DEZINFORMACJA I PROPAGANDA W SEKTORZE BANKOWYM

SYGN. WIB PAB 7/2022

Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

PROGRAM ANALITYCZNO BADAWCZY

Warszawa, maj 2022

O Raporcie

Raport **Dezinformacja i propaganda w sektorze bankowym** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Autorzy:

Raport przygotowany przez zespół w składzie:

dr hab. inż. Piotr Dela – nadzór nad raportem
– jest absolwentem Wydziału Cybernetyki Wojskowej Akademii Technicznej, studiów podyplomowych w Akademii Obrony Narodowej i studiów podyplomowych w Instytucie Polityki Światowej w Waszyngtonie. Od początku pracy zawodowej związany z instytucjami centralnymi MON i szkolnictwem wojskowym. Nauczyciel akademicki Akademii Obrony Narodowej w Warszawie (Akademii Sztuki Wojennej) i Akademii Kaliskiej im. Prezydenta Stanisława Wojciechowskiego. Główny specjalista w Morskim Centrum Cyberbezpieczeństwa w Gdyni.
Autor ponad 100 artykułów, referatów, podręczników, opracowań naukowych i monografii. Obszar zainteresowań naukowych obejmuje: systemy wspomagania decyzji, systemy i sieci teleinformatyczne, bezpieczeństwo informacyjne, bezpieczeństwo i militaryzacja cyberprzestrzeni.

dr inż. Robert Janczewski
– jest absolwentem Politechniki Warszawskiej, Wydziału Elektroniki i Technik Informacyjnych, Kierunku Elektronika i Telekomunikacja. Jest doktorem nauk o obronności. Nauczyciel akademicki związany z kilkoma uczelniami, m.in. AMW Gdynia, ASzWoj Warszawa, UWM Olsztyn czy WSPol Szczytno. Adiunkt w Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie. Główny specjalista w Morskim Centrum Cyberbezpieczeństwa w Gdyni.
Autor i współautor artykułów, referatów, opracowań naukowych, rozdziałów do monografii i monografii z zakresu cyberbezpieczeństwa i procesów informacyjnych. Członek rad naukowych oraz komitetów organizacyjnych konferencji tematycznych. Swój wysiłek badawczy skupia na zagadnieniach związanych z cyberprzestrzenią, cyberbezpieczeństwem oraz procesami informacyjnymi. Zainteresowania naukowe koncentruje również na procesach informacyjnych w środowisku cybernetycznym, a także cyberrozpoznaniu.

dr inż. Jakub Syta
– od ponad 20 lat promuje ideę, że zarządzanie cyberbezpieczeństwem może być proste. W tym czasie współtworzył szereg zespołów zajmujących się świadczeniem usług w zakresie bezpieczeństwa systemów informacyjnych, zrealizował projekty dla dziesiątek organizacji, współtworzył rozwiązania wykorzystywane do świadczenia zaawansowanych usług z zakresu cyberbezpieczeństwa.
Jest zastępcą dyrektora Morskiego Centrum Cyberbezpieczeństwa – think tank'u stworzonego przy Akademii Marynarki Wojennej w Gdyni oraz wykładowcą akademickim. Kierownik studiów Executive MBA „Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi" na AMW, redaktor naczelny czasopisma naukowego „Cybersecurity and Cybercrime". Równolegle z pracą naukową rozwija ofertę profesjonalnych usług cyberbezpieczeństwa w największej firmie telekomunikacyjnej w Polsce.
Posiada wiele certyfikatów zawodowych, m.in. CISM, CISSP i CISA.

PROGRAM ANALITYCZNO BADAWCZY

O Programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 roku jako odpowiedź na potrzeby sektora bankowego w zakresie analizy zjawisk, tworzenia opracowań i porządkowania wiedzy w obszarach cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania ich wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz kreowania wartości dla klientów bankowości. PAB WIB kładzie duży nacisk na rozwój współpracy ze środowiskami akademickimi i eksperckimi, poszukując synergii w zakresie zainteresowań badawczych autorów oraz potrzeb rozwojowych sektora bankowego.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- **Nowe technologie i cyberbezpieczeństwo**
- **Zdolność banków do finansowania gospodarki**
- **Bankowość spółdzielcza**
- **Rynek nieruchomości**
- **Zielony ład i finansowanie energetyki odnawialnej**
- **Finansowanie projektów innowacyjnych**

Więcej na temat działalności programu na stronie www.pab.wib.org.pl

Kontakt:

dr Andrzej Banasiak
Koordynator Programu
m: 696 405 104
e: abanasiak@wib.org.pl

Jacek Gieorgica
m: 603 626 254
e: jgieorgica@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Tomasz Pawlonka
m: 505 917 778
e: tpawlonka@wib.org.pl

PROGRAM ANALITYCZNO BADAWCZY

Spis treści

Wstęp

Rozwój cyberprzestrzeni przyczynił się z jednej strony do rozwoju usług bankowych, z drugiej zaś zwiększył ryzyko zagrożeń związanych z nowymi rodzajami przestępstw. Są one najczęściej związane z przestępczością pospolitą i są ukierunkowane na kradzież zasobów finansowych zarówno klientów systemów bankowych, jak i samych banków.

Informacyjny charakter cyberprzestrzeni umożliwia także rozwój zagrożeń znacznie bardziej poważniejszych, niosących ze sobą zagrożenia dla systemu finansowego i bankowego, zarówno w skali lokalnej, jak i globalnej. Zagrożeniami tymi są dezinformacja i propaganda. I chociaż w przestrzeni publicznej są one często zastępowane określeniem *fakenews*, to należy w sposób jednoznaczny zaznaczyć, że jest to zbyt duże uproszczenie. *Fakenews* jest tylko i wyłącznie fałszywą informacją, natomiast propaganda i dezinformacja są działaniami zaplanowanymi w czasie, pozwalającymi realizować przyjęte cele, najczęściej strategiczne. Bazują one na różnorodnych przekazach informacyjnych, w tym na *fakenewsach*, które stanowią najczęściej element zaplanowanej dezinformacji lub czarnej propagandy.

Cel główny:

Zidentyfikowanie i zamodelowanie współczesnego wymiaru dezinformacji i propagandy mogących mieć wpływ na sektor bankowy.

Cele szczegółowe:

1. Charakterystyka współczesnej dezinformacji.
2. Charakterystyka współczesnej propagandy.
3. Określenie celów realizowanych w kampaniach informacyjnych.
4. Opracowanie modelu zjawiska.
5. Wskazanie sposobów identyfikowania dezinformacji i propagandy.
6. Identyfikacja narzędzi wykorzystywanych w zwalczaniu dezinformacji i propagandy.

Problemy badawcze:

Wstępnie przewidziane cele badawcze będą zrealizowane w wyniku sformułowania problemów badawczych:

1. Jaki jest charakter współczesnej dezinformacji i propagandy szerzonej w cyberprzestrzeni?
2. Jakie cele mogą być realizowane w kampaniach informacyjnych?
3. Jak zamodelować zjawisko dezinformacji i propagandy w sektorze bankowym?
4. W jaki sposób identyfikować dezinformację i propagandę?
5. Jakie narzędzia mogą być wykorzystywane do zwalczania dezinformacji i propagandy w sektorze bankowym?

Metody badawcze:

Do metod badawczych wykorzystywanych w opracowaniu raportu należą:

- metoda badania dokumentów – szeroka analiza dostępnego piśmiennictwa oraz zasobów Internetu,
- metoda analizy indywidualnych przypadków, wykorzystywana głównie przy analizie kampanii informacyjnych,
- sondaż diagnostyczny,
- analiza, synteza, porównanie, uogólnienie.

Badania planuje się przeprowadzić w oparciu o następujące źródła danych:

- artykuły naukowe i literatura specjalistyczna dotycząca omawianego zagadnienia,
- badania zasobów sieci Internet w zakresie fałszywych wiadomości w sektorze bankowym,
- wiedza ekspercka – wynikająca między innymi z doświadczenia zespołu badawczego,
- nieskategoryzowane wywiady z ekspertami.

Charakterystyka współczesnej dezinformacji i propagandy

1.1. Istota i znaczenie informacji

Informacja od pradawnych czasów stanowiła zasób strategiczny. Decydowała o zwycięstwach i porażkach, kreowała postawy i poglądy, wyznaczała kierunki postępowania, obalała królów, wzniecała rewolucje, wpędzała w biedę lub powodowała bogactwo. Dlatego też stanowiła najcenniejszy zasób, który należało starannie chronić i jednocześnie nieustannie zdobywać. Nie inaczej jest współcześnie, w świecie, w którym dzięki technologiom teleinformatycznym, dostęp do informacji stał się niebywale prosty i szybki. Technologie te spowodowały równocześnie, nieznane dotąd, wyzwania związane z ochroną posiadanych zasobów informacyjnych. Informacja, jak nigdy wcześniej, stała się zasobem (wartością, towarem), o który toczone są walki w świecie rzeczywistym, ale też coraz częściej w świecie wirtualnym, cyberprzestrzeni. Dlatego też rozwijane są w coraz większym stopniu wyrafinowane systemy ochronno-obronne, które mają przeciwstawić się równie wyrafinowanym metodom ataku ukierunkowanym na przejęcie, modyfikację lub zniszczenie zasobów informacyjnych. To swoisty wyścig zbrojeń, wyścig pancerza z pociskiem, w którym przewagę zawsze będzie posiadał agresor jako ten, który posiada inicjatywę i przewagę strategiczną.

O wiele trudniejszym wyzwaniem, przed którym stoją współczesne podmioty bezpieczeństwa, jest wykorzystanie informacji jako broni, narzędzia służącego do ataku na konkretną grupę osób, społeczeństwo, naród. I chociaż informacja jako broń wykorzystywana była zawsze, to nigdy nie było to stosowane na taką skalę, jak współcześnie. Związane to jest oczywiście z rozwojem cyberprzestrzeni, w głównej mierze z portalami informacyjnymi i społecznościowymi, które są doskonałym środowiskiem rozprzestrzeniania informacji do ogromnej liczby osób w bardzo krótkim czasie, zbliżonym do czasu rzeczywistego. Zanim jednak przejdziemy do identyfikowania tych przekazów, wskazywania różnic pomiędzy *dezinformacją* i *propagandą, kłamstwem*, *fakenewsem*, *prawdą* i *wiedzą,* należy w pierwszej kolejności odnieść się do istoty informacji i jej znaczenia dla bezpieczeństwa podmiotu.

Informacja współcześnie definiowana jest różnorodnie, czasami wręcz sprzecznie lub zamiennie z takimi określeniami jak dane, wiedza czy też mądrość. Obserwowane jest to szczególnie w czasach pandemii, gdzie z jednej strony posługujemy się wiedzą naukową, popartą wieloletnimi badaniami naukowymi i doświadczeniem naukowców, z drugiej zaś wiedzą tak zwanych „ekspertów" podważających dorobek naukowy i rozprzestrzeniających różnorodne teorie spiskowe. Zjawiska te nie są nowe i dotyczą każdego obszaru ludzkiej egzystencji. Także w obszarze ekonomicznym i gospodarczym mieliśmy z tym do czynienia, najczęściej w postaci różnorodnych piramid finansowych i wielopoziomowych biznesów.

