaufania społecznego, polaryzacji oraz delegitymizacji instytucji państwowych. W efekcie doszło do wytworzenia spójnej metanarracji, według której demokracja w Polsce jest fikcją, a wybory - jedynie pozorem wolnego wyboru. Należy dodatkowo podkreślić, że wskazana metanarracja zbieżna jest z narracjami przekazywanymi w niektórych zagranicznych infosferach, m.in. rosyjskiej i białoruskiej.

Monitoring rosyjskich, białoruskich oraz chińskich przestrzeni informacyjnych

W ramach monitoringu analizowano rosyjskie, białoruskie oraz chińskie infosfery pod kątem rozpowszechniania narracji odnoszących się do procesu wyborczego w RP lub mogących wpływać na jego przebieg.

Rosja

Główne rosyjskie tezy i narracje dezinformacyjne zidentyfikowane w okresie przedwyborczym w polskiej infosferze służyły podważeniu zaufania do procesów demokratycznych i/lub współpracy międzynarodowej, a także pogrążeniu kandydatów, którzy prezentowani byli jako pro-zachodni. Wyróżnić należy w szczególności:

- prezentowanie Polski jako „marionetki NATO" - Polskę przedstawiano jako niesuwerennego aktora służącego interesom USA i dążącego do eskalacji sytuacji w Europie Środkowej i Wschodniej;
- podważanie szans Ukrainy na zwycięstwo w konflikcie - w narracji tej wskazywano, że „Ukraina jest skazana na zagładę", a Zachód ma być zmęczony udzielaniem wsparcia, które rzekomo jest pozbawione sensu;
- przedstawianie Polski jako „fałszywej demokracji" - według tej narracji proces wyborczy miał być kontrolowany przez elity prowojenne (PO-PiS), co miało zniechęcać do aktywności obywatelskiej;
- sugerowanie, że radykalny światopogląd to jedyny „patriotyczny wybór";

– osoby o radykalnych, nacjonalistycznych i antyukraińskich poglądach pozycjonowano jako obrońców polskiej tożsamości.

Białoruś

Celem białoruskich służb specjalnych w polskiej infosferze było dyskredytowanie demokratycznych procesów poprzez przedstawianie polskich wyborów jako chaotycznych, bezsensownych i kontrolowanych z zewnątrz. W ten sposób legitymizowano autorytaryzm władz Białorusi, którą prezentowano jako państwo stabilne i suwerenne.

Komunikaty dezinformacyjne rozpowszechniane przez służby białoruskie opierano głownie na strachu. Poruszały one kwestie możliwej „wojny domowej", „upadku instytucji" i „upadku moralnego".

Chiny

Nie zaobserwowano bezpośredniego zaangażowania Chin w kampanię, którego celem byłoby wpływanie na wybory w Polsce. Państwo Środka wykorzystało jednak do swojej polityki wewnętrznej rosyjskie narracje dotyczące Polski. Spełniały one dwa zadania: wzmacniały nastroje antyzachodnie i antydemokratyczne oraz umożliwiały swobodny przepływ rosyjskich narracji do infosfery (tzw. information laundering) za pośrednictwem kanałów powiązanych z Pekinem, takich jak TikTok / RedNote lub inne media kontrolowane przez państwo.

Prezentacja takich narracji miała dowodzić, że demokracja jest wadliwym systemem, który może prowadzić jedynie do podziałów i niepokojów społecznych. Opisywane przez chińskie agencje medialne polskie wybory przedstawiano jako walkę „proeuropejskiego i proukraińskiego" świata z „proTrumpowskim i antyukraińskim".

Na działania Państwa Środka w zakresie opisywania procesu wyborów w Polsce miało wpływ porozumienie z Rosją, rozumiane jako bliskie strategiczne partnerstwo w dziedzinie wojskowości, gospodarki i spraw międzynarodowych, a także wymiany informacji. TASS i państwowa agencja informacyjna Xinhua nawiązały umowę o współpracy (rosyjskie media są oficjalnie obecne w sinosferze i kształtują opinię publiczną w kwestiach związanych z polityką zagraniczną i geopolityką)

Przykłady wybranych operacji wpływu związanych z wyborami prezydenckimi

Między styczniem a majem 2025 r. do administratorów platform internetowych zgłoszono ponad 16 tys. kont powiązanych z różnymi operacjami wywierania wpływu na Facebooku, X i platformie TikTok. Niektóre operacje były bezpośrednio związane z wyborami prezydenckimi, inne pośrednio, a część dotyczyła wyborów tylko w kontekście narracji wspierających, które mogły mieć wpływ na sposób postrzegania polityki przez wyborców.

W okresie wyborczym OAD NASK zidentyfikował na portalach społecznościowych również profile podszywające się pod kandydatów na prezydenta i rozpowszechniające treści

pochodzące z innych kont. Niektóre z profili osiągały znaczące zasięgi i zdołały zgromadzić od kilkudziesięciu do kilkuset tysięcy obserwujących. Po interwencji OAD NASK profile na TikToku zostały zablokowane. Tylko do końca kwietnia zidentyfikowano 176 incydentów na różnych platformach związanych z podszywaniem się pod kandydatów na urząd prezydenta. Skutecznie udało się zablokować 169 takich kont (96 proc.).

Operacja A

Na początku kwietnia 2025 r. w wyniku prac OAD NASK ujawniono trwającą w anglojęzycznej przestrzeni informacyjnej operację dezinformacyjną dotyczącą m.in. Polski i procesu wyborczego, opartą na masowej działalności siatek nieautentycznych kont (tzw. botów). Doprowadziło to do neutralizacji ponad 15 tysięcy kont działających w ramach tej kampanii. Operacja była prowadzona głównie za pośrednictwem platformy X i wykorzystywano w niej zmanipulowane materiały wideo, grafiki oraz kody QR/puzzle.

Rozpowszechniane przez boty wpisy, fałszywie informowały m.in. o ryzyku wystąpienia zamachów terrorystycznych w Polsce podczas wyborów 18 maja 2025 r. Łącznie zidentyfikowano ponad 100 wpisów i materiałów wideo rozpowszechnionych w ramach tej kampanii, które były publikowane przez wybrane konta, a następnie amplifikowane przez siatki botów.

Mimo że w trakcie operacji poruszano polskie wątki, nie odnotowano przenoszenia się tych treści do polskojęzycznej infosfery. Operacja skierowana była głównie do odbiorców anglojęzycznych.

Podczas kampanii w dystrybuowanych wiadomościach zamieszczano m.in. kody QR i puzzle. Takie działanie służyło zaangażowaniu sił i środków analityków w celu przekierowania ich uwagi z innych operacji dezinformacyjnych. Działania aktorów dezinformacji koncentrowały się głównie na mediach, instytucjach i środowiskach badawczych, starając się przeciążyć ich zasoby i wprowadzić fałszywe narracje do głównego nurtu dyskursu publicznego, jednocześnie oddziałując również na opinię publiczną. Operacja ta stanowiła kolejny element trwającej od kilku lat kampanii dezinformacyjnej.

Operacja B

W ramach prac OAD NASK od końca 2024 r. wykrywano i za pomocą zgłoszeń przerywano łańcuchy dezinformacyjne operacji prowadzonej przez rosyjską Social Design Agency, mającej na celu zmianę opinii publicznej na niekorzyść Ukrainy, osłabienie jej wsparcia ze strony Zachodu oraz uderzanie w instytucje unijne. W niewielkim stopniu w ramach tej operacji rozpowszechniano treści dezinformacyjne dotyczące wybranych kandydatów.

Dzięki działaniom OAD NASK w ostatnim półroczu zidentyfikowano i doprowadzono do usunięcia ponad 400 kont funkcjonujących w ramach kampanii. W operacji wykorzystywano m.in. zmodyfikowane przez sztuczną inteligencję materiały wideo, strony i profile podszywające się pod ukraińskie instytucje i siatki botów w mediach społecznościowych. Rozpowszechniano dezinformację skierowaną do odbiorców w Polsce, USA, Ukrainie i Europie.

Operacja C

W okresie wyborczym zespół OAD NASK analizował operację dezinformacyjną wymierzoną w jednego z kandydatów na prezydenta oraz organizacje ukraińskie działające na terenie Polski. Oprócz dezinformacji w cyberprzestrzeni pojawiały się także próby wpływania na pracę urzędów miast poprzez wysyłanie maili z wnioskami o uzyskanie zgody przez mniejszość ukraińską na rzekome wiece poparcia kandydata.

Operacja ta miała na celu wywołanie wrażenia, że Ukraińcy w Polsce mają lepsze zdanie o kandydacie, który rzekomo przedkłada ukraińską rację stanu ponad polską. W trakcie tej kampanii zidentyfikowano i zgłoszono 9 domen zawierających zmodyfikowane za pomocą AI zdjęcia z oficjalnej strony polityka.

Operacja D

W wyniku prac prowadzonych przez NASK wykryto i przeanalizowano siatkę ponad 220 stron tworzonych z wykorzystaniem AI operujących na Facebooku. Treści publikowane na analizowanych stronach można określić jako tzw. AI slope oraz boomertrap, które coraz częściej pojawiają się w sieci, wraz z łatwiejszym dostępem do sztucznej inteligencji. W treściach tych poruszano wątki religijne, co może świadczyć o pozycjonowaniu profili pod osoby starsze lub o określonym światopoglądzie.

Strony powiązane były z witrynami prowadzonymi m.in. przez administratorów z Armenii oraz Maroka i tworzyły rozbudowaną infrastrukturę - najprawdopodobniej w celu dalszego wykorzystania lub odsprzedaży.

NASK zgłaszał (wielokrotnie, bez reakcji platform społecznościowych) strony łamiące regulamin platformy i nadal prowadzi monitoring siatki na wypadek dalszego wykorzystania stworzonej infrastruktury w celach dezinformacyjnych.

Operacja E

Operacja w środowisku cyfrowym „Spotted” - wskutek zgłoszenia od obywatela OAD NASK potwierdził, iż jeden z portali typu „Spotted” na Facebooku celowo udostępnił fałszywy post budujący znaczne zasięgi, by następnie włączyć go w kampanię wyborczą poprzez dodanie grafiki zachęcającej do głosowania na jednego z kandydatów.

Ten sam post został udostępniony i edytowany w ten sam sposób przez kilkanaście innych kont typu „spotted” na terenie całego kraju, zyskując znaczące zasięgi na Facebooku. OAD NASK przeanalizował 12 kont typu „spotted” zamieszanych w incydent, ustalając ich powiazania z konkretnymi osobami i podmiotami gospodarczymi, po czym przekazał materiały do ABW.

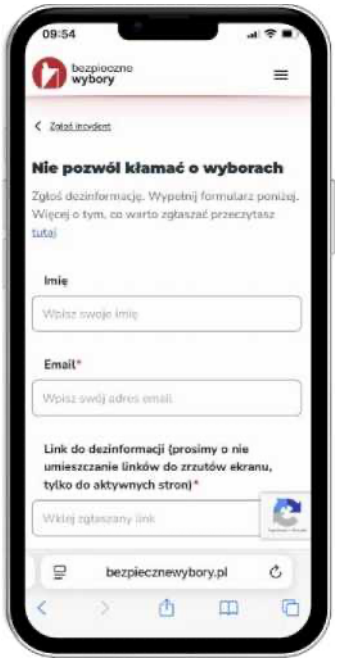
Operacja F

W ramach prowadzonego monitoringu wykryto kampanię wykorzystującą metodę rozpowszechniania fałszywych treści poprzez komentarze publikowane pod postami na portalu Facebook. W treści komentarzy zamieszczany był link do artykułów na zewnętrznej witrynie, zawierających fałszywe, wytworzone przy wykorzystaniu AI materiały. Artykuły dotyczyły kandydatów, ich rzekomych powiązań z rosyjskimi oligarchami, zmiany terminu głosowania czy zamachów na życie startujących w wyborach. OAD NASK systematycznie zgłaszał przypadki wystąpienia kampanii i podjął starania w kierunku zablokowania witryny.

Operacja G

W drugim tygodniu maja 2025 r.zgłoszono potencjalną ingerencję w wybory poprzez publikację reklam politycznych na platformach Mety. Trwająca od kwietnia kampania w tym okresie (27 kwietnia - 3 maja) znacząco zwiększyła nakłady reklamowe i tym samym wpływ na opinię publiczną. Analiza OAD NASK ujawniła możliwe powiązania tej konkretnej kampanii z podmiotami zagranicznymi.

Analizie poddano 135 reklam, które wyświetlane były na obszarze Polski, promując jednego z kandydatów na prezydenta i uderzając w dwóch innych. Zaangażowane w kampanię konta reklamowe w ciągu 7 dni wydały na promocję więcej niż jakikolwiek komitet wyborczy. NASK niezwłocznie przekazał informacje o operacji do służb, a zgłoszenia profili publikujących reklamy - do Mety. Po publikacji komunikatu na stronie NASK reklamy stały się nieaktywne, najprawdopodobniej wskutek działań osoby opłacającej reklamy (automatyczne wygaśnięcie bądź celowe wyłącznie reklam).



Rysunek 24: Bezpiecznewybory.pl

Według zapewnień platformy, administratorzy kampanii prowadzili ją z obszaru Polski (weryfikacja numerem telefonu, dokumentem tożsamości oraz lokalizacja urządzenia), jednak analizy domen wykonane przez OAD NASK wykazały powiązania operacji z obywatelami i podmiotami gospodarczymi z państw trzecich. Należy mieć na uwadze fakt, iż przejście takiej cyfrowej weryfikacji leży w zakresie możliwości

zewnętrznych aktorów dezinformacji, nie była zatem uznana za przesłankę wystarczającą do podważenia ewidentnych powiązań zagranicznych.

Ponadto, wieczorem 9 maja 2025 r. zawiadomiono OAD NASK o podejrzanej propozycji płatnej współpracy, otrzymanej przez jednego z influencerów. Niezwłocznie przeprowadzono analizę powiązań podmiotów i osób stojących za zorganizowaną akcją rekrutowania influencerów, którzy za odpowiednim wynagrodzeniem mieli promować określone tematy i wartości w okresie przedwyborczym. Zespół OAD NASK w sposób anonimowy uzyskał informacje nt. kampanii prowadzonej przez jedną z fundacji. Z wypowiedzi przedstawiciela fundacji wynikło, iż akcja nie ma mieć charakteru politycznego, jednak zaangażowani influencerzy będą poruszać tematy wrażliwe społecznie w zależności od tematów popularnych podczas kampanii. Deklarowano, że nie przewiduje się popierania konkretnego kandydata ani nie ma celu publikacji treści politycznych, jednak jest to program dotyczący wyborów i bazuje na tematach w danej chwili najbardziej angażujących opinię publiczną.

OAD NASK ustalił wspólne zagraniczne powiązania (w zakresie niektórych podmiotów i osób) tej operacji z kampanią reklamową prowadzoną przez strony na platformie Facebook. Sprawy zostały zgłoszone przez NASK do ABW. Prokuratora wszczęła śledztwo w powyższej sprawie.

Operacja H

28 maja OAD NASK ujawnił kolejną potencjalną operację wpływu zagranicznego, bazującą na grafikach w serwisach Facebook oraz X. Kampania prowadzona przez polski profil znanej międzynarodowej organizacji, agitowała na rzecz jednego z kandydatów na prezydenta i dyskredytowała drugiego. Operacja wpływu w całości opierała się na wpisach w mediach społecznościowych oraz sugestywnych grafikach i wbrew doniesieniom medialnym, w tym wypadku nie stwierdzono wykorzystania reklam. OAD NASK niezwłocznie zgłosił kampanię moderacji platform Facebook (skuteczna) oraz X (nieskuteczna).

W tym zakresie należy przywołać zapisy Kodeksu wyborczego definiujące prawne działania mogące stanowić agitację wyborczą (zdefiniowaną w art. 105 § 1 Kodeksu wyborczego). Zgodnie z Kodeksem agitację mogą podejmować wyłącznie komitety wyborcze uczestniczące w wyborach oraz wyborcy. Prowadzenie agitacji wyborczej przez inne podmioty stanowi naruszenie przepisów Kodeksu wyborczego.

Aplikacja do weryfikacji zaświadczeń pozwalających na głosowanie w dowolnym lokalu wyborczym

W trakcie wyborów miało miejsce wykorzystywanie przez niektórych członków komisji wyborczych aplikacji stworzonej przez Stowarzyszenie Ruch Kontroli Wyborów (RKW)[7] mającej służyć do weryfikacji zaświadczeń pozwalających na głosowanie w dowolnym lokalu wyborczym. Zachęcanie do używania tej aplikacji było także promowane w mediach społecznościowych, w tym przez polityków.

[7] https://stowarzyszenierkw.org/polityka/wybory/jak-sprawdzic-czy-juz-ktos-nie-glosowal-na-zaswiadczenie-o-prawie-do-glosowania-w-innym-miejscu-niz-miejsce-zamieszkania/

Rysunek 25: Strona internetowa zachęcająca do korzystania z nieautoryzowanej aplikacji

Rysunek 26: Wpis na portalu X zachęcający do korzystania z nieautoryzowanej aplikacji

Państwowa Komisja Wyborcza przypominała o obowiązującym wzorze zaświadczenia o prawie do głosowania, określonym w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji, oraz o obowiązku obwodowych komisji wyborczych polegającym na odebraniu zaświadczenia od wyborcy, dołączeniu go do dokumentacji wyborczej i wydaniu na tej podstawie karty do głosowania. Komisja jednoznacznie także podkreślała, że nieujęta w przepisach prawa procedura weryfikacji zaświadczeń na podstawie nieautoryzowanej aplikacji nie mogła stanowić podstawy do odmowy wydania karty do głosowania.

Pomimo jednoznacznych wytycznych, na obszarze właściwości Okręgowej Komisji Wyborczej w Krakowie podczas pierwszego głosowania odnotowano dwa przypadki odmowy wydania kart do głosowania osobom uprawnionym, które przedłożyły ważne zaświadczenia o prawie do głosowania. Odmowa ta została uzasadniona zastrzeżeniami zgłoszonymi przez zastępczynię przewodniczącego komisji, która – powołując się na wyniki działania aplikacji zainstalowanej w telefonie komórkowym – uznała, że osoby te miały już rzekomo oddać głos wcześniej. Analogiczne zdarzenie miało miejsce również na obszarze działania Okręgowej Komisji Wyborczej w Warszawie. W obu przypadkach komisarze wyborczy podjęli decyzję o odwołaniu ze składu komisji osób odpowiedzialnych za niezgodne z prawem działania.

Z całą stanowczością należy podkreślić, że żadne przepisy Kodeksu wyborczego ani wytyczne Państwowej Komisji Wyborczej nie przewidują możliwości stosowania niezatwierdzonych narzędzi informatycznych w procedurze dopuszczania do głosowania wyborców legitymujących się ważnym zaświadczeniem. Praktyka ta nie tylko groziła spowodowaniem chaosu organizacyjnego w lokalach wyborczych, lecz także przyczyniła się do wywołania atmosfery podejrzliwości i napięcia wobec obywateli głosujących na podstawie zaświadczeń, co stawiało ich niesłusznie w krzywdzącym świetle. Działania te mogły zniechęcić część wyborców do skorzystania z przysługującego im prawa, podważając tym samym fundamentalną zasadę powszechności udziału w wyborach.