Z punktu widzenia nauki, w ujęciu zarówno teoretyków, jak również praktyków, *informacja* jest pojęciem pierwotnym, niedającym się w prosty sposób zdefiniować, zidentyfikować, mówiąc kolokwialnie – zaszufladkować. Uwarunkowane to jest między innymi tym, że informacja funkcjonuje w różnorodnym środowisku (politycznym, fizycznym, matematycznym, ekonomicznym, religijnym, prawnym itp.). Spora grupa autorów rezygnuje z definiowania informacji, poprzestając na jej intuicyjnym i potocznym postrzeganiu. Niemniej jednak należy zaznaczyć, że samo słowo *informacja* wywodzi się z łacińskiego słowa *informatio*, określanego jako *wyobrażenie*, *wyjaśnienie*, *zawiadomienie*, co pozwala na wyciągnięcie wniosków, że dotyczy ona sfery postrzegania, percepcji odbiorcy tejże informacji. Patrząc przez pryzmat dorobku wielu pokoleń naukowców zajmujących się teorią informacji można dostrzec, że największy dorobek w tym obszarze mieli Claude E. Shannon, Norbert Wiener, Russell L. Ackoff, Andrew Webster. Postrzegali oni informację jako[1]:

- *Informacja to komunikacja, łączność, w wyniku której likwiduje się nieokreśloność* (Claude E. Shannon).
- *Informacja jest nazwą treści zaczerpniętej ze świata zewnętrznego, nie jest więc ani materią, ani energią* (Norbert Wiener).
- *Jest to przekazywanie wiedzy do odbiorcy informacji, ze względu na jej wartość, umożliwiające zmniejszenie niepewności działania odbiorcy informacji* (Russell L. Ackoff).
- *Informacja jest to wiedza przekazywana przez innych ludzi bądź uzyskiwana przez studia, obserwacje, badania* (Andrew Webster).

W polskiej myśli naukowej znamienne są rozważania Leopolda Ciborowskiego, który w książce *Walka informacyjna* podjął się analizy terminu *informacja*, powołując się na definicje stworzone przez naukowców z obszaru cybernetyki i fizyki. Zauważył, że informacja jest bodźcem oddziałującym na układ recepcyjny człowieka, który skutkuje zbudowaniem, w jego wyobraźni, przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej i abstrakcyjnej kojarzącym

[1] W. Flakiewicz, *Podejmowanie decyzji kierowniczych*, Państwowe Wydawnictwo Ekonomiczne, Warszawa 1973, s. 38.

się z tym bodźcem. Ciborowski podkreślił, że związek między człowiekiem i informacją jest nierozerwalny: *tak jak foton nie może istnieć bez pędu, tak informacja nie może istnieć bez umysłu ludzkiego. Tylko ten organ natury ludzkiej dostosowany jest do nieskończonego przetwarzania transformowanych doznań recepcyjnych w wyobrażenia informacyjne.* […] *każda informacja jest szczególną formą sygnału, która oprócz wspólnych cech wyróżnialności, właściwych dla sygnału i informacji, posiada jeszcze tę właściwość, że inspiruje umysł ludzki do tworzenia pewnej wyobraźni*[2]. Tym samym określił, że informacja jest zależna od człowieka. Nie uwzględniono tutaj aspektów rozwoju technologii, w tym głównie sztucznej inteligencji, która, w założeniach projektowych, powinna być zdolna do operowania na zbiorach informacji tak jak człowiek.

Z kolei Piotr Sienkiewicz, uznany polski cybernetyk i informatyk, postrzega informację jako *zbiór faktów, zdarzeń, cech, obiektów ujęty w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne*[3]. Jest ona zbieżna z poglądami Ciborowskiego, z tym, że w powyższej definicji nie zdefiniowano, kim jest odbiorca informacji.

Sama informacja w swej istocie ma wymiar strukturalny, co wyraża się tym, że w każdej strukturze zawiera się informacja warunkująca zachowanie prawidłowej formy tej struktury, odnosząca się do celów, wartości oraz sposobów funkcjonowania danej struktury. Na rysunku 1.1. zobrazowano model tej struktury.

Analiza przedstawionych elementów, począwszy od podstawy do wierzchołka, czyli od surowych danych (fizycznej postaci informacji), poprzez zorganizowane informacje (dane, które mogą być zinterpretowane za pomocą posiadanego aparatu interpretacyjno-poznawczego), informacje przetworzone do poziomu wiedzy (zinterpretowane, zrozumiane i przyjęte) oraz najwyższego poziomu informacji, czyli mądrości (bazującej na wiedzy, nauce, wykształceniu i doświadczeniu), pozwala na spostrzeżenie, że dane, aby mogły się stać informacją, muszą zostać przetworzone, a do tego jest niezbędna wiedza i aparat interpretacyjno-poznawczy. Suche fakty, dane w tabelkach Excela staną się informacją tylko wtedy, gdy będziemy potrafili się do nich odnieść, przetworzyć na bazie posiadanej wiedzy i doświadczenia.

Dwa najniższe szczeble piramidy informacyjnej odnoszą się do podejścia przetwarzania, zaś dwa górne do podejścia strukturalnego. Dane przetwarzamy, informację interpretujemy i na tej podstawie budujemy struktury, które pozwalają zarządzać posiadaną wiedzą i mądrością.

Szczeble te są autonomiczne, niezależne do siebie. Większa ilość danych nie oznacza automatycznie większej ilości informacji. Analogicznie, większa ilość informacji nie jest tożsama ze zwiększeniem wiedzy, wręcz przeciwnie – zbyt duża ilość informacji może ograniczyć wiedzę poprzez wpływ na jej szybkie spożytkowanie.

Wiedza będąca motorem napędowym ludzkości jest *zasobem wiadomości, które ludzie zdobywają poprzez badania naukowe, i przekazują następnym pokoleniom, np. w książkach lub przez nauczanie,* lub też tym *czego się nauczyliśmy, co zapamiętaliśmy i co umiemy wykorzystać*"[4].

Rysunek 1.1. Piramida informacyjna
Źródło: P. Sienkiewicz, Wiek informacji. Wykład inauguracyjny Wyższej Szkoły Informatyki, Warszawa 2000.

[2] L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń 1999, s. 59.
[3] P. Sienkiewicz, *Systemy kierowania,* Wiedza Powszechna, Warszawa 1989, s. 128.
[4] *Słownik języka polskiego*, Wydawnictwo Naukowe PWN, Warszawa 2007.

Jest również *ogółem wiarygodnych informacji o rzeczywistości wraz z umiejętnością ich wykorzystania*[5]. To też *rezultat wszelkich aktów poznania; związki między wiedzą a poznaniem mają charakter wzajemnego oddziaływania; wiedza jest rezultatem poznania, a zarazem poznanie jest w dużej mierze uwarunkowane przez wiedzę*[6]. Wiedza charakteryzuje się pewnymi cechami, do których można zaliczyć:

– dominację nad innymi strategicznymi zasobami organizacji;

– niewyczerpalność wartości z chwilą jej przekazania lub wykorzystania;

– możliwość jej równoległego, równoczesnego wykorzystywania przez wszystkie podmioty posiadające do niej dostęp;

– możliwość jej wykorzystania w dowolnym czasie;

– brak korelacji pomiędzy wiedzą a umiejętnością jej wykorzystania.

Informacja jest podstawą do budowania każdego systemu wiedzy. Warunkuje sukces w każdej dziedzinie działalności człowieka, w szczególności w takich sferach, jak: gospodarka, ekonomia, polityka, bezpieczeństwo, społeczeństwo. Powyższe jest prawdziwe wtedy i tylko wtedy, gdy system wiedzy będzie budowany w oparciu o wiarygodne i aktualne informacje, a do ochrony informacji zastosujemy podejście systemowe.

W przytaczanych definicjach pojawia się aspekt komunikacji, komunikowania. Według zapisów encyklopedycznych komunikowanie to: *podać coś do wiadomości; przekazać jakąś informację, zawiadomić o czymś*[7]. *Komunikować się* zdefiniowano jako: *utrzymywać z kimś kontakt, porozumiewać się*. Przekazywanie informacji w akcie komunikowania, postrzegane jako proces komunikacji międzyludzkiej, zostało zobrazowane w modelu Claude Shannon, na rysunku 1.2.

W modelu tym proces przekazywania informacji rozpoczyna się od nadawcy, określanego zamiennie jako źródło informacji. Przekaz ten (informacja w postaci danych) jest przekształcany przez nadajnik w odpowiedni sygnał (zrozumiały dla systemów technicznych), który za pośrednictwem kanału jest przekazywany do odbiornika, gdzie następuje jego zamiana na postać zrozumiałą dla odbiorcy (dane, które odbiorca potrafi przekształcić w informację). Sygnał w trakcie przekazywania przez kanał jest podatny na różnorodne szumy (zakłócenia), mające wpływ na jego poprawną interpretację przez odbiornik. Komunikacja w tym modelu może być podzielona na osiem elementów[8]:

1. Źródło jest twórcą aktu komunikacji;

2. Przekaz jest treścią komunikacji, informacją, która jest przekazywana;

3. Koder przetwarza informację w formę, która może być zakomunikowana, także w postaci, która nie jest bezpośrednio rozumiana przez ludzkie zmysły;

4. Kanał jest medium lub systemem transmisyjnym używanym dla przekazu komunikatu z jednego miejsca do innego;

5. Dekoder odwraca proces kodowania;

6. Odbiorca jest adresatem komunikacji;

7. Sprzężenie zwrotne między źródłem a odbiorcą może służyć do regulacji przepływu komunikacji;

8. Szum jest niepożądanym zniekształceniem, które może zakłócać wymianę informacji.

Model ten jest powszechnie wykorzystywany w systemach technicznych, a jego najprostszymi reprezentantami są modele odniesienia ISO/OSI i TCP/IP. Z uwagi na swój techniczny aspekt zakłada się, że szum

Rysunek 1.2. Model komunikacyjny Shannona

Źródło: T. Goban-Klas, P. Sienkiewicz, Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999, s. 5.

[5] *Nowa encyklopedia powszechna PWN, tom 4*, Wydawnictwo Naukowe PWN, Warszawa 1996.

[6] *Wielka encyklopedia PWN, tom 17*, Wydawnictwo Naukowe PWN, Warszawa 2003.

[7] *Słownik języka polskiego*, t. I, Wydawnictwo Naukowe PWN, Warszawa 1993, s. 981.

[8] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania,* Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999, s. 6.

powstający w kanale komunikacyjnym jest pochodną stosowanych rozwiązań technicznych i związaną z nimi niezawodnością i wydajnością. Szum może być także powodowany celowym oddziaływaniem na funkcjonalność kanałów komunikacyjnych. W tym przypadku mamy do czynienia z działaniem ukierunkowanym na funkcjonalność systemów technicznych, a nie na użytkowników i ich zdolność percepcji otrzymanej informacji.

Odmiennie proces przekazywania informacji widzi Horold Lasswell. Model przez niego opracowany składa się z pięciu zasadniczych części, przedstawionych na rysunku 1.3.

Rysunek 1.3. Model analizy aktu komunikowania Harolda Lasswella
Źródło: T. Goban-Klas, P. Sienkiewicz, Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999, s. 7.

Model ten jest wykorzystywany do form międzyludzkiego komunikowania, w których nadawca za główny cel przekazu stawia sobie zmianę postaw, poglądów lub zachowania odbiorców. Jest on wykorzystywany do tworzenia kampanii informacyjnych, prowadzonych za pośrednictwem środków masowego przekazu, ukierunkowanych na manipulowanie świadomością odbiorców. Środowiskiem przekazu sprzyjającym manipulowaniu jest współcześnie cyberprzestrzeń z wiodącą rolą portali społecznościowych.

Przeprowadzone analizy wykazały, że współcześnie informacja jest czymś dużo więcej niż tylko wiadomością, znakiem lub inną formą komunikowania. W swojej istocie jest ona zarówno opisem rzeczywistości, jak i odzwierciedleniem tej rzeczywistości, niekoniecznie z nią zgodnym.

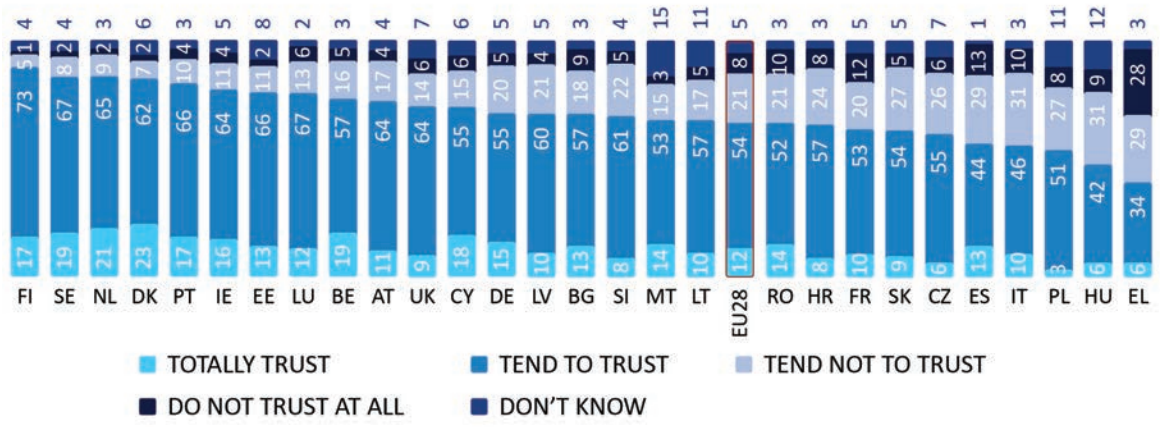
Powyższe jest niezmiernie istotne z punktu widzenia działań, jakie są podejmowane w cyberprzestrzeni. Informacja bowiem jest odbiciem obrazu rzeczywistości, a nie samą rzeczywistością, tym samym nie musi być prawdą lub stanem faktycznym. Na podstawie odbicia budowana jest wiedza, która jest pochodną wielu czynników, takich jak: wykształcenie, doświadczenie, przekonanie, nastawienie, samopoczucie itp. Wiedza będąca pochodną *wiarygodnych* informacji jest gwarantem poprawności interpretacji informacji i odpowiedniego się do niej ustosunkowania. Jeżeli uzyskany w wyniku aktu komunikowania obraz rzeczywistości nie będzie zgodny z prawdą, a pozyskana informacja nie będzie cechowała się *wiarygodnością*, to stworzona na jej podstawie wiedza będzie błędna i nie zagwarantuje prawidłowego postrzegania rzeczywistości. W takie podejście do komunikowania wpisuje się walka w cyberprzestrzeni, ukierunkowana na informację, w której ogromne znaczenie odgrywa komunikacja strategiczna, dezinformacja i propaganda.

Pojęciem związanym bezpośrednio z informacją jest *przestrzeń informacyjna*, której rozwój jest nierozerwalnie związany z historią ludzkości. Pierwotnie przestrzeń ta obejmowała swym zasięgiem lokalne społeczności – takie, jak plemiona czy grupy etniczne. Z upływem czasu, wraz z rozwojem struktur społecznych i wykorzystywanych sposobów i narzędzi komunikacyjnych, jej zasięg się zwiększał. Ograniczenia komunikacyjne związane były z zasięgiem, czasem i sposobem przekazywania informacji. Ograniczenia te zostały przełamane wraz z rozwojem telegrafu, telefonu, szeroko pojmowanej telekomunikacji, informatyki i teleinformatyki, co umożliwiło diametralne zmiany w przestrzeni informacyjnej, która obejmuje swym zasięgiem całą powierzchnię kuli ziemskiej, a wymiana informacji jest natychmiastowa. Współczesna przestrzeń informacyjna jest złożoną całością różnorodnych interakcji, wartości i funkcji łączących światy rzeczywiste, wirtualne, indywidualne, społeczne, przeszłe, obecne jak i przyszłe[9]. To już nie tylko przestrzenne narzędzie wymiany informacji pomiędzy składowymi systemu bezpieczeństwa podmiotu, ale również odbicie ich wzajemnych powiązań i relacji[10].

W 2018 roku w Unii Europejskiej przeprowadzono badania dotyczące fakenewsów i dezinformacji[11],

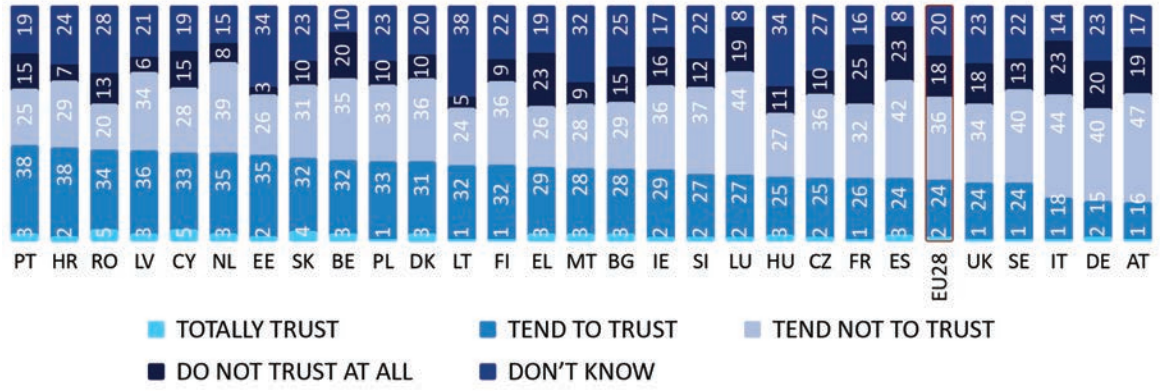
[9] Por.: S. Jaskuła, *Informacyjna przestrzeń tożsamości*, Materiały Szkoleniowe Ośrodka Rozwoju Edukacji, ORE, Warszawa 2010, s. 1.
[10] Por.: R. Kwećka, *Strategia bezpieczeństwa informacyjnego państwa*, Akademia Obrony Narodowej, Warszawa 2014, s. 25.
[11] *Fake news and disinformation online*, Survey requested by the European Commission, Directorate-General for Communications Networks, Content & Technology and co-ordinated by the Directorate-General for Communication, Flash Eurobarometer 464, kwiecień 2018.

w których uwzględniono wszystkie media stanowiące współczesną przestrzeń informacyjną. Ocenie poddano wiarygodność informacyjną mediów w oczach obywateli Unii Europejskiej. Na rysunku 1.4. i 1.5. przedstawiono poziom zaufania do tradycyjnej telewizji i portali społecznościowych.



Rysunek 1.4. Poziom zaufania Europejczyków do telewizji

Źródło: Fake news and disinformation online, Survey requested by the European Commission, Directorate-General for Communications Networks, Content & Technology and co-ordinated by the Directorate-General for Communication, Flash Eurobarometer 464, kwiecień 2018, s. 7.



Rysunek 1.5. Poziom zaufania Europejczyków do portali społecznościowych

Źródło: Fake news and disinformation online, Survey requested by the European Commission, Directorate-General for Communications Networks, Content & Technology and co-ordinated by the Directorate-General for Communication, Flash Eurobarometer 464, kwiecień 2018, s. 9.

We wspominanych badaniach udział wzięło 26 576 respondentów z 28 krajów członkowskich Unii Europejskiej. Na uwagę zasługuje fakt, że w dalszym ciągu tradycyjne media cieszą się większym zaufaniem niż media online, niemniej jednak ich znaczenie z roku na rok spada. Zaufanie do klasycznych mediów kształtowało się na poziomie od 70% dla radia, poprzez 66% dla telewizji i 63% dla drukowanych gazet i magazynów. Zaufanie do mediów dostępnych w sieci Internet było niższe i wynosiło od 47% dla gazet i magazynów dostępnych online, 27% dla hostingu wideo i podcastów i 26% dla portali społecznościowych i aplikacji informacyjnych. Wyniki badań umożliwiają dostosowanie przekazów informacyjnych do odpowiednich mediów i ich odbiorców, i zwiększenie ich skuteczności oddziaływania.

1.2. Bezpieczeństwo informacyjne

Każdy świadomy zagrożeń podmiot bezpieczeństwa ukierunkowuje swoją działalność na ochronę posiadanych zasobów, zwłaszcza informacyjnych, które są jednym z najważniejszych we współczesnym świecie. Niestety są też takie podmioty, które są nieświadome istniejących zagrożeń lub też nie widzą potrzeby ochrony tego, co cenne, uważając, że za ich ochronę odpowiada państwo. Najczęściej podmiotami tymi są ludzie, którzy o znaczeniu

ochrony informacji dowiadują się w chwili, gdy staną się ofiarami przestępstwa popełnionego w cyberprzestrzeni, ukierunkowanego na kradzież tożsamości, przejęcie kont pocztowych lub kont w portalach społecznościowych, kradzież pieniędzy z kont bankowych poprzez przejęcie informacji autoryzujących transakcje, szantaż i wymuszenie poprzez np. zaszyfrowanie zasobów osobistego komputera czy też wykradzenie kompromitujących materiałów. Zagrożenia te dotyczą także małych organizacji i najczęściej są powodowane już nie tylko nieświadomością, lecz względami ekonomicznymi. Bezpieczeństwo bowiem kosztuje, zarówno w aspekcie organizacyjnym (opracowanie i wdrożenie procedur postępowania oraz właściwej struktury organizacyjnej), ludzkim (zatrudnienie specjalistów z obszaru cyberbezpieczeństwa), jak i pod względem materiałowym (zakup sprzętu, oprogramowania i usług niezbędnych do zwiększenia poziomu bezpieczeństwa). Dla podmiotów takich jak państwa, korporacje, organizacje międzynarodowe, banki ochrona posiadanych zasobów informacyjnych jest czynnikiem krytycznym, warunkującym skuteczność organizacji. Działania z obszaru ochrony i obrony zasobów informacyjnych wpisują się w *bezpieczeństwo informacyjne podmiotu*, które w odróżnieniu od *bezpieczeństwa informacji*, jest pojęciem złożonym i dużo trudniejszym do uchwycenia. Dlatego też ważne jest umiejętne kreowanie bezpieczeństwa informacyjnego, polegającego nie tylko na ochronie własnych zasobów informacyjnych, lecz przede wszystkim na przeciwstawieniu się wrogim kampaniom informacyjnym ukierunkowanym na osłabienie i destabilizację atakowanego podmiotu. Informacja jest bowiem nie tylko obiektem wrogiego oddziaływania, ale także, a może przede wszystkim, narzędziem ataku, współczesną bronią.