Najpoważniejsze zastrzeżenia budzą jednak przypadki, w których – na podstawie błędnych i niezweryfikowanych wyników działania wspomnianej aplikacji – członkowie obwodowych komisji wyborczych faktycznie odmówili wydania kart do głosowania osobom legitymującym się ważnym zaświadczeniem o prawie do głosowania. Tego rodzaju działania należy uznać za

jednoznacznie sprzeczne z obowiązującym prawem i wysoce naganne. Ograniczenie praw wyborczych obywateli może następować wyłącznie w oparciu o wyraźną podstawę prawną i podlegać musi ścisłej kontroli legalności – nie może natomiast wynikać z subiektywnych ocen, przypuszczeń ani stosowania nieautoryzowanych i niesprawdzonych narzędzi technicznych. Zważywszy, że problem dotyczył potencjalnie wszystkich osób głosujących na podstawie zaświadczenia, incydenty tego rodzaju należy traktować jako poważne i rażące naruszenie prawa wyborczego, które mogło prowadzić do bezpodstawnego pozbawienia obywateli prawa udziału w głosowaniu.

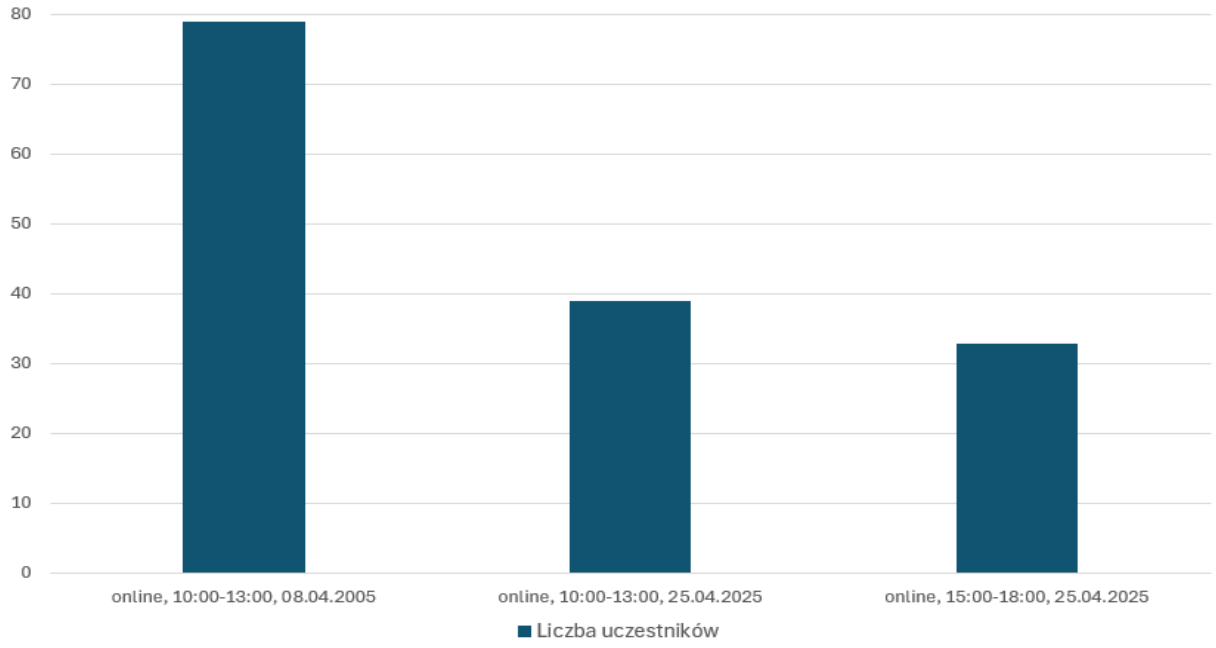
Dezinformacja stanowi jedno z kluczowych zagrożeń dla stabilności demokratycznych społeczeństw. Jej celem jest eskalacja napięć politycznych, pogłębianie istniejących podziałów społecznych oraz radykalizacja postaw obywateli. W skrajnych przypadkach może prowadzić do podważania legitymacji demokratycznie wybranych władz przez część społeczeństwa, co zagraża integralności procesów wyborczych i zaufaniu do instytucji państwowych.

W obliczu rosnącego zagrożenia dezinformacją istotne jest podejmowanie inicjatyw edukacyjnych z zakresu rozpoznawania fałszywych treści i właściwego reagowania.

W okresie wyborczym do zadań OAD NASK należało przeprowadzenie stacjonarnych szkoleń pt. „Bądźmy cyberodporni!", w których wzięli udział przedstawiciele komitetów wyborczych kandydatów na Prezydenta RP. Zorganizowano 2 szkolenia stacjonarne w siedzibie NASK: 28 lutego 2025 r. w spotkaniu wzięło udział 12 osób z 7 komitetów wyborczych; z kolei 28 marca 2025 r. - 13 osób z 5 komitetów wyborczych. Eksperci NASK podczas 3-godzinnego spotkania przekazywali wiedzę na temat dezinformacji oraz najważniejszych cyberzagrożeń z elementami cyberhigieny.

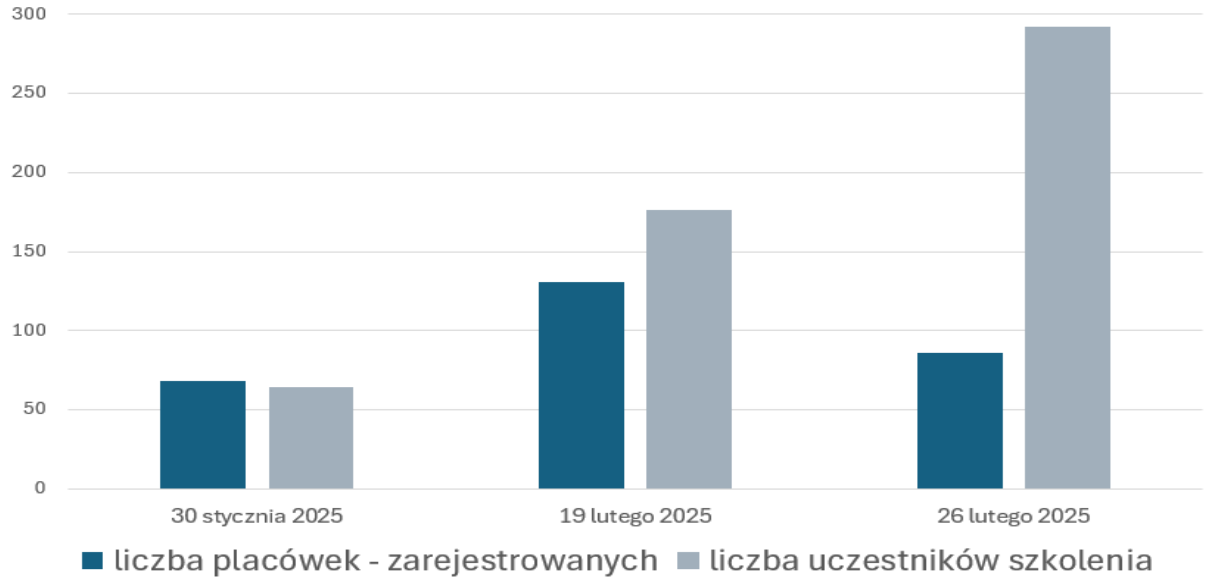
Rysunek 27: Zadania NASK w zakresie bezpieczeństwa wyborów

Zorganizowano 3 spotkania online dla 151 uczestników z 77 placówek dyplomatycznych i MSZ na całym świecie.



Rysunek 28: Liczba uczestników

Przeprowadzono ponadto warsztaty w formule online dla 532 uczestników z 285 jednostek samorządu terytorialnego, podczas których eksperci NASK przekazywali wiedzę na temat dezinformacji z elementami cyberhigieny.



Rysunek 29: Uczestnicy spotkań

Kluczowe znaczenie ma systematyczne podnoszenie świadomości społeczeństwa na temat zagrożeń informacyjnych. Edukacja obywateli, rozwijanie kompetencji medialnych oraz budowanie odporności na manipulację są niezbędne do ochrony przestrzeni informacyjnej przed wpływami zewnętrznymi.

3 ZAANGAŻOWANIE KRAJOWYCH SŁUŻB KONTRWYWIADOWCZYCH (ABW I SKW) ORAZ MINISTERSTWA SPRAW ZAGRANICZNYCH W PROCES ZAPEWNIANIA BEZPIECZEŃSTWA WYBORCZEGO

W obliczu narastających zagrożeń hybrydowych oraz coraz bardziej złożonych operacji wpływu prowadzonych przez podmioty zewnętrzne, kluczową rolę w systemie ochrony procesu wyborczego odgrywają zarówno krajowe służby kontrwywiadowcze – ABW i Służba Kontrwywiadu Wojskowego (SKW) – jak i MSZ, w szczególności Departament Komunikacji Strategicznej i Przeciwdziałania Dezinformacji Międzynarodowej (DKSiPDM).

ABW, jako wiodąca instytucja odpowiedzialna za bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, realizuje działania ukierunkowane na identyfikację i neutralizację zagrożeń informacyjnych, technologicznych oraz operacyjnych, które mogą wpływać na integralność procesu wyborczego. W ramach swoich kompetencji ABW prowadzi monitoring aktywności podmiotów zewnętrznych, analizę ryzyk systemowych oraz współpracę z innymi instytucjami odpowiedzialnymi za bezpieczeństwo państwa.