Bezpieczeństwo informacji, składowa bezpieczeństwa informacyjnego podmiotu, definiowane jest różnorodnie, w zależności od aspektów i dziedziny odpowiedzialności. Mówiąc ogólnie, *bezpieczeństwo informacji to stan, w którym zapewniona jest swoboda dostępu i przepływu informacji połączona z racjonalnym i prawnym wyodrębnieniem takich kategorii, które podlegają ochronie ze względu na bezpieczeństwo podmiotów, których dotyczą*[12]. To też *stan lub ochrona przed niekontrolowanymi stratami i skutkami, kombinacja usług zapewniających poufność, integralność i dostępność*[13].

Analizy literatury wykazały, że dosyć często *bezpieczeństwo informacyjne* jest mylone z *bezpieczeństwem informacji*. Ten dysonans wynika najprawdopodobniej z powszechnie stosowanej w naukach o bezpieczeństwie klasyfikacji podmiotowej i przedmiotowej samego bezpieczeństwa. W klasyfikacji podmiotowej informacja nie występuje jako podmiot bezpieczeństwa, nie jest postrzegana jako byt. Patrząc przez pryzmat samej definicji informacji, jest ona często postrzegana jako wytwór ludzkiego umysłu uwarunkowany posiadanym aparatem poznawczym i danymi, które ten aparat postrzega, przetwarza, przyswaja, ustosunkowuje się i podejmuje działania. Dlatego też najczęściej występują definicje, w których jest mowa nie o samym bezpieczeństwie informacji, ale o *bezpieczeństwie danych* postrzeganym jako *ogół przedsięwzięć podejmowanych w celu zabezpieczenia danych przetwarzanych w systemie teleinformatycznym przed nieupoważnionym dostępem począwszy od ich powstania, poprzez okres użytkowania i dystrybucji aż do zniszczenia*[14].

W klasyfikacji przedmiotowej mamy do czynienia z bezpieczeństwem informacyjnym jako bezpieczeństwo przedmiotowe podmiotu bezpieczeństwa. Użycie formy przymiotnikowej sprawia, że zawsze chodzi o bezpieczeństwo informacyjne podmiotu bezpieczeństwa, takiego jak: człowiek, społeczeństwo, organizacja, państwo, organizacja międzynarodowa. A skoro mówimy o bezpieczeństwie podmiotu jako całości, to należy zastanowić się, czy bezpieczeństwo to może być zrealizowane tylko i wyłącznie na drodze ochrony posiadanych zasobów informacyjnych. Analizy przykładów historycznych wykazały, że bezpieczeństwo informacyjne podmiotu nie może być zawężone tylko do ochrony zasobów i terminy "bezpieczeństwo informacyjne" i "bezpieczeństwo informacji" nie mogą być stosowane zamiennie. Bezpieczeństwo informacji jest jednym z elementów składowych bezpieczeństwa informacyjnego podmiotu.

Bezpieczeństwo informacji w swojej istocie ogranicza się do zapewnienia tak zwanych atrybutów informacji. Osiągane jest na trzech poziomach: organizacyjnym, technicznym i fizycznym, najczęściej poprzez implementację systemu zarządzania bezpieczeństwem informacji, bazującym na przyjętych normach. Prawidłowe definicje bezpieczeństwa informacji można odnaleźć najczęściej w normatywach. Jedna z takich definicji identyfikuje bezpieczeństwo informacji jako *stan lub ochrona przed niekontrolowanymi stratami*

[12] W. Fehler, *Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i prawne*, Wydawnictwo Arte, Warszawa 2012.
[13] PN-I-02000:2002 *Technika informatyczna – Zabezpieczenie w systemach informatycznych – Terminologia*, Polski Komitet Normalizacyjny, Warszawa 2002.
[14] Patrz: *Słownik terminów z zakresu bezpieczeństwa narodowego*, Akademia Obrony Narodowej, Warszawa 2008.

i skutkami, kombinacja usług zapewniających poufność, integralność i dostępność[15]. Wymienione poufność, integralność i dostępność są krytycznymi atrybutami informacji warunkującymi jej bezpieczeństwo. Inne definicje bezpieczeństwa informacji postrzegają ją jako *ochronę i obronę informacji i systemów informacyjnych przed nieupoważnionym dostępem lub modyfikacją informacji w czasie jej przechowywania, obróbki lub przesyłania, oraz przed zakłóceniami w dostępie osób upoważnionych; bezpieczeństwo informacji obejmuje przedsięwzięcia niezbędne do wykrywania, dokumentowania i przeciwdziałania takim zagrożeniom*[16] lub też jako *ochronę informacji przed nieupoważnionym rozpowszechnianiem, przekazywaniem, wprowadzeniem zmian lub zniszczeniem zarówno przypadkowym, jak i zamierzonym*[17].

Analiza obowiązujących norm wykazała, że bezpieczeństwo informacji jest także postrzegane przez pryzmat bezpieczeństwa systemów teleinformatycznych przetwarzających informację, co skutkuje dodaniem takich atrybutów bezpieczeństwa jak: niezaprzeczalność, rozliczalność, autentyczność i niezawodność[18].

Bezpieczeństwo informacyjne wykracza w istotny sposób poza ramy obowiązujących norm. Informacja stała się narzędziem i środkiem w dążeniu do przyjętych celów działania. W bezpieczeństwie informacyjnym, oprócz zapewnienia bezpieczeństwa informacji, niezwykle istotne jest stosowanie elementów walki informacyjnej z dezinformacją i propagandą włącznie. Jej umiejętne wykorzystanie pozwala nie tylko na działanie z pozycji dodatniej w stosunku do potencjalnych przeciwników, ale także umożliwia kreowanie rzeczywistości, które może postawić dowolny podmiot bezpieczeństwa zarówno w korzystnym, jak i niekorzystnym świetle. Każdy podmiot bezpieczeństwa musi być jednocześnie świadomy, że także on może być celem oddziaływania informacyjnego, dezinformacji i propagandy ukierunkowanych na dyskredytację, zmniejszenie wpływów, poniesienie wymiernych strat czy nawet zniszczenie i eliminację. Zdolność skutecznego przeciwstawienia się wrogim kampaniom informacyjnym i zidentyfikowanie, kto za nimi stoi, staje się newralgicznym elementem funkcjonowania każdego podmiotu i najważniejszym czynnikiem skutecznego działania. Sprowadzenie problemu wyłącznie do ochrony posiadanych zasobów informacyjnych nie gwarantuje współcześnie działania z pozycji dodatniej.

Bezpieczeństwo informacyjne to transsektorowy obszar bezpieczeństwa, który odnosi się do środowiska informacyjnego. Jest to ciągły proces, którego celem jest zapewnienie bezpiecznego funkcjonowania podmiotu bezpieczeństwa w przestrzeni informacyjnej poprzez panowanie we własnej infosferze i zabezpieczenie własnych interesów. Jego realizacja wymaga:

- zapewnienia odpowiedniego poziomu ochrony posiadanych zasobów informacyjnych,
- przeciwstawienia się wrogim kampaniom dezinformacyjnym i propagandzie,
- prowadzenia aktywnych, informacyjnych działań ofensywnych wobec rywali (przeciwników).

Powyższe zadania powinny znaleźć odzwierciedlenie w strategii każdego państwa, a ich implementacja umożliwi stworzenie systemu bezpieczeństwa informacyjnego[19]. Bezpieczeństwo informacyjne występuje zarówno w środowisku wewnętrznym, zewnętrznym, militarnym, niemilitarnym, osobowym, społecznym, technologicznym, jak i wielu innych. Dla zapewnienia całościowego bezpieczeństwa informacyjnego ważne jest określenie celów realnych i głównych niewiadomych, które powinny być rozpatrywane z uwzględnieniem: zagrożeń, wyzwań, szans i ryzyka.

Bezpieczeństwo informacyjne jest najdelikatniejszą sferą bezpieczeństwa, zarówno w państwie, jak również na arenie międzynarodowej. Ma bezpośredni wpływ na skuteczność funkcjonowania całego systemu bezpieczeństwa narodowego i międzynarodowego. Dodatkowo działania w tym obszarze muszą być podejmowane z uwzględnieniem praw człowieka i obywatela, a w szczególności poszanowania prawa do prywatności i wolności słowa, co nie jest takie proste i oczywiste. Najczęściej bowiem, wraz ze wzrostem poziomu bezpieczeństwa informacyjnego ograniczane są prawa człowieka i obywatela.

Nieodzownym elementem bezpieczeństwa informacyjnego jest walka informacyjna, która współcześnie jest elementem polityki podmiotów

[15] Patrz: *PN-I-02000:2002 Technika Informatyczna – Zabezpieczenie w systemach informatycznych – Terminologia*.
[16] *Regulamin działań wojsk lądowych nr 115/2008*, DWLąd, Warszawa 2008, s. 402.
[17] *AAP-31(A) Słownik terminów i definicji dotyczących systemów łączności i informatyki NATO,* STANAG 5064, Agencja Standaryzacji NATO, 2001., s. 12.
[18] Szerzej na temat atrybutów: J. Kowalewski, *Modelowanie bezpieczeństwa informacji … op. cit., s. 35*
[19] Z. Nowakowski, H. Szafran, R. Szafran, *Bezpieczeństwo w XXI wieku. Strategia bezpieczeństwa narodowego Polski i wybranych państw*, Towarzystwo Naukowe Powszechne, Rzeszów 2009, s. 67.

bezpieczeństwa, takich jak państwa czy też korporacje, a ich głównym celem jest działanie z pozycji dodatniej w stosunku do przeciwnika (rywala, konkurenta biznesowego). Zdobywanie informacji, ochrona własnych zasobów informacyjnych oraz prowadzenie kampanii informacyjnych odgrywają i będą odgrywać coraz większą rolę w otaczającym nas świecie.

W zakres bezpieczeństwa informacyjnego, oprócz wymienionych bezpieczeństwa informacji, dezinformacji i propagandy, wchodzi także komunikacja strategiczna, jako jedne z narzędzi skutecznego kształtowania pozytywnego wizerunku podmiotu bezpieczeństwa, zarówno we własnym środowisku, jak i w otoczeniu. Komunikacja strategiczna jest postrzegana jako *synteza działań informacyjnych danego podmiotu strategicznego (np. państwa, sojuszu, koalicji) ukierunkowanych na kształtowanie poglądów, ocen, opinii itp. oraz decyzji innych podmiotów z otoczenia korzystnych dla własnych interesów strategicznych*[20]. Prekursorami w rozwoju komunikacji strategicznej byli Amerykanie, którzy postrzegali ją jako *skoncentrowane procesy i wysiłki podejmowane w celu zrozumienia oraz zaangażowania kluczowych odbiorców dla stworzenia, wzmocnienia lub utrwalenia warunków korzystnych dla realizacji narodowych interesów i celów poprzez zastosowanie skoordynowanych informacji, tematów, planów, programów oraz działań zsynchronizowanych z przedsięwzięciami realizowanymi przez pozostałe elementy władz państwowych*[21].

Znaczenie komunikacji strategicznej zwiększyło się wraz z rozwojem mediów i możliwością dotarcia do szerokiego grona odbiorców. Coraz większą rolę odgrywa cyberprzestrzeń i portale społecznościowe, stanowiące doskonałe środowisko do prowadzenia kampanii informacyjnych. Komunikacja strategiczna dotyczy takich sfer, jak[22]:

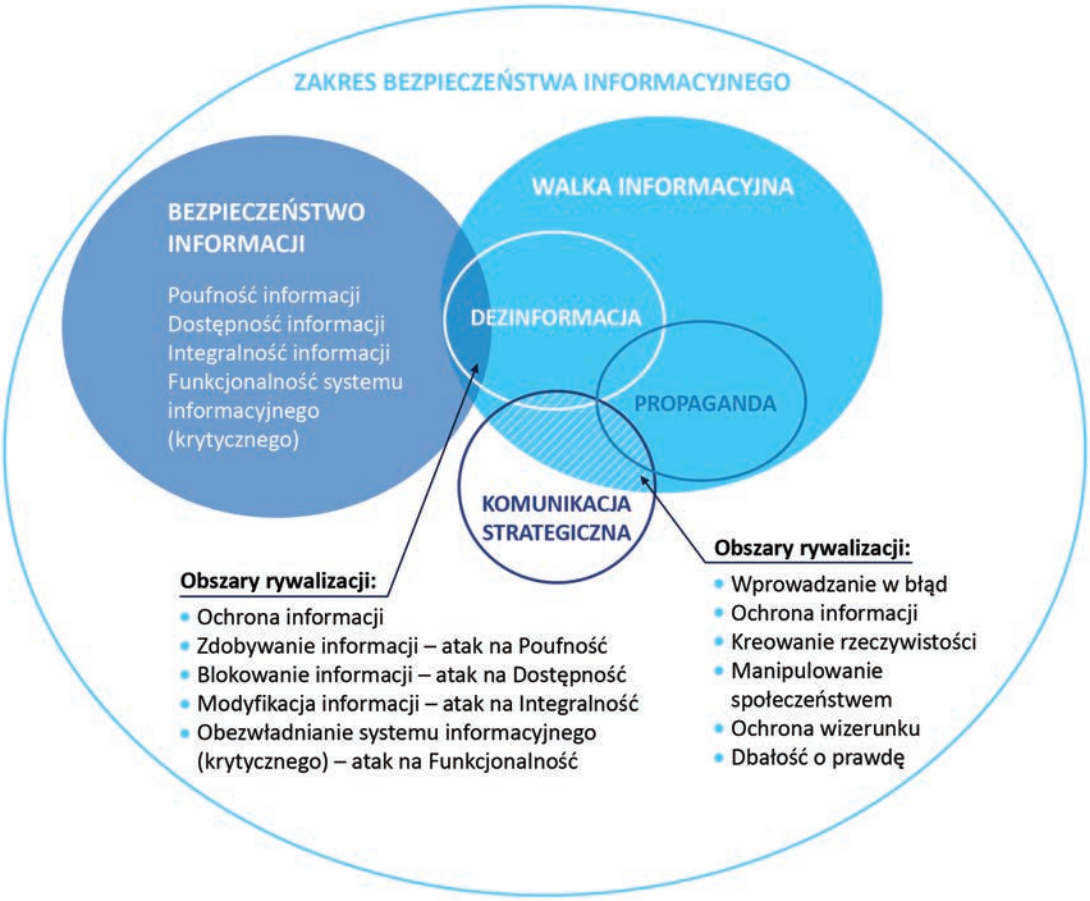
- dyplomacja publiczna,
- public affairs – komunikacja społeczna,
- operacje informacyjne,
- operacje psychologiczne.

Dyplomacja publiczna odpowiada za kreowanie pozytywnego wizerunku państwa na arenie międzynarodowej. Robione to jest na drodze działalności informacyjnej i kulturowej, za pomocą promowania wartości i tożsamości historycznej wśród tych wszystkich odbiorców, którzy stanowią społeczność międzynarodową. Public affairs swoim przekazem jest ukierunkowane na społeczeństwo danego państwa i wykorzystuje rozmaite narzędzia komunikowania wewnątrzpaństwowego. Operacje informacyjne z kolei mogą mieć charakter zarówno ofensywny, jak i defensywny. Działania ofensywne podejmowane są w celu *wpływania na informację i systemy informacyjne przeciwnika przy jednoczesnej ochronie własnej informacji i systemów informacyjnych*[23]. Działania defensywne związane są z *przedsięwzięciami na rzecz ochrony systemów informacyjnych oraz szeroko rozumianej poprawy komunikacji w płaszczyznach: polityki, procedur, operacji, personelu i technologii, oddziałujących na sprawność zarządzania państwem*[24]. Ostatni element komunikacji strategicznej – operacje psychologiczne – związane są z pozyskiwaniem, kreowaniem i pozycjonowaniem informacji, które z oczekiwanie wysokim prawdopodobieństwem wpłyną na sposób postrzegania rzeczywistości przez odbiorców[25].

Na rysunku 1.6. przedstawiono główne obszary odpowiedzialności bezpieczeństwa informacyjnego. Pierwszy z nich obejmuje zapewnienie bezpieczeństwa informacji w aspekcie zachowania poufności, dostępności i integralności informacji oraz utrzymania funkcjonalności systemów informacyjnych i krytycznych. Drugi jest związany z przeciwstawieniem się wrogim kampaniom informacyjnym w celu ochrony własnego wizerunku i dbałości o prawdę.

Bezpieczeństwo informacyjne w zależności od podmiotu, który za nie odpowiada i przyjętych celów działania może mieć wymiar zarówno pozytywny, jak i negatywny. W wymiarze pozytywnym na pierwszy plan wysuwa się ochrona własnych zasobów informacyjnych oraz dbałość o wizerunek i prawdę. Tym samym istotnego znaczenia, oprócz ochrony informacji, nabiera komunikacja strategiczna. Bezpieczeństwo informacyjne w wymiarze negatywnym jest ukierunkowane w głównej mierze na agresywne zdobywanie informacji o stronie przeciwnej oraz kreowanie rzeczywistości poprzez szerzenie dezinformacji i propagandy.

[20] J. Nowicka, W. Załoga, Z. Ciekanowski, *Komunikacja strategiczna w naukach o zarządzaniu i jakości oraz w naukach o bezpieczeństwie*, „Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach", 2018 nr 1 (14), s. 196.
[21] T. Kacała, *Komunikacja strategiczna*, [w:] Przegląd Morski nr 3/2012, s. 18.
[22] Ibidem, s. 197.
[23] Ibidem.
[24] Ibidem.
[25] Ibidem.



Rysunek 1.6. Zakres bezpieczeństwa informacyjnego
Źródło: P. Dela, Założenia działań w cyberprzestrzeni, Wydawnictwo Naukowe PWN, Warszawa 2022.

1.3. Zagrożenia informacyjne

Analiza literatury wykazała, że podstawą współczesnych zagrożeń informacyjnych jest sterowanie informacją, której podwaliny wywodzą się z cybernetyki, a dokładniej z pracy Norberta Wienera zatytułowanej *Cybernetics or Control and Communication in the Animal and the Machine*[26]. Z kolei polski cybernetyk Marian Mazur w książce *Jakościowa teoria informacji*[27] przedstawił i wyodrębnił te elementy cybernetyki, które są wykorzystywane głównie jako narzędzie walki informacyjnej. Przedmiotami stworzonej teorii sterowania informacją, głównie w ujęciu jakościowym, są systemy i relacje zachodzące między nimi, co przedstawiono na rysunku 1.7.

W zaprezentowanym ujęciu *sterowanie informacją*, pomiędzy oryginałem (postrzeganym jako zjawisko, fakt lub też dana) a obrazem (postrzeganym jako informacja wytworzona na podstawie tegoż oryginału), polega na transformacji informacji zarówno wiernej, jak również zniekształconej. Przykładem systemu korzystającego

Rysunek 1.7. Proces sterowania i tworzenia informacji
Źródło: Opracowanie na podstawie M. Mazur, Cybernetyka i charakter, WSZiP im. Bogdana Jańskiego w Warszawie, Warszawa 1999, s. 45

[26] N. Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine*, (Hermann & Cie) & Camb. Mass. (MIT Press), Paris 1948.
[27] M. Mazur, *Jakościowa teoria informacji*, Wydawnictwo Naukowo Techniczne, Warszawa 1970.

ze sprzężenia zwrotnego jest człowiek, postrzegany jako jednostka sterowalna, podatna na manipulacje, perswazję, czy też działania pod przymusem; jak i sterująca, będąca liderem, motywująca inne osoby do działania. Sterowanie informacją może mieć formę aktywną, w której generowane są informacje ukierunkowane bezpośrednio na sterowanie obiektem oddziaływania, jak również formę pasywną, w której informacja jest biernie wykorzystywana do sterowania wieloma obiektami.

W procesach zarządzania informacją wykorzystywane są najczęściej takie metody, jak[28]: transinformowanie, parainformowanie, pseudoinformowanie, dezinformowanie i metainformowanie.

Transinformowanie polega na wiernym i dokładnym przekształcenie oryginału w obraz. Zachodzi ono wtedy, gdy: oryginał jest zarazem obrazem, oryginał jest taki sam jak obraz, obraz jest analogicznie przedstawiony, oryginał jest pośrednio zniekształcony, a następnie jest odwrotnie przekształcony w obraz.

Parainformowanie związane jest głównie z błędami popełnianymi podczas odniesienia się do oryginału, uwarunkowanymi ułomnością, niedoskonałością ludzkiego umysłu czy też wadą interpretacyjną, niezrozumieniem.