SKW, jako służba wyspecjalizowana w ochronie kontrwywiadowczej Sił Zbrojnych RP, koncentruje się na zabezpieczeniu infrastruktury krytycznej oraz przeciwdziałaniu zagrożeniom o charakterze wojskowym (w tym w sferze cyfrowej). Jej działania mają na celu eliminację potencjalnych wektorów ingerencji w proces wyborczy, w tym poprzez ochronę systemów teleinformatycznych wykorzystywanych przez instytucje państwowe.

MSZ, poprzez wyspecjalizowany DKSiPDM, pełni istotną funkcję w zakresie przeciwdziałania zagranicznym operacjom wpływu prowadzonym w przestrzeni międzynarodowej. Działania MSZ koncentrują się na identyfikacji i demaskowaniu kampanii dezinformacyjnych wymierzonych w proces wyborczy w Polsce, a także na współpracy z partnerami międzynarodowymi w zakresie wymiany informacji i koordynacji odpowiedzi strategicznej.

W poniższym podrozdziale przedstawione zostały informacje z zakresu, charakterystyki oraz skuteczności działań podejmowanych przez ABW, SKW oraz MSZ w ramach operacyjnego i strategicznego zabezpieczenia procesu wyborczego, ze szczególnym uwzględnieniem aspektów kontrwywiadowczych, cyberbezpieczeństwa oraz przeciwdziałania operacjom wpływu prowadzonym przez podmioty państwowe i niepaństwowe.

3.1 AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO (ABW)

ABW - w ramach działań wpisujących się w założenia "Parasola Wyborczego" ukierunkowanych na zabezpieczenie niezakłóconego przebiegu wyborów prezydenckich w RP - na bieżąco rozpoznawała wszelkie zdarzenia i sygnały mogące wskazywać na podejmowanie - zwłaszcza przez państwa trzecie - prób wpływania na sytuację wewnętrzną RP, w tym w obszarze potencjalnej ingerencji w proces wyborczy poprzez działania w cyberprzestrzeni i sferze informacyjnej. Służba podjęła się realizacji szeregu czynności w następujących obszarach:

Wzmacnianie odporności organów wyborczych na zagrożenia w cyberprzestrzeni

Zespół CSIRT GOV, znajdujący się w strukturze ABW, prowadził ocenę bezpieczeństwa systemów i sieci IT wykorzystywanych w procesie wyborczym, podczas której na bieżąco informował przedstawicieli organów wyborczych o wykrytych podatnościach w infrastrukturze, ze szczególnym uwzględnieniem tych, które wymagały podjęcia niezwłocznych działań przez administratorów. W ramach oceny bezpieczeństwa Zespół CSIRT GOV (ABW) przeprowadzał również testy socjotechniczne, które miały na celu weryfikację świadomości i odporności użytkowników systemów we wskazanych podmiotach.

Ponadto celem wzmacniania świadomości użytkowników przeprowadzono szereg szkoleń personelu zaangażowanego w organizację przebiegu wyborów w zakresie zagrożeń w cyberprzestrzeni. Szkoleniami objęto zarówno szczebel kierowniczy, jak i kadrę pracowniczą, w tym również administratorów systemów i sieci.

Rozpoznawanie cyberzagrożeń oraz obsługa incydentów

W ramach przedsięwzięcia "Parasol Wyborczy" Zespół CSIRT GOV (ABW) prowadził wzmożony monitoring zagrożeń w cyberprzestrzeni RP. Szczególną uwagę zwrócono na działania dezinformacyjne, co wymagało monitorowania cyberprzestrzeni w zakresie rejestrowanych domen, stron podszywających się pod instytucje oraz podmioty. Podjęte czynności wynikały z możliwości zaistnienia zagrożeń ze strony innych państw mogących angażować się w działania mające na celu destabilizację procesu wyborczego.

Od 1 lutego do 1 czerwca 2025 r. Zespół CSIRT GOV (ABW) zarejestrował łącznie 6744 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego w swoim obszarze kompetencyjnym, spośród których 1544 zostało zakwalifikowanych jako faktyczne incydenty bezpieczeństwa teleinformatycznego. Z tego 27 incydentów związanych było z oddziaływaniem na podmioty związane z procesem wyborczym. Przedstawione dane oraz statystyki nie zawierają informacji o działaniach podejmowanych w trybie niejawnym.

Incydenty podzielono - w zależności od rodzaju i charakteru zdarzenia - według kategorii:

***PODATNOŚĆ*, *SOCJOTECHNIKA*, *PUBLIKACJA*, *NIEDOSTĘPNOŚĆ*, *SKANOWANIE*, *ATAK*, *KASKADA*, *TREŚCI*, *WIRUS*.**

1. Kategoria PODATNOŚĆ związana była z identyfikowanymi przez Zespół CSIRT GOV (ABW) lukami bezpieczeństwa wynikającymi z podatności zasobów i usług dostępnych z poziomu sieci Internet podmiotów będących we właściwości CSIRT GOV (ABW). Łącznie w kategorii

tej zarejestrowano 583 incydenty, z czego 3 dotyczyły systemów i sieci właściwych dla instytucji związanych z procesem wyborczym.

2. Wśród aktywności rejestrowanej w kategorii SOCJOTECHNIKA Zespół CSIRT GOV (ABW) identyfikował wiadomości phishingowe, których celem było zarówno wyłudzenie danych logowania do usług elektronicznych lub innych danych wrażliwych, infekcja złośliwym oprogramowaniem, jak również wyłudzenie środków finansowych. W raportowanym okresie zarejestrowanych zostało 351 incydentów tej kategorii, z czego 5 dotyczyło instytucji związanych z procesem wyborczym.
3. W ramach kategorii PUBLIKACJA wystąpiły liczne upublicznienia danych wrażliwych, zawierające m.in. dane logowania do usług elektronicznych, prywatne klucze PGP czy informacje o specyfikacji infrastruktury teleinformatycznej instytucji. Odnotowano 269 incydentów o określonym charakterze, w tym 5 dotyczących instytucji związanych z procesem wyborczym.

4 Zespół CSIRT GOV (ABW) zarejestrował również liczne incydenty związane z kategorią NIEDOSTĘPNOŚĆ. Pośród niej identyfikowano głównie zdarzenia, które zaklasyfikowano jako ataki mające na celu wywołanie niedostępności świadczonej usługi. Wpływ na tę kategorię zagrożenia w głównej mierze miała również aktywność grup haktywistycznych, które swoje działania ukierunkowują na państwa NATO i Unii Europejskiej w związku z konfliktem zbrojnym w Ukrainie.

5 Ataki DoS/DDoS, za którymi stoją tego typu grupy, mają na celu przede wszystkim osiągnięcie efektu w postaci wydźwięku propagandowego podejmowanych aktywności. Zidentyfikowano 184 incydenty, w tym 89 ataków DoS/DDoS oraz 3 zdarzenia odnoszące się do podmiotów związanych z procesem wyborczym.

6 Kategoria SKANOWANIE obejmuje zdarzenia wskazujące na możliwość przygotowania ofensywnych działań mających na celu przełamanie zabezpieczeń lub naruszenie dostępności usług. Pośród tej kategorii odnotowanych zostało 57 incydentów, w tym 1 dotyczący instytucji związanej z procesem wyborczym.

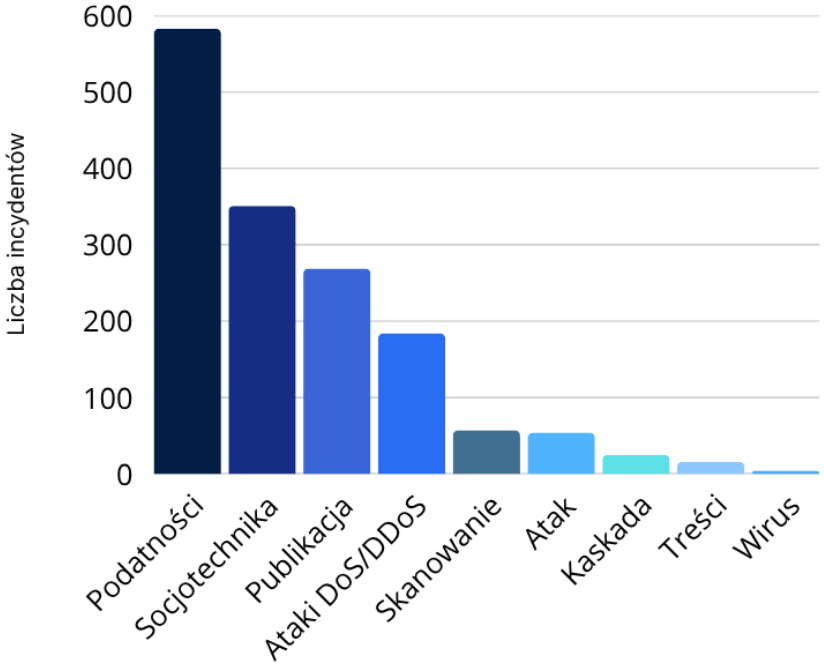
7 W ramach kategorii ATAK zarejestrowano zdarzenia obejmujące próby przełamania zabezpieczeń poprzez wykorzystywanie podatności, ataki typu bruteforce, kompromitacje kont i systemów oraz eksfiltrację danych z przejętych zasobów TI. Łącznie zidentyfikowano 54 incydenty tego rodzaju, z czego 1 dotyczył instytucji związanej z procesem wyborczym.

8 Kategoria KASKADA odnosi się do zgłoszeń i incydentów związanych ze zdarzeniami o charakterze terrorystycznym, na podstawie art. 27 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Są to wszelkie czynności dążące do minimalizacji zagrożenia o charakterze terrorystycznym podejmowane przez CSIRT GOV (ABW) w zakresie koordynacji obsługi incydentów. W sumie zarejestrowanych zostało 25 incydentów o takim charakterze.