Pseudoinformowanie, określane jako informowanie pozorne, polega na uzyskiwaniu informacji na podstawie innych informacji cząstkowych, będących zbiorem różnorodnych danych, pozyskanych z różnych źródeł, często niesprawdzonych, niewiarygodnych czy wręcz przekłamanych i zmanipulowanych. Wyróżnia się pseudoinformowanie symulacyjne, dysymulacyjne i konfuzyjne. Pierwsze z nich – *pseudoinformowanie symulacyjne* – określane także jako informowanie rozwlekłe, polega na przekształceniu jednego oryginału w kilka poszczególnych obrazów, które odnoszą się do tego samego obrazu i nie wnoszą nic nowego. *Pseudoinformowanie dysymulacyjne,* określane także jako informowanie ogólnikowe, związane jest z przekształceniem kilku oryginałów w jeden całościowy obraz, oddający ogólny charakter poszczególnych oryginałów w dużym uproszeniu. Z kolei *pseudoinformowanie konfuzyjne* – informowanie niejasne – polega na przekształceniu jednego oryginału w kilka obrazów, z których jeden z nich jest rezultatem kilku oryginałów, co może skutkować pomyleniem oryginału z obrazem.

Dezinformowanie polegające na tworzeniu informacji fałszywej, ukierunkowane jest na celowe wprowadzanie w błąd. Wyróżnia się *dezinformowanie symulacyjne*, *dezinformowanie dysymulacyjne* i *dezinformowanie konfuzyjne*. *Dezinformowanie symulacyjne* – zmyślanie – polega na tworzeniu fałszywego obrazu, którego wzorem nie jest oryginał. W *dezinformowaniu dysymulacyjnym* – zatajaniu – transformacja oryginału w obraz jest wybiórcza, zawierająca tylko te elementy, które pasują twórcy przekazu. Z kolei *dezinformowanie konfuzyjne* – przekręcanie – ukierunkowane jest na przekształcaniu oryginału w obraz, dopasowanego do oczekiwań i percepcji otoczenia.

Ostatni element, *metainformowanie*, czyli informowanie o informowaniu, polega na sterowaniu, w którym liczy się szybkość przekazania informacji stronie przeciwnej. Przekaz ten może być zarówno wierny, pozorny, jak i fałszywy.

Wprowadzenie w procesy sterowania informacją pozwala przejść do głównych zagrożeń informacyjnych występujących w cyberprzestrzeni. Są nimi dezinformacja i propaganda.

1.3.1. Dezinformacja

Dezinformacja jest przeciwieństwem informacji i oznacza w swej istocie informację fałszywą, niezgodną z prawdą. Jest ona ukierunkowana na wprowadzanie w błąd jej odbiorcy, co zostało odzwierciedlone w jej encyklopedycznej i słownikowej definicji, mówiącej o tym, że jest to *wprowadzenie kogoś w błąd przez podanie mylących lub fałszywych informacji*[29]. Inne definicje postrzegają dezinformację także jako *proces polegający na celowym, błędnym informowaniu*[30] lub też jako *sytuację, w której brakuje rzetelnych informacji*[31].

Termin dezinformacja po raz pierwszy pojawił się w literaturze anglojęzycznej w 1926 roku w londyńskim miesięczniku *The Whitehall Gazette & St James's Review*[32]. Określenia tego użyto opisując działania sowieckich służb specjalnych. Rok później w piśmie *Siegodnia* wspomniano, że dezinformacja należy do głównych działań GPU (Państwowy Zarząd Polityczny przy Ludowym Komisariacie Spraw Wewnętrznych Rosyjskiej Federacyjnej Socjalistycznej Republiki Radzieckiej)[33].

Paradoksem dezinformacji jest to, że historia powstania samego terminu dezinformacja związana jest bezpośrednio z radziecką dezinformacją. W *Wielkiej Encyklopedii Radzieckiej* z 1952 roku, w definicji dezinformacji odniesiono się do jej *rzekomego* francuskiego pochodzenia

[28] Szerzej: M. Mazur, *Cybernetyka i charakter,* WSZiP im. Bogdana Jańskiego w Warszawie, Warszawa 1999, s. 127.

[29] https://sjp.pwn.pl/sjp/dezinformacja;2554971.html, [11.09.2019].
[30] A. Markowski, *Wielki słownik poprawnej polszczyzny*, Wydawnictwo PWN, Warszawa 2004, s. 172.
[31] S. Dubisz, *Uniwersalny słownik języka polskiego*, t. I, Wydawnictwo PWN, Warszawa 2003, s. 602
[32] The Embassies and Foreign Affairs, „The Whitehall Gazette & St James's Review", Londyn 1926, s. 8.
[33] J.J. Dziak, *Chekisty: A History of the KGB,* Lexington Books, Lexington 1987, s. 42.

i jej powszechnym stosowaniu przez kapitalistyczne media do, jak to określono, ogłupiania ludzi. Do dziś treści zawarte w omawianej definicji są powszechnie używane do identyfikowania pochodzenia dezinformacji[34].

Kolejnym ujęciem dezinformacji jest definicja podana przez Vladimira Volkoffa, który postrzega ją w dwóch ujęciach: *wąskim i szerokim. W wąskim tego słowa znaczeniu mieści się ona w połowie drogi między wprowadzeniem w błąd a wpływaniem. Podczas gdy wprowadzanie w błąd* [...] *jest czynnością jednorazową, związaną z konkretnym zadaniem, dopuszcza pewną amatorszczyznę, wykorzystuje najprzeróżniejsze środki i zmierza do wmówienia pewnych określonych rzeczy określonym osobom, dezinformacja jest prowadzona w sposób systematyczny, fachowy zawsze za pośrednictwem mass mediów i jest adresowana do opinii publicznej, a nie sztabów krajów – obiektów działań. I analogicznie: podczas gdy wpływanie przejawia się w działaniach pozornie niezorganizowanych, oportunistycznych, głównie ilościowych, dezinformacja stawia sobie za cel realizację konsekwentnego programu zmierzającego do zastąpienia w świadomości, a przede wszystkim podświadomości mas będących przedmiotem tych działań, poglądów uznanych za niekorzystne dla dezinformatora takimi, które uważa on za korzystne dla siebie*[35]. Znamienne jest to, że współcześnie zamiennie używane jest określenie dezinformacja i fakenews. Jest to błąd pojęciowy i zamienne używanie tych dwóch terminów należy uznać za nadużycie, nadinterpretację lub niewiedzę. Jeżeli zadaniem fakenews, kłamstwa, jest wprowadzenie w błąd na potrzeby chwili, bieżącej sytuacji, to dezinformacja jest zaplanowana, wdrożona systemowo, realizująca przyjęte cele.

Vladimir Volkoff wymienił także metody dezinformacji, takie jak[36]: odwrócenie faktów, negacja faktów, mieszanie prawdy i kłamstwa, rozmycie, kamuflaż, interpretacja, generalizacja, ilustracja, nierówna reprezentacja, równa reprezentacja.

Odwrócenie faktów polega na celowym działaniu dezinformatora ukierunkowanym na całkowitym zakłamaniu, zaprzeczeniu i zrzuceniu winy ze sprawcy na ofiarę. Klasyczny przykład tego typu dezinformacji związany był z niemieckim prowokacjami i zrzuceniem winy za wywołanie II wojny światowej na Polskę i Polaków, lub też stworzenie i permanentne stosowanie w przestrzeni publicznej określenia „polski obóz śmierci". Współcześnie ten typ propagandy, z uwagi na rozwój społeczeństwa informacyjnego i dostęp do technologii informacyjnych, jest rzadko stosowany.

Negacja faktów stosowana jest w przypadku, gdy opinia publiczna nie jest w stanie sprawdzić, jak było naprawdę. W tym przypadku dezinformator z premedytacją będzie wypierał prawdy i stosował kłamstwa, zaprzeczenia. Ten rodzaj propagandy może być stosowany do chwili ujawnienia rzeczywistości, zapoznania opinii publicznej z tym, jak było naprawdę. Niemniej jednak, z uwagi na fakt, że opinia publiczna nigdy nie będzie zaznajomiona ze wszystkim szczegółami i niuansami omawianej sprawy, do dalszego dezinformowania może być wykorzystywane *mieszanie prawdy i kłamstwa*. Najlepszym przykładem odwrócenia faktów, negacji tychże faktów i mieszaniem prawdy i kłamstwa jest przypadek zestrzelenia samolotu pasażerskiego na Ukrainie w 2014 roku. Rosja, wypierając się swojego udziału w zestrzeleniu samolotu, stosowała klasyczne techniki odwrócenia faktów (to nie my – to Ukraińcy), negacji faktów (tam nie było naszych żołnierzy, a zestrzelenia dokonał samolot ukraiński) i mieszania prawdy i kłamstwa (śledztwo nie jest obiektywne – dopuśćcie naszych śledczych do wyników śledztwa). Uwagę należy zwrócić na skuteczność tychże działań.

Rozmycie jest techniką dezinformacji polegającą na odwróceniu uwagi audytorium od istoty sprawy, poprzez jej ukierunkowanie na szereg nieistotnych, nic nieznaczących informacji. Szczegółowym rodzajem rozmycia jest *kamuflaż*, polegający na drobiazgowym rozpisywaniu się na temat zaistniałej sytuacji w celu odwrócenia uwagi od jej istoty, zasadniczego problemu. W przypadku, kiedy faktom i zdarzeniom nie da się już zaprzeczyć, stosowana jest *interpretacja* polegająca na takim doborze słów, aby wywołać odpowiednie nastawienie odbiorcy informacji, sprzyjające dezinformatorowi, agentowi wpływu.

Generalizacja jest techniką dezinformacji polegającą na odniesieniu jednego zidentyfikowanego przypadku na całe środowisko. Jest to technika powszechnie stosowana w polityce i życiu społecznym i ma wiele wspólnego z technikami wskazywania wroga i doczepiania ogólników wykorzystywanych w propagandzie. Przykładem generalizacji jest uznanie Polaków za antysemitów na podstawie jednostkowych przypadków antysemityzmu. Bezpośrednio z generalizacją jest związana technika *ilustracji*, polegająca na wykorzystaniu zaistniałego, jednostkowego faktu do zilustrowania szerszego zjawiska występującego w danej grupie, społeczeństwie.

Nierówna interpretacja stosowana jest wtedy, gdy faktom niekorzystnym dla dezinformatora poświęca się bardzo mało miejsca na rzecz faktów mu sprzyjających, ukazujących w korzystnym świetle. Najczęściej metoda ta stosowana jest w polityce do manipulacji percepcją wyborców. Z kolei *równa interpretacja* stanowi najczęściej ostatni etap kampanii informacyjnej ukierunkowanej na uwiarygodnienie dezinformatora

[34] Szerzej: I. M. Pacepa, R. J. Rychlak, *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu*, Helion, Gliwice 2013, s. 53-54.
[35] V. Volkoff, *Psychosocjotechnika*, *dezinformacja oręż wojny*, Antyk, Warszawa 1999, s. 8.
[36] Ibidem, s. 157–172.

i utrwalenie jego pozycji w dezinformowanej grupie społecznej. Poglądy dezinformatora przedstawiane są jako wiarygodne i atrakcyjne, poparte opiniami ekspertów, w przeciwieństwie do poglądów rywala, który jest krytykowany i wyśmiewany przez pseudoekspertów.

Techniki te stosowane są we wszelkiego rodzaju manipulacjach informacyjnych oraz kampaniach dezinformacyjnych i nie wyczerpują całego arsenału metod i narzędzi dezinformacji.

Początków dezinformacji można dopatrywać się daleko wstecz, w najstarszych rozwiniętych cywilizacjach czy też początkach zorganizowanych konfliktów zbrojnych. Przykładem mogą być myśli Sun Tzu, który uważał, że *wojna jest to wprowadzanie w błąd. Jeśli zatem jesteś zdolny, udawaj mało zdolnego. Gdy porywasz swoje wojska do działania, udawaj bierność. Jeżeli twój cel jest bliski, zachowuj się tak, jakby był odległy. A gdy jest odległy, udawaj, że jest bliski*[37]. W każdej wojnie niezbędnym, kluczowym elementem jest umiejętność i zdolność wprowadzania przeciwnika w błąd, poprzez podawanie fałszywych informacji i tworzenia na ich podstawie fałszywego obrazu rzeczywistości. Dezinformacja jest zjawiskiem ponadczasowym, bardzo mocno zapisanym w naszej przeszłości, teraźniejszości i przyszłości. Można stwierdzić, że jest naturalnym elementem stosunków społecznych.

Dezinformacja może mieć wymiar taktyczny i strategiczny. Ta pierwsza trwa krótko, kilka miesięcy, a jej główny cel jest ukierunkowany na wprowadzanie w błąd w jednej lub kilku powiązanych ze sobą kwestiach. Przykładami tego rodzaju dezinformacji mogą być:

- podsunięcie fałszywych danych nowego rodzaju uzbrojenia;
- zmodyfikowanie danych statystycznych w celu wywołania opinii, iż stan gospodarki danego państwa jest lepszy lub gorszy od rzeczywistego;
- opublikowanie sfałszowanych materiałów kompromitujących polityka, partię lub też rząd.

Dezinformacja strategiczna polega na systematycznym i długotrwałym przekazywaniu sfabrykowanej informacji oraz fałszywych sygnałów politycznych, których głównym celem jest wytworzenie wypaczonego obrazu rzeczywistości, powodującego błędną ocenę sytuacji. To działanie ukierunkowane na wprowadzenie w błąd przeciwnika (rywala, oponenta, adwersarza) co do podstawowych kwestii polityki państwa[38].

W przeciwieństwie do dezinformacji taktycznej, może ona trwać nawet kilkadziesiąt lat i należy do sfery działalności służb specjalnych. Przykłady dezinformacji strategicznej można znaleźć w książce Roya Godsona i Jamesa J. Wirtza *Stategic denial and deception*[39].

Przykładem kompleksowego dezinformowania jest teoria opracowana przez rosyjskiego psychologa i matematyka Władimira Lefewra, zwana najczęściej jako *zarządzanie refleksyjne*[40]*(ang. reflexive control)*. Metoda ta polega na tworzeniu specyficznego modelu obiektu podlegającemu sterowaniu. Obiekt ten (osoba, grupa osób) tworzy w swojej świadomości nie tylko własny obraz świata, ale również posiada zdolności do analizowania własnych myśli i wyobrażeń[41]. Według Lefewra zarządzanie refleksyjne to *podstępne, iluzoryczne działania oparte na prowokacji, intrygach i kamuflażu, wykorzystywanych do sterowania obrazami świata w świadomości podmiotu poznającego*[42].

Metody stosowane w oparciu o teorię zarządzania refleksyjnego mogą doprowadzić do masowych zmian w nastawieniu społeczeństwa. Do najważniejszych metod zalicza się[43]:

- metoda nacisków siłowych poprzez demonstrowanie siły militarnej, tworzenie sojuszy wojskowych, wsparcie dla wewnętrznych sił antyrządowych;
- metoda wywierania wpływu na podejmowanie decyzji przez przeciwnika, publikacja fałszywych doktryn, strategii, planów, zamiarów;
- metoda kreowania i przekazywania fałszywych informacji o aktualnej sytuacji;
- metoda wpływania na czas decyzji przeciwnika poprzez eskalację nieprzewidywanych działań zbrojnych.

Krajem, w którym dezinformacja stanowiła istotne narzędzie polityki państwa był Związek Radziecki, co było podyktowane przyjętą polityką konfrontacji z zachodem i szerzeniem koncepcji oblężonej twierdzy. Dezinformacja w wydaniu radzieckim przyjęła formę planowych, kompleksowych i skoordynowanych kampanii, będących częścią przedsięwzięć

[37] Sun Tzu, *Sztuka wojny,* Wydawnictwo Przedświt, Warszawa 1994, s. 61.
[38] S. Lewczenko*, Private Channel* [w:] *Influence: A KGB Disinformation Tool, Counterpoint: A monthly report on Soviet Active Measures*, t. 3, kwiecień 1988 nr 11, s. 1.
[39] R. Godston, J.J. Wirtz, *Strategic denial and decption: the twenty-first century challenge*, National Strategy-Information Center, Washington, D.C. 2012.
[40] Patrz: M. Wojnowski, *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI wieku*, Przegląd Bezpieczeństwa Wewnętrznego nr 12/15.
[41] T. Aleksandrowicz, *Podstawy walki informacyjnej,* Editions Spotkania, Warszawa 2016, s.163.
[42] A. Kuzior, A. Kwiliński, *Zarządzanie refleksyjne – prolegomena*, https://www.researchgate.net/publication/353352807_Zarzadzanie_refleksyjne_-_prolegomena_A_Kuzior_A_Kwilinski, [7.02.2022].
[43] T. Aleksandrowicz, *Podstawy walki informacyjnej … op. cit.*, s. 164-165.

realizowanych w ramach tak zwanych *aktywnych środków* (*ang. active measures)*. Szacuje się, że na realizację działań związanych z dezinformacją Związek Radziecki wydał od 3 do 4 mld USD, a w realizację przedsięwzięć z tym związanych było zaangażowanych około 15000 osób.[44] W opinii Richarda Shultza i Raya Godsona w realizację przedsięwzięć w ramach *active measures* zaangażowane były dwa departamenty Komitetu Centralnego Komunistycznej Partii Związku Radzieckiego: Departament Informacji Międzynarodowej i Departament Międzynarodowy, oraz Zarząd A, stanowiący element I Dyrektoriatu KGB[45]. Zdobyte doświadczenia są współcześnie wykorzystywane przez Rosję i są podporządkowane realizacji interesów narodowych Federacji Rosyjskiej.

Dezinformacja może mieć różnorodne formy i być realizowana według odmiennych planów, w różnym czasie podyktowanym przyjętym celem działania. Niemniej jednak zasadniczym celem jest oszustwo, wprowadzenie w błąd odbiorcy informacji co do faktycznych zamiarów i planów dezinformatora. Na rysunku 1.8. przedstawiono przykłady reklam dezinformujących klientów sektora finansów. Podobnych przykładów dezinformacji można znaleźć dużo więcej. Często są one powiązane z artykułami, w których wypowiadają się „eksperci" na temat świetlanej przyszłości potencjalnych klientów, jak w przypadku afery GetBack. Przypadek ten dotyczy także afery Berniego Madoffa, mistrza manipulacji i oszusta, skazanego na 150 lat więzienia za zdefraudowanie 170 miliardów dolarów[46].

Współcześnie cyberprzestrzeń stała się doskonałym środowiskiem do szerzenia dezinformacji.

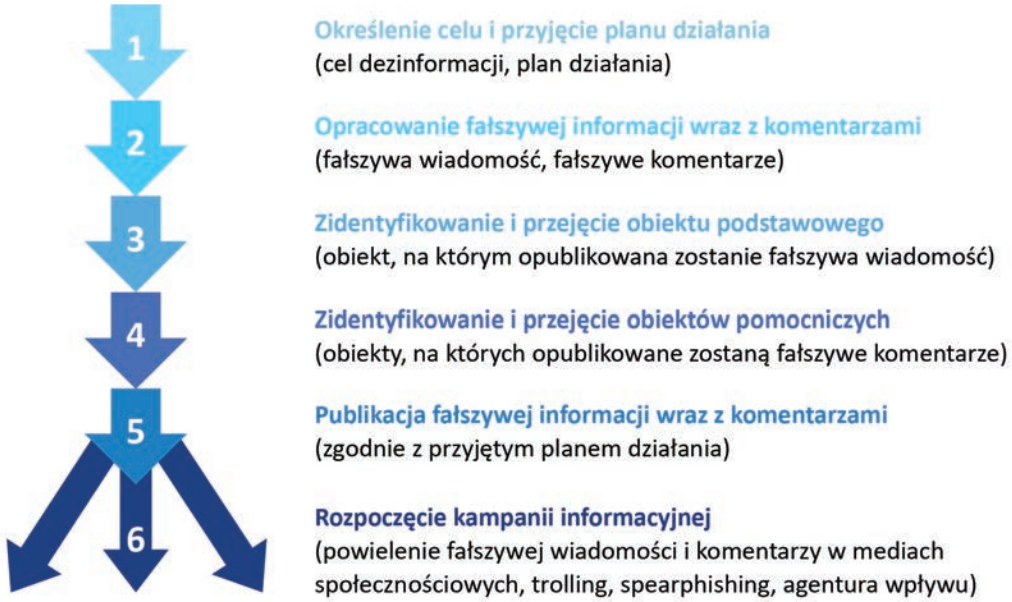
W procesie dezinformacji szerzonej w cyberprzestrzeni można wyróżnić: określenie celu dezinformacji i planu jej przeprowadzenia, przygotowanie fałszywej informacji wraz z komentarzami, zidentyfikowanie i przejęcie obiektu użytego do dezinformacji, zidentyfikowanie i przejęcie obiektów pośrednich dla zwiększenia zasięgu oddziaływania, publikacja fałszywej informacji wraz z komentarzami, rozpoczęcie kampanii informacyjnej w portalach społecznościowych związanej z powielaniem treści umieszczonych w obiektach pośrednich, wzmocnienie przekazu

Rysunek 1.8. Przykład reklamy dezinformującej klientów sektora finansów.
Źródło: https://www.ikalkulator.pl/blog/bezpieczna-kasa-oszczednosci-pierwsza-duza-afera-finansowa-iii-rp/ [7.02.2022]; https://subiektywnieofinansach.pl/awantura-o-uokik-czy-reklamy-amber-gold-rzeczywiscie-byly-takie-rzetelne/ [7.02.2022].