9 Kategoria TREŚCI odnosi się przede wszystkim do incydentów naruszających szeroko pojmowane dobra publiczne, np. informacje wymierzone w wizerunek podmiotów państwowych czy zawierające treści dezinformacyjne - w tym przede wszystkim obejmujące wykorzystywanie wizerunku osób sprawujących kierownicze funkcje w państwie m.in. celem wyłudzenia środków finansowych od obywateli. Całkowita liczba zdarzeń tego typu wyniosła 16 incydentów, w tym 1 odnoszący się do instytucji związanej z procesem wyborczym.

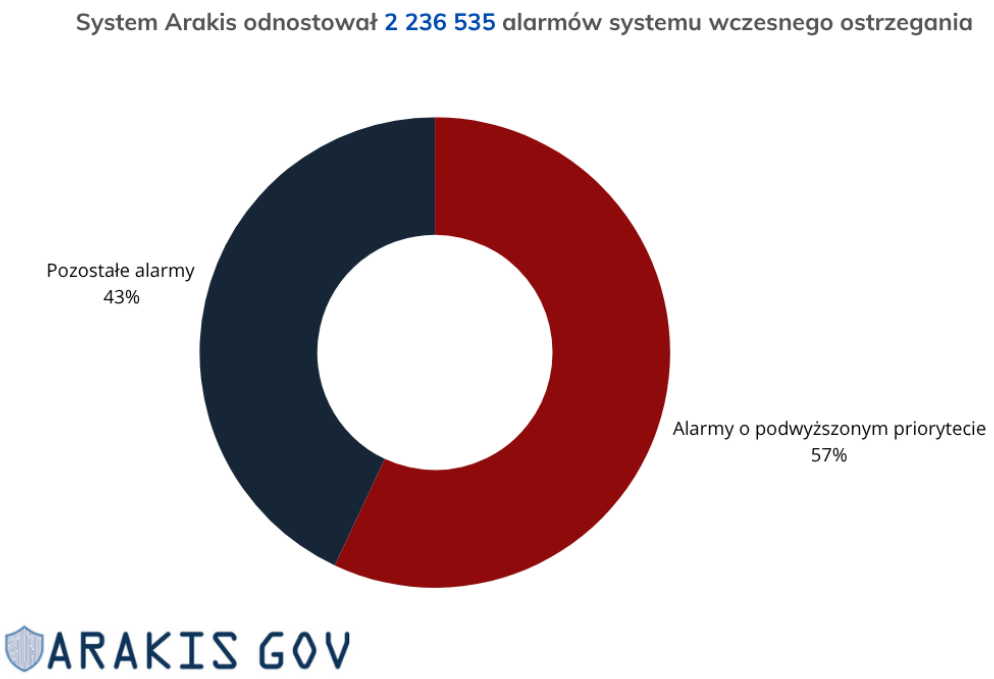
10 W ramach kategorii WIRUS Zespół CSIRT GOV (ABW) obsługiwał zgłoszenia dotyczące złośliwego oprogramowania zidentyfikowanego na stacjach roboczych, serwerach oraz urządzeniach sieciowych. We wskazanym okresie zarejestrowano 4 incydenty powiązane z powyższą kategorią.

Żadne z zarejestrowanych zgłoszeń i incydentów o kategoriach KASKADA oraz WIRUS nie dotyczyły instytucji związanych z procesem wyborczym. Pozostałe 8 incydentów dotyczących instytucji związanych z procesem wyborczym odnosi się do zdarzeń niewpisujących się w powyższe kategorie.



Rysunek 30: Incydenty podzielono - w zależności od rodzaju i charakteru zdarzenia - według kategorii

Ponadto odnotowano 2 236 535 alarmów systemu wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej z siecią Internet. Z identyfikowanych zagrożeń wykrytych przez system ARAKIS GOV około 57% stanowiło alarmy o podwyższonym priorytecie reakcji.



Rysunek 31: Zestawienie wyników z systemu ARAKIS GOV

Jednocześnie podczas trwania procesu wyborczego rozdystrybuowano 237 ostrzeżeń o zidentyfikowanych zagrożeniach teleinformatycznych, w tym 85 odnoszących się do złośliwego ruchu sieciowego oraz 27 dotyczących zidentyfikowanych podatności.

Monitorowanie przestrzeni informacyjnej i identyfikacja kampanii dezinformacyjnych:
W ramach prowadzonych czynności ABW potwierdziła, że nie uległ zmianie *modus operandi* rosyjskiej agresji informacyjnej, który - tak jak w przeszłości - stale dostosowywany był do trwającego w Polsce dyskursu społeczno-politycznego i obejmował promowanie tematów mających za zadanie zwiększenie efektu polaryzacji społecznej. Rosyjski aparat propagandowy oraz - powielający ich przekaz - reprezentanci środowisk prorosyjskich w Polsce eksploatowali tematy wywołujące kontrowersje czy drażliwe społecznie i budzące skrajne emocje. Wśród dominujących w przekazie propagandowym narracji należy wymienić zwłaszcza kwestie dotyczące społeczności ukraińskiej w RP, wojny na Ukrainie i problematyki migracji. Ponadto rozpowszechniali tezy mające podważać zaufanie do procesu wyborczego czy instytucji państwowych.

Jednocześnie ABW weryfikowała sygnały dotyczące prowadzenia niesygnowanej agitacji wyborczej na terytorium RP.

Przedstawiciele ABW uczestniczyli w organizowanych przez MC spotkaniach dotyczących treści dezinformacyjnych w kontekście wyborów prezydenckich w formule „War Room".

ABW przekaże do MC niejawne opracowanie stanowiące podsumowanie podejmowanych przez Agencję czynności na rzecz zabezpieczenia wyborów prezydenckich.

3.2 SŁUŻBA KONTRWYWIADU WOJSKOWEGO (SKW)

SKW w ramach programu „Parasol Wyborczy" prowadziła stały monitoring w zakresie cyberzagrożeń, w tym w przestrzeni informacyjnej, związany z identyfikacją zagrożeń dla procesu wyborczego, w szczególności w kontekście przypadków wykorzystania tematyki wojskowej w przekazie aparatu informacyjno-propagandowego przeciwnika, innych narracji propagandowych kierowanych do żołnierzy Sił Zbrojnych SZ (SZ) RP oraz aktywności środowisk antysystemowych.

Rysunek 32: Działania SKW w zapewnianiu bezpieczeństwa wyborów

W wyniku wskazanego monitoringu i analizy stwierdzono, że żołnierze nie znajdowali się w priorytetowym zainteresowaniu aparatu przeciwnika, niemniej wątki wojskowe (teza o rzekomo planowanym wysłaniu SZ RP na Ukrainę) pojawiały się wśród istotnych narracji w czasie wyborów prezydenckich.

W wyniku monitoringu SKW zidentyfikowała, zapoczątkowaną w okresie marzec/kwiecień 2025 r. aktywność siatki kilkuset nieautentycznych kont w serwisie społecznościowym X.

Informacje w tej sprawie zostały przesłane m.in. do MC, NASK i MSZ. Jednocześnie SKW pozostawała w gotowości w przypadku konieczności wsparcia innych instytucji w obsłudze poważnych incydentów w cyberprzestrzeni.

Ponadto przedstawiciele SKW regularnie uczestniczyli w organizowanych przez MC spotkaniach dotyczących treści dezinformacyjnych w kontekście wyborów prezydenckich w formule „War Room".

3.3 MINISTERSTWO SPRAW ZAGRANICZNYCH (MSZ)

MSZ koordynuje prace Zespołu ds. przeciwdziałania zagranicznym operacjom informacyjnym wymierzonym w proces wyborczy. Zespół, poza przedstawicielami MSZ, składa się z reprezentantów KPRM, MON, MSWiA, MC, NASK, DKWOC, ABW, AW, SWW, SKW. Zespół służy koordynacji i wymianie informacji dotyczących zewnętrznego aspektu ingerencji i manipulacji informacją. Zespół składa się z ekspertów i ma charakter apolityczny. Zadaniem Zespołu nie jest ocena narracji pojawiających się w polskiej infosferze, a sprawdzanie czy promowanie danych treści nie ma charakteru zagranicznej operacji informacyjnej i sztucznego wzmacniania treści np. poprzez przygotowane wcześniej tzw. farmy botów, opłacane konta w mediach społecznościowych czy innego rodzaju wpływy zagraniczne.

Zespół spotykał się od marca 2025 r. co do zasady raz w tygodniu, w formule niejawnej. Sprawozdania z każdego spotkania były przekazywane kanałem niejawnym do instytucji zaangażowanych w pracę Zespołu. Rola koordynacyjna MSZ wynika z decyzji Prezesa Rady Minstrów (RM). Po wyborach Zespół został przekształcony w Międzyresortowy Zespół ds. Przeciwdziałania Zagranicznej Ingerencji i Manipulacji w Środowisku Informacyjnym na podstawie zarządzenia Prezesa RM.

Rada Odporności

Przy Ministrze Spraw Zagranicznych powołano Radę Konsultacyjną do spraw Odporności na Dezinformację Międzynarodową. Rada Odporności to nowa platforma współpracy administracji, uczelni, samorządów, organizacji społecznych i biznesu. Jej celem jest budowanie odporności społeczeństwa na dezinformację międzynarodową oraz formułowanie opinii i rekomendacji działań w obszarze przeciwdziałania temu zagrożeniu. W skład Rady Odporności weszło 22 ekspertów z rekomendacji organizacji pozarządowych i uczelni, cieszących się uznaniem ponad 100 podmiotów zaangażowanych w walkę z dezinformacją w Polsce. Pracami kieruje pełnomocnik Ministra Spraw Zagranicznych do spraw przeciwdziałania dezinformacji międzynarodowej. Rada Odporności została powołana zarządzeniem Ministra Spraw Zagranicznych z dnia 11 września 2024 r.

28 kwietnia Rada opublikowała apel do społeczeństwa, mediów i polityków w związku z wyborami Prezydenta RP. W apelu Rada wskazała na narastające zagrożenie ze strony zewnętrznych kampanii dezinformacyjnych, które mają na celu zakłócanie procesów wyborczych i polaryzację społeczeństwa. W apelu zalecono korzystanie wyłącznie ze sprawdzonych źródeł informacji, powstrzymywanie się od rozpowszechniania niezweryfikowanych treści oraz o odpowiedzialność w debacie publicznej. Rada podkreśla rolę profesjonalnych mediów i organizacji fact-checkingowych w ochronie jakości debaty publicznej. Całość apelu dostępna jest na stronie MSZ.

Współpraca

MSZ współpracuje między innymi z **Europejską Służbą Działań Zewnętrznych**, która koordynuje działanie tzw. **Rapid Alert System – platformy pozwalającej na wymianę informacji o incydentach zagranicznej ingerencji i manipulacji informacją (FIMI - Foreign Information Manipulation and Interference, Zagraniczne manipulacje informacjami i ingerencje w informacje).** Informacje te oraz raporty dot. zewnętrznej ingerencji i manipulacji informacyjnych wymierzonych w proces wyborczy przekazywane są do NASK.

Raporty dotyczące FIMI dostarczane są też MSZ przez placówki dyplomatyczne na całym świecie oraz organizacje pozarządowe. Informacje z tych źródeł umieszczane są w cotygodniowych biuletynach dot. dezinformacji przygotowywanych przez MSZ i wysyłanych partnerom w administracji rządowej.

4 TECHNOLOGIE ANONIMIZACJI W INGERENCJI WYBORCZEJ – ANALIZA WYZWAŃ DLA BEZPIECZEŃSTWA PROCESÓW DEMOKRATYCZNYCH

W kontekście wyborów prezydenckich w Polsce w 2025 r., realizowanych w ramach programu „Parasol Wyborczy". Analizy i badania nad metodami anonimizacji cyberprzestępców nabierają szczególnego znaczenia. Doświadczenie ostatnich cyklów wyborczych, w tym z dwóch tur wyborów prezydenckich, dostarczają cennych wniosków na temat skuteczności współczesnych metod przeciwdziałania ingerencjom cyfrowym. Jednocześnie ujawniają one istotne wyzwania związane z identyfikacją sprawców takich ataków, co jest bolączką organów ścigania wszystkich państw świata.

Jednym z kluczowych problemów pozostaje skuteczna anonimizacja stosowana przez cyberprzestępców. Choć stanowi ona zaawansowaną technicznie formę ochrony prywatności, w praktyce znacząco utrudnia, a często wręcz uniemożliwia szybką reakcję instytucji odpowiedzialnych za zapewnienie cyberbezpieczeństwa. W okresie wyborczym, kiedy natężenie incydentów cyfrowych rośnie, opóźnienia w identyfikacji źródeł zagrożeń mogą mieć poważne konsekwencje dla integralności procesu demokratycznego, zaś same podjęcie reakcji może powodować próby budowania narracji o przeciw demokratycznych lub nawet autorytarnych zachowaniach administracji publicznej.

Dodatkowo, obecne uwarunkowania prawne – zarówno krajowe, jak i międzynarodowe – nie nadążają za tempem rozwoju technologii wykorzystywanych przez cyberprzestępców. Brak spójnych i skutecznych mechanizmów współpracy transgranicznej oraz ograniczenia w zakresie wymiany danych operacyjnych sprawiają, że efektywna reakcja na incydenty oraz namierzanie sprawców pozostają nie tylko poważnym wyzwaniem, a niemożliwym przedsięwzięciem.

Architektura współczesnych zagrożeń - systematyczne niszczenie śladów cyfrowych

Zaraz po zakończeniu zaplanowanych działań związanych z ingerencją w procesy wyborcze (również pozostałe procesy przestępcze), adwersarze systematycznie przechodzą do etapu zacierania śladów swojej obecności cyfrowej. Analiza przypadków ataków cyfrowych wykazuje, że cyberprzestępcy wykorzystujący serwery VPS (Virtual Private Server) do przeprowadzania ataków na obraną infrastrukturę stosują zaawansowane techniki niszczenia dowodów. Proces ten obejmuje nadpisanie kluczowych katalogów /home, /var, a następnie głównego katalogu /, co prowadzi do nieodwracalnego usunięcia danych dotyczących prowadzonej operacji.

Współczesne operacje cyberprzestępcze w tym ingerencji wyborczej wykorzystują rozproszoną infrastrukturę VPS do koordynowania wieloetapowych ataków. Serwery VPS z współdzieloną przestrzenią dyskową z puli pamięci RAID (ang. Redundant Array of Independent Disks – nadmiarowa macierz niezależnych dysków) na głównym serwerze umożliwiają płynne przejście między fizycznymi dyskami, co znacząco utrudnia zachowanie

zawartości i przeprowadzenie skutecznej analizy powłamaniowej (ang. forensic). Z uwagi na koszty operacyjne, większość dostawców VPS nie oferuje ciągłego tworzenia kopii zapasowych, co dodatkowo komplikuje proces śledczy.

Ponadto, celem minimalizacji ryzyka wykrycia podczas operacji, adwersarze łączą się z serwerami VPS za pomocą szyfrowanego ruchu, wykorzystując tunele SSH lub bezpośrednio sieci anonimizujące, takie jak Tor i VPN. Zakłada się, że prawdopodobieństwo de-anonimizacji prawidłowo skonfigurowanych połączeń Tor jest znikome (choć nie niemożliwe), co czyni tę technologię niezwykle skutecznym narzędziem dla cyberprzestępców. Dodatkowo geolokalizacja serwerów wykorzystywanych do ingerencji wyborczej nie dostarcza precyzyjnych informacji o lokalizacji sprawców. Serwer fizycznie może znajdować się we np. Francji, ale jego adres IP może być przypisany do puli adresów np. z Rumunii, co znacząco komplikuje proces identyfikacji stacji roboczej/serwera użytkownika. Cyberprzestępcy celowo wybierają dostawców, którzy nie informują o fizycznej lokalizacji serwerów, a analizując adresy wyjściowe VPS wykorzystywanych w złośliwych kampaniach, można zauważyć, że zmieniają się one między różnymi krajami i dostawcami. Dlatego też, numery ASN (Autonomous System Number) stają się kluczowe w śledztwie, ponieważ są przydzielane do konkretnych regionów, jednak cyberprzestępcy coraz częściej wykorzystują techniki routingu przez wiele różnych ASN.

Należy zaznaczyć, że dodatkową warstwą anonimizacji adwersarzy są kryptowaluty. Wykorzystanie walut wirtualnych, a szczególnie Monero i Bitcoin, w sposób anonimowy czyni śledzenie sprawców ingerencji wyborczej niezwykle trudnym. Monero oferuje zaawansowane techniki kryptograficzne, takie jak Stealth Addresses, Ring Signatures i RingCT, które zapewniają znacznie wyższy poziom prywatności niż Bitcoin. powyższe przy współczesnym krajobrazie zagrożeń wyborczych charakteryzującym się rozwojem modelu "Hacking as a Service" (HaaS), gdzie specjalistyczne usługi ingerencji wyborczej są oferowane na dark webie za stosunkowo niskie opłaty. Za 100 dolarów można wynająć botnet zdolny do rozpowszechniania tysięcy postów dezinformacyjnych, podczas gdy za 500 dolarów dostępne są zaawansowane narzędzia manipulacji opinii publicznej. Te usługi są regularnie opłacone kryptowalutami, co dodatkowo utrudnia identyfikację zleceniodawców oraz umożliwia przeprowadzanie operacji bez głębokiej wiedzy technicznej.

5 WNIOSKI

Ocena programu „Parasol Wyborczy"

Program „Parasol Wyborczy" stanowił pierwszą w historii Polski kompleksową operację ochrony procesu wyborczego przed zagrożeniami cyfrowymi i dezinformacyjnymi, realizowaną w ramach skoordynowanego działania instytucji państwowych.

W zakresie cyberbezpieczeństwa Program „Parasol Wyborczy" okazał się skutecznym narzędziem, gdyż nie odnotowano żadnych cyberataków, które wpłynęłyby na proces wyborczy. Jest to wynik ogromu pracy włożonej przez szereg instytucji, aby zapewnić odporność systemów teleinformatycznych związanych z procesem wyborczym oraz podnieść kompetencje kadr w organach wyborczych oraz innych podmiotach odpowiedzialnych za przeprowadzenie wyborów. Ponadto, współpraca instytucji odpowiedzialnych za cyberbezpieczeństwo państwa w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa umożliwiła skuteczne reagowanie na zagrożenia w czasie rzeczywistym.

Nieadekwatność przepisów prawnych do zagrożeń cyfrowych

Analiza przeprowadzonych działań ujawnia nieadekwatność obecnych rozwiązań legislacyjnych do charakterystyki współczesnych zagrożeń w cyberprzestrzeni. Obowiązujące przepisy prawne mają niedoskonały charakter i umożliwiają jedynie reakcyjne przeciwdziałanie dezinformacji, podczas gdy natura zagrożeń cyfrowych wymaga działań prewencyjnych o znacznie większej dynamice. Podjęte działania wyczerpywały wachlarz narzędzi dostępnych w obecnym systemie prawnym, jednak okazały się niewystarczające wobec skali wyzwań.

Należy ponadto zaznaczyć, że tematyka dezinformacji wykracza poza ramy prawne Krajowego Systemu Cyberbezpieczeństwa ustanowionego ustawą o Krajowym Systemie Cyberbezpieczeństwa. Ustawa ta obejmuje jedynie technicznie zdefiniowane cyberbezpieczeństwo[8], a nie obszaru bezpieczeństwa przestrzeni informacyjnej, czy węziej dezinformacji. Również procedowana nowelizacja ustawy o KSC[9] pozostaje przy technicznym rozumieniu cyberbezpieczeństwa[10]. Instytucje KSC są właściwe do podejmowania działań w zakresie dezinformacji jedynie w przypadku, gdy jest ona bezpośrednio powiązana incydentami cyberbezpieczeństwa. Obszar dezinformacji i właściwość poszczególnych instytucji pozostaje w dużej mierze nieuregulowany, poszczególne instytucje podejmują działania w tym zakresie na podstawie swoich kompetencji ogólnych.

Dodatkowo należy zaznaczyć, że działania stanowiące agitację wyborczą (zdefiniowaną w art. 105 § 1 Kodeksu wyborczego) mogą podejmować wyłącznie komitety wyborcze uczestniczące w wyborach oraz wyborcy. Prowadzenie agitacji wyborczej przez inne podmioty stanowi

[8] Art. 2 pkt 4 definiuje cyberbezpieczeństwo jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".
[9] Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32).
[10] Nowelizacja odwołuje się do definicji cyberbezpiczeństwa określonego w unijnym akcie o cyberbezpieczeństwie, tj: cyberbezpieczeństwo oznacza „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami".

naruszenie przepisów Kodeksu wyborczego. Zmiany przepisów Kodeksu wyborczego dokonane ustawą z dnia 11 stycznia 2018 r. o zmianie niektórych ustaw w celu zwiększenia udziału obywateli w procesie wybierania, funkcjonowania i kontrolowania niektórych organów publicznych (Dz. U. poz. 130 z późn. zm.), polegające na nadaniu art. 106 § 1 Kodeksu wyborczego nowego brzmienia (rozszerzenie kategorii podmiotów uprawnionych do prowadzenia agitacji wyborczej o wyborców) i uchyleniu art. 499 (depenalizacja prowadzenia agitacji wyborczej bez pisemnej zgody pełnomocnika wyborczego) nie zalegalizowały prowadzenia agitacji wyborczej przez podmioty inne, niż komitety wyborcze i wyborcy. W wyniku tych zmian działanie takie nie jest zagrożone sankcją, lecz pozostaje niezgodne z prawem.

Ograniczenia jurysdykcyjne w cyberprzestrzeni

Specyfika funkcjonowania sieci komputerowych, charakteryzująca się brakiem fizycznych granic oraz możliwością ukrywania rzeczywistej lokalizacji poprzez sieci VPN i serwery VPS, sprawia, że egzekwowanie prawa krajowego wobec podmiotów działających w cyberprzestrzeni jest praktycznie niemożliwe. Charakterystyka działalności podmiotów zorganizowanych, w tym państwowych, odpowiedzialnych za szerzenie treści szkodliwych i polaryzacyjnych, w połączeniu z ich zaawansowanymi zdolnościami technicznymi oraz dogłębną znajomością lokalnych systemów prawnych, sprawia, że pełne i skuteczne przeciwdziałanie tego typu aktywności w przestrzeni informacyjnej pozostaje wyzwaniem przekraczającym możliwości jakiegokolwiek podmiotu publicznego działającego w ramach prawa krajowego.

Ograniczenia automatyzacji w wykrywaniu dezinformacji

Obecny stan technologii sztucznej inteligencji nie pozwala na pełną automatyzację oceny treści pod kątem dezinformacji, co stanowi istotne ograniczenie w procesie masowego monitoringu przestrzeni informacyjnej. Treści dezinformacyjne często mają znaczenie wyłącznie kontekstowe i wydźwięk lokalny, oparte są na wzorcach kulturowych, dwuznaczności, sarkazmie i ironii, co czyni je praktycznie nierozpoznawalnymi dla systemów automatycznych opartych o AI.

Profesjonalizacja operacji APT

Charakterystyka grup APT wykazała ich wysoką profesjonalizację i dogłębną znajomość lokalnych systemów prawnych. Skuteczne przeciwdziałanie tego typu aktywności wymaga, aby taka grupa popełniła błędy na kilku etapach jednocześnie, co jest mało prawdopodobne w przypadku dobrze zorganizowanych operacji państwowych.

Polaryzacja jako czynnik ograniczający

Działania mające na celu przeciwdziałanie dezinformacji w wysokospolaryzowanym środowisku społecznym napotykają na znaczny opór i zarzuty stosowania narzędzi cenzorskich, co prowadzi do dalszego wzrostu antagonizmów społecznych. Inicjatywy legislacyjne mające na celu dostosowanie prawa do wyzwań związanych z funkcjonowaniem w cyberprzestrzeni są systematycznie podważane poprzez oskarżenia o naruszanie wolności słowa oraz podstawowych wartości demokratycznych, co skutkuje impasem legislacyjnym i uniemożliwia skuteczne przeciwdziałanie zagrożeniom.

Budowanie metanarracji antydemokratycznych

Analiza rozpowszechnianych treści dezinformacyjnych wykazała, że służyły one przede wszystkim budowaniu metanarracji podważającej fundamenty procesów demokratycznych. Narracje obejmujące oskarżenia o fałszerstwa wyborcze, manipulacje wynikami, ingerencje zewnętrzne oraz teorie spiskowe dotyczące zamachów i anulowania wyborów miały na celu wzbudzenie poczucia zagrożenia, chaosu i niepewności.

Efektywność koordynacji międzyinstytucjonalnej

Istotną wartość w zabezpieczenie wyborów w cyberprzestrzeni wniosła współpraca w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa, będącym formatem spotkań koordynacyjnych instytucji odpowiedzialnych za bezpieczeństwo teleinformatyczne na poziomie krajowym. Program potwierdził wartość skoordynowanego podejścia międzyinstytucjonalnego, gdzie współpraca m.in. między MC, NASK, COI, ABW, AW, SKW, , CBZC i MSZ umożliwiła skuteczne reagowanie na zagrożenia w czasie rzeczywistym. Mechanizmy te stanowią model dla przyszłych inicjatyw bezpieczeństwa narodowego. Jednocześnie wciąż są odczuwalne pewne ograniczenia w zakresie koordynacji, dlatego warte rozważenia jest powołanie w przyszłości centralnej instytucji państwowej odpowiedzialnej za cyberbezpieczeństwo na poziomie krajowym.

W projektowanej zmianie ustawy o KSC sformalizowane zostanie funkcjonowanie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa. Formuła spotkań koordynacyjnych w formacie ww. gremium, w których biorą udział przedstawiciele kluczowych dla cyberbezpieczeństwa kraju instytucji, stanowi istotną wartość dodaną dla KSC, dzięki szybkiej wymianie informacji i sprawnemu reagowaniu na pojawiające się incydenty cyberbezpieczeństwa.

W kolejnym kroku nastąpi rozszerzenie charakteru Połączonego Centrum Operacyjnego Cyberbezpieczeństwa przez ustanowienie pod tą nazwą komórki organizacyjnej urzędu obsługującego ministra właściwego do spraw informatyzacji, która będzie organizacyjnie i merytorycznie obsługiwać Pełnomocnika i spotkania ww. gremium, koordynować z ramienia Pełnomocnika działania instytucji zapewniających cyberbezpieczeństwo na poziomie krajowym oraz realizować część zadań ministra właściwego do spraw informatyzacji przewidzianych w ustawie o KSC.

Implementacja prawa Unii Europejskiej

Kluczową szansą na poprawę skuteczności przeciwdziałania dezinformacji jest zapewnienie należytego stosowania DSA, który wprowadza wymogi i obowiązki wobec platform mediów społecznościowych. MC pracuje nad przepisami krajowymi w tym zakresie, co umożliwi szybsze i skuteczniejsze reagowanie na zagrożenia informacyjne.

Budowa narodowej odporności cyfrowej i strategii przeciwdziałania dezinformacji

Systematyczne podnoszenie świadomości społeczeństwa na temat zagrożeń informacyjnych oraz rozwijanie kompetencji cyfrowych stanowi kluczowy element długoterminowej strategii ochrony procesu demokratycznego. Edukacja obywateli i budowanie odporności na manipulację są niezbędne do ochrony przestrzeni informacyjnej przed wpływami zewnętrznymi.

Koniecznym jest wypracowanie systemowych mechanizmów przeciwdziałania dezinformacji. Rekomendacje dotyczące funkcjonowania takiego systemu z uwzględnieniem doświadczeń oraz znajomości właściwości obecnie działających podmiotów zaangażowanych w proces walki z dezinformacją został wyznaczony jako jeden z celów działań dla Międzyresortowego Zespołu ds. Przeciwdziałania Zagranicznej Ingerencji i Manipulacji w Środowisku Informacyjnym powołanego podstawie zarządzenia Prezesa RM.

ZAKOŃCZENIE

Program „Parasol Wyborczy" stanowił pierwszą w historii Polski kompleksową operację ochrony procesu wyborczego przed zagrożeniami cyfrowymi i dezinformacyjnymi, realizowaną w ramach skoordynowanego działania instytucji państwowych. Implementacja programu w kontekście wyborów prezydenckich 2025 r. potwierdziła zarówno skuteczność przyjętego podejścia międzyinstytucjonalnego, jak i ujawniła fundamentalne ograniczenia wynikające z anachronicznego systemu prawnego oraz specyfiki funkcjonowania cyberprzestrzeni. Pozytywnie należy ocenić współpracę międzyinstytucjonalną realizowana w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa oraz koordynacja działań między MC, ABW, AW, SKW, , CBZC, MSZ, COI i NASK w ramach Parasola Wyborczego, co umożliwiło skuteczne reagowanie na zagrożenia w czasie rzeczywistym.

Wybory prezydenckie 2025 r. odbyły się bezpiecznie przy rekordowej frekwencji wynoszącej 71,63%, co stanowiło najwyższy wynik od 1990 r. i świadczyło o wysokim poziomie zaufania społecznego do procesu wyborczego. NASK uczestniczący w programie skutecznie zidentyfikował i zneutralizował ponad 16 000 nieautentycznych kont działających w sposób skoordynowany, co stanowiło 17% wszystkich konwersacji dotyczących wyborów prezydenckich na głównych platformach społecznościowych. OAD NASK obsłużył około 27,5 tysięcy zgłoszeń potencjalnych incydentów, z czego 23,7 tysięcy zostało uznanych za zasadne i przekazane do dalszej obsługi.

Jednakże analiza przeprowadzonych w ramach programu działań ujawniła nieadekwatność obecnych rozwiązań legislacyjnych do charakterystyki współczesnych zagrożeń w cyberprzestrzeni. Obowiązujące przepisy prawne mają niedoskonały charakter i umożliwiają jedynie reakcyjne przeciwdziałanie dezinformacji, podczas gdy natura zagrożeń cyfrowych wymaga działań prewencyjnych o znacznie większej dynamice. Specyfika funkcjonowania sieci komputerowych, charakteryzująca się brakiem fizycznych granic oraz możliwością ukrywania rzeczywistej lokalizacji poprzez m.in. sieci VPN i serwery VPS, sprawia, że egzekwowanie prawa krajowego wobec podmiotów działających w cyberprzestrzeni jest praktycznie niemożliwe.

Charakterystyka działalności podmiotów zorganizowanych, w tym państwowych (grupy APT), odpowiedzialnych za szerzenie treści szkodliwych i polaryzacyjnych, w połączeniu z ich zaawansowanymi zdolnościami technicznymi oraz dogłębną znajomością lokalnych systemów prawnych, sprawia, że pełne i skuteczne przeciwdziałanie tego typu aktywności w przestrzeni informacyjnej pozostaje wyzwaniem przekraczającym możliwości jakiegokolwiek podmiotu publicznego działającego w ramach zarówno prawa krajowego, jak i międzynarodowego.

Obecny stan technologii sztucznej inteligencji nie pozwala na pełną automatyzację oceny treści pod kątem dezinformacji, co stanowi istotne ograniczenie w procesie masowego monitoringu przestrzeni informacyjnej. Treści dezinformacyjne często mają znaczenie wyłącznie kontekstowe i wydźwięk lokalny, oparte są na wzorcach kulturowych, dwuznaczności, sarkazmie i ironii, co czyni je praktycznie nierozpoznawalnymi dla systemów automatycznych.

Działania mające na celu przeciwdziałanie dezinformacji w wysokospolaryzowanym środowisku społecznym napotykają na znaczny opór i zarzuty stosowania narzędzi cenzorskich, co prowadzi do dalszego wzrostu antagonizmów społecznych. Próby modernizacji prawa w zakresie cyberprzestrzeni są podważane poprzez oskarżenia o naruszanie wolności słowa i wartości demokratycznych, co tworzy błędne koło uniemożliwiające skuteczne przeciwdziałanie zagrożeniom.

Kluczową szansą na poprawę skuteczności przeciwdziałania dezinformacji jest zapewnienie należytego stosowania DSA, który dostarcza narzędzi wywierania nacisku i egzekucji wobec platform mediów społecznościowych. MC pracuje nad przepisami krajowymi w tym zakresie, co ma umożliwić szybsze i skuteczniejsze reagowanie na zagrożenia informacyjne. Przyszłe programy ochrony wyborów powinny opierać się na wzmocnionej współpracy międzynarodowej, szczególnie w ramach NATO i UE, gdzie można wykorzystać wspólne mechanizmy wymiany informacji o zagrożeniach. Koniecznym jest również wypracowanie rekomendacji systemowych mechanizmów przeciwdziałania dezinformacji

Systematyczne podnoszenie świadomości społeczeństwa na temat zagrożeń informacyjnych oraz rozwijanie kompetencji cyfrowych stanowi kluczowy element długoterminowej strategii ochrony procesu demokratycznego. Edukacja obywateli i budowanie odporności na manipulację są niezbędne do ochrony przestrzeni informacyjnej przed wpływami zewnętrznymi.

Podsumowując, program „Parasol Wyborczy" udowodnił, że skoordynowane działania państwa polskiego mogą skutecznie chronić proces wyborczy przed zagrożeniami hybrydowymi, mimo fundamentalnych ograniczeń systemowych. Spokojny przebieg wyborów prezydenckich 2025 r. przy najwyższej frekwencji od 1990 r. oraz relatywnie niskiej liczbie incydentów potwierdza skuteczność zastosowanych rozwiązań.

Koniecznym jest jednak wzmocnienie systemowych mechanizmów przeciwdziałania cyberzagrożeniom i dezinformacji w tym wypracowanie standardów komunikacji identyfikowanych zagrożeń. Obecne działania, które wyczerpywały wachlarz narzędzi dostępnych w obecnym środowisku legislacyjnym, demonstrują możliwości międzyinstytucjonalnej koordynacji w obliczu złożonych wyzwań bezpieczeństwa.

Bez zmiany ram legislacyjnych i opracowania nowego modelu prawnego adekwatnego do dynamiki zagrożeń cyfrowych, państwo polskie nie będzie optymalnie przygotowane na działania wobec coraz bardziej wyrafinowanych operacji wpływu prowadzonych przez podmioty zewnętrzne. Konieczne jest stworzenie krajowych ram przeciwdziałania dezinformacji.

Program „Parasol Wyborczy" stanowi solidną podstawę do dalszego rozwoju polskich kompetencji w zakresie ochrony procesów wyborczych przed zagrożeniami hybrydowymi i może służyć jako model dla innych krajów demokratycznych.

Doświadczenia z realizacji programu „Parasol Wyborczy" potwierdzają, że ochrona współczesnych procesów demokratycznych wymaga nie tylko zaawansowanych narzędzi technicznych i sprawnej koordynacji międzyinstytucjonalnej, ale przede wszystkim społecznego konsensusu co do konieczności modernizacji prawa oraz budowania narodowej odporności cyfrowej opartej na edukacji obywateli i rozwijaniu kompetencji cyfrowych. **Tylko**

kompleksowe podejście łączące aspekty techniczne, prawne, organizacyjne i społeczne może zapewnić skuteczną ochronę polskiej demokracji w erze cyfrowej transformacji.

Spis Rysunków:

Rysunek 1: Instytucje realizujące program ‘Parasol Wyborczy’ 6
Rysunek 2: Obszary działań w ramach parasola wyborczego 7
Rysunek 3: Ministerstwo Cyfryzacji oraz jednostki podległe i nadzorowane 11
Rysunek 4: Kampania informacyjna "Z mObywatelem wybory są łatwiejsze" 12
Rysunek 5: Kampania informacyjna TROLE 13
Rysunek 6: Kampania informacyjna TROLE 13
Rysunek 7: Kampania edukacyjno- informacyjna „Przepis na dezinformację” 14
Rysunek 8: Kampania edukacyjno- informacyjna „Przepis na dezinformację” 14
Rysunek 9: Usługa Wybory w aplikacji mObywatel 2.0 15
Rysunek 10: Centralny Rejestr Wyborców w mObywatel 2.0 15
Rysunek 11: Funkcjonalności w usłudze „Wybory” w aplikacji mObywatel 2.0 16
Rysunek 12: Aplikacja mObywatel 2.0 do pobrania 16
Rysunek 13: Wiadomość PUSH - weryfikacja miejsca głosowania 16
Rysunek 14: Przykładowe treści złośliwych wiadomości SMS 19
Rysunek 15: Przykład nadpisu wiadomości 19
Rysunek 16: Przykładowa treść złośliwych wiadomości SMS z poprzedniej kampanii wyborczej 19
Rysunek 17: Zestawienie CSIRT NASK dot. zarejestrowanej liczby zgłoszeń powiązanych z II turą wyborów 21
Rysunek 18: Prawdopodobne podszycie pod materiał wyborczy 21
Rysunek 19: Zadania Ośrodka Analizy Dezinformacji 23
Rysunek 20: Kadr ze spotu kampanii edukacyjnej „Nie pozwól sobie odebrać głosu” 24
Rysunek 21: Osłona informacyjna kampanii wyborczej 2025 r. 25
Rysunek 22: Dane dot. monitoringu przestrzeni informacyjnej i obsługi zgłoszeń 26
Rysunek 23: II tura wyborów prezydenckich 27
Rysunek 24: Bezpiecznewybory.pl 33
Rysunek 25: Strona internetowa zachęcająca do korzystania z nieautoryzowanej aplikacji 35
Rysunek 26: Wpis na portalu X zachęcający do korzystania z nieautoryzowanej aplikacji 35
Rysunek 27: Zadania NASK w zakresie bezpieczeństwa wyborów 36
Rysunek 28: Liczba uczestników 37
Rysunek 29: Uczestnicy spotkań 37
Rysunek 30: Incydenty podzielono - w zależności od rodzaju i charakteru zdarzenia - według kategorii 41
Rysunek 31: Zestawienie wyników z systemu ARAKIS GOV 42
Rysunek 32: Działania SKW w zapewnianiu bezpieczeństwa wyborów 43

Spis tabel:

Tabela 1: Liczba zarejestrowanych incydentów w CSIRT-ach poziomu krajowego w 2024 r. .. 9