[44] M. Ajir, B. Vailliant, *Russian Information Warfare: Implications for Deterrence Theory,* [w:] Strategic Studies Quarterly, Fall 2018, *s. 72*, https://www.jstor.org/stable/26481910?seq=1#metadata_info_tab_contents, [15.12.2020]

[45] R.H. Shultz, R. Godson: *Dezinformatsia. Active Measures in Soviet Strategy*, Pergamon Press, Nowy Jork 1984, s. 20.

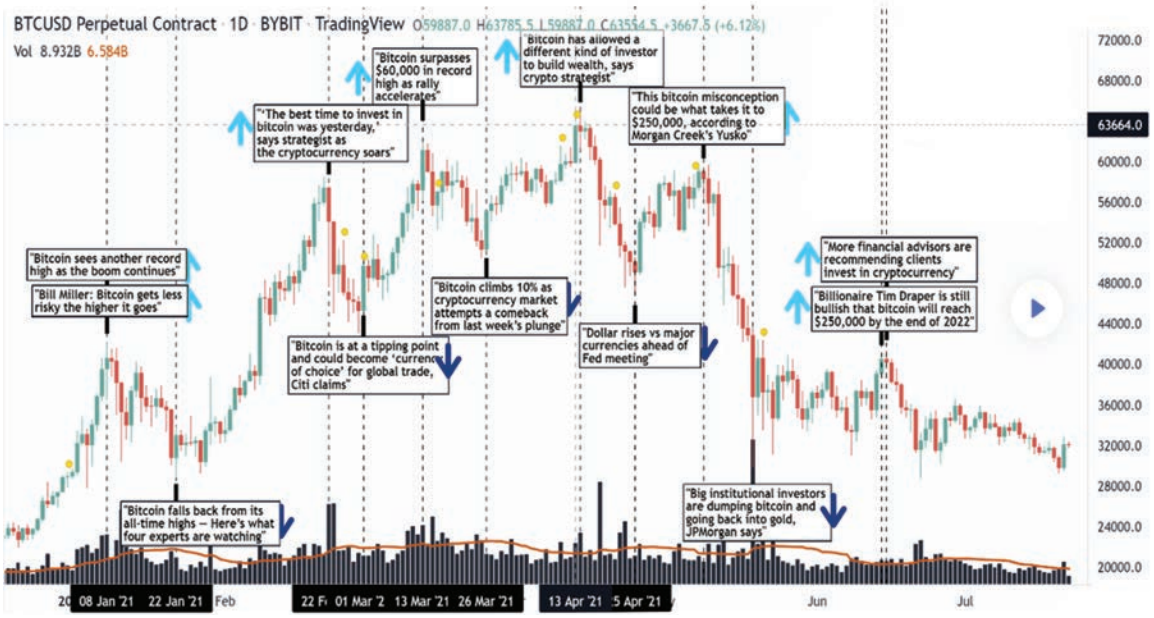
[46] https://www.investopedia.com/terms/b/bernard-madoff.asp, [7.02.2022].



Rysunek 1.9. Etapy dezinformacji realizowanej w cyberprzestrzeni.
Opracowanie własne.

poprzez rozsyłanie maili z przejętych kont pocztowych osób, które mają uwiarygodnić przekaz. Etapy dezinformacji zaprezentowano na rysunku 1.9.

Podsumowując, dezinformacja jest zaplanowanym przekazem informacyjnym realizującym przyjęte cele taktyczne (krótka perspektywa) lub strategiczne (długa perspektywa). Ten drugi przypadek – dezinformacja strategiczna – jest niezmiernie trudny do zidentyfikowania i wymaga odniesienia czasowego, pozwalającego na zidentyfikowanie w przeszłości sterowanych przekazów informacyjnych, specyficznych dla danego środowiska. Dezinformacja taktyczna może być wspierana fałszywymi informacjami, fakenewsami łatwymi do zidentyfikowania w krótkiej perspektywie czasowej. Niemniej jednak pozwala ona na sterowanie zachowaniami odbiorców informacji, szczególnie w środowisku podatnym na insynuacje, jak np. w przypadku kryptowalut. Na rysunku 1.10. przedstawiono wpływ przekazów informacyjnych na



Rysunek 1.10. Wpływ informacji na kurs kryptowaluty bitcoin.
Źródło: https://www.tradingview.com/chart/BTCUSD/w2FpasSV-Bitcoin-Mainstream-Media-Disinformation-Campaigns/, [8.02.2022].

kurs bitcoina. Przykładem siły oddziaływania pojedynczej wypowiedzi jest wpływ oświadczeń Elona Muska na kurs bitcoina[47].

1.3.2. Propaganda

Zagrożeniem informacyjnym bezpośrednio związanym z potrzebą wpływania rządzących na społeczeństwo jest *propaganda*. Z pierwszymi przypadkami tego typu działań mamy do czynienia już w kulturze mezoamerykańskiej i egipskiej, gdzie zapisy hieroglificzne, składające się z symboli i obrazów, przedstawiały historię w sposób korzystny dla ich twórcy, najczęściej dla władzy lub kapłanów. Było to możliwe, ponieważ jedynie władcy oraz kapłani posiadali umiejętność tworzenia hieroglifów, przez co przekaz był jednokierunkowy, skierowany od władzy do ludu. Pierwsze zapisy związane z określeniem terminu *propaganda* pochodzą z roku 1622, kiedy to Papież Grzegorz XV powołał Kongregację Propagandy Wiary (*łac. Congregatio de Propaganda Fide*). Do powszechnego obiegu termin ten wszedł w okresie pierwszej wojny światowej, jako nowa technika perswazji i oddziaływania na społeczeństwo[48]. Propagandę najczęściej postrzegano jako rozprzestrzenianie stronniczych idei i poglądów, często używając przy tym podstępu, kłamstwa czy też manipulacji. Największy swój rozwój propaganda zanotowała wraz z ekspansją systemów totalitarnych takich jak faszyzm i komunizm. Od tego momentu termin *propaganda* obejmował również swoim zakresem sugestię i wywieranie wpływu, przy użyciu manipulacji symbolami i mechanizmami psychologicznymi.

Propaganda obejmuje również swoim zasięgiem posługiwanie się obrazami, sloganami, stereotypami, uprzedzeniami i emocjami. Jest to swoisty komunikat stworzony na potrzeby z góry określonego celu, mający skłonić odbiorcę tegoż komunikatu do dobrowolnego przyjęcia punktu widzenia zawartego w komunikacie i uznania go za swój[49].

Współcześnie propaganda jest definiowana jako *proces składający się z planowanego użycia każdej formy publicznych lub masowo wytwarzanych komunikatów zaprojektowanych tak, aby wpływały na umysły i emocje wybranej grupy odbiorców, w z góry określonym celu (społecznym, militarnym, ekonomicznym, politycznym)*[50]. Kluczowymi elementami propagandy w tym ujęciu są plany działania i cele, do jakich w ramach tych planów się podąża. Bez opracowanego planu i określonego celu działania nie można mówić o propagandzie, lecz jedynie o kłamstwie lub manipulacji. Nie każde kłamstwo i manipulacja (fakenews) pojawiające się w przestrzeni informacyjnej są propagandą, ale każda kampania propagandowa jest oparta na kłamstwach i manipulacji.

Propaganda realizowana jest według schematu składającego się z pięciu podstawowych etapów określanych jako STASM, od pierwszych liter ich angielskich nazw. Zostały one zidentyfikowane przez Paula M.A. Linebargera w książce *Psychological warfare*, w postaci[51]:

- S *Source* (źródła – kanały informacyjne propagandy);
- T *Time* (czas rozpoczęcia i prowadzenia kampanii propagandowej);
- A *Audience* (publiczność – odbiorcy propagandy);
- S *Subject* (temat – sprawa, której dotyka kampania propagandowa);
- M *Mission* (misja – cel kampanii propagandowej powiązany z celem politycznym).

Pierwszy element dotyczy *kanałów informacyjnych*, za pomocą których prowadzona będzie kampania propagandowa. Współcześnie są to: prasa, telewizja, ulotki, Internet, wiece, bezpośrednie spotkania, fałszywe autorytety, agenci wpływu, celebryci, influencerzy itp. *Czas* jest związany z tym, kiedy i jak długo będzie prowadzona kampania propagandowa. Jego precyzyjne określenie jest niezwykle istotne. Łatwiej jest wpływać na społeczeństwo będące w kryzysie, stojące przed wyzwaniami lub wyborami, jednocześnie nie dając przeciwnikom czasu na stosowną reakcję. Czas jest kluczowym czynnikiem w kampaniach informacyjnych związanych z wyborami. Dobór czasu jest także podyktowany percepcją grupy docelowej i budowaniem w tej grupie odpowiednich przekonań, poglądów, nastroju sprzyjającego propagandyście. *Publika*, będąca grupą docelową kampanii propagandowej, charakteryzuje się swoimi systemami wartości, przekonaniami, nawykami, kulturą, tradycjami i środowiskiem informacyjnym, z którego pozyskuje wiedzę na temat otaczającej rzeczywistości. Dlatego też, uwzględniając powyższe, inny przekaz będzie kierowany do ludzi wykształconych, świadomie

[47] https://www.thesun.co.uk/tech/17574335/tesla-reveals-secret-bitcoin-stash-worth-2billion-elon-musk/, [8.02.2022]; https://www.theguardian.com/technology/2021/may/12/elon-musk-tesla-bitcoin, [8.02.2022].
[48] E. Aronson, A. Pratkanis, *Wiek propagandy*, Państwowe Wydawnictwo Naukowe, Warszawa 2004, s. 17.
[49] A. Chorobiński, *Walka informacyjna jako fundamentalny składnik działalności terrorystycznej w przyszłości*, s. 4; http://konkursy.byd.pl/userfiles/files/chorobinski.pdf, [11.09.2019].
[50] P.M.A. Linebarger, *Psychological warfare*, Combat Forces Press, Washington D.C. 1954, Second Edition Reprinted by Combat Forces Press, Washington, D.C. 1972, s. 61
[51] Ibidem, s. 67.

korzystających ze sprawdzonych źródeł informacji, inny z kolei do osób budujących swoje poglądy na świat na podstawie mediów społecznościowych czy też ulubionych kanałów informacyjnych. *Temat propagandy* jest bezpośrednio związany z oczekiwaniami wybranej grupy docelowej (*publiczności*), niejako rozwiązujący stojące przed nią problemy lub trafiający w ich oczekiwania i upodobania. Ostatnim – a zarazem najważniejszym elementem jest *cel*, dla którego realizowana jest kampania propagandowa. To podstawowy element, jaki powinien zostać określony już na początku planowania kampanii propagandowej. Na rysunku 1.11. przedstawiono proces organizowania kampanii propagandowej.

Rysunek 1.11. Proces tworzenia kampanii propagandowej
Opracowanie własne.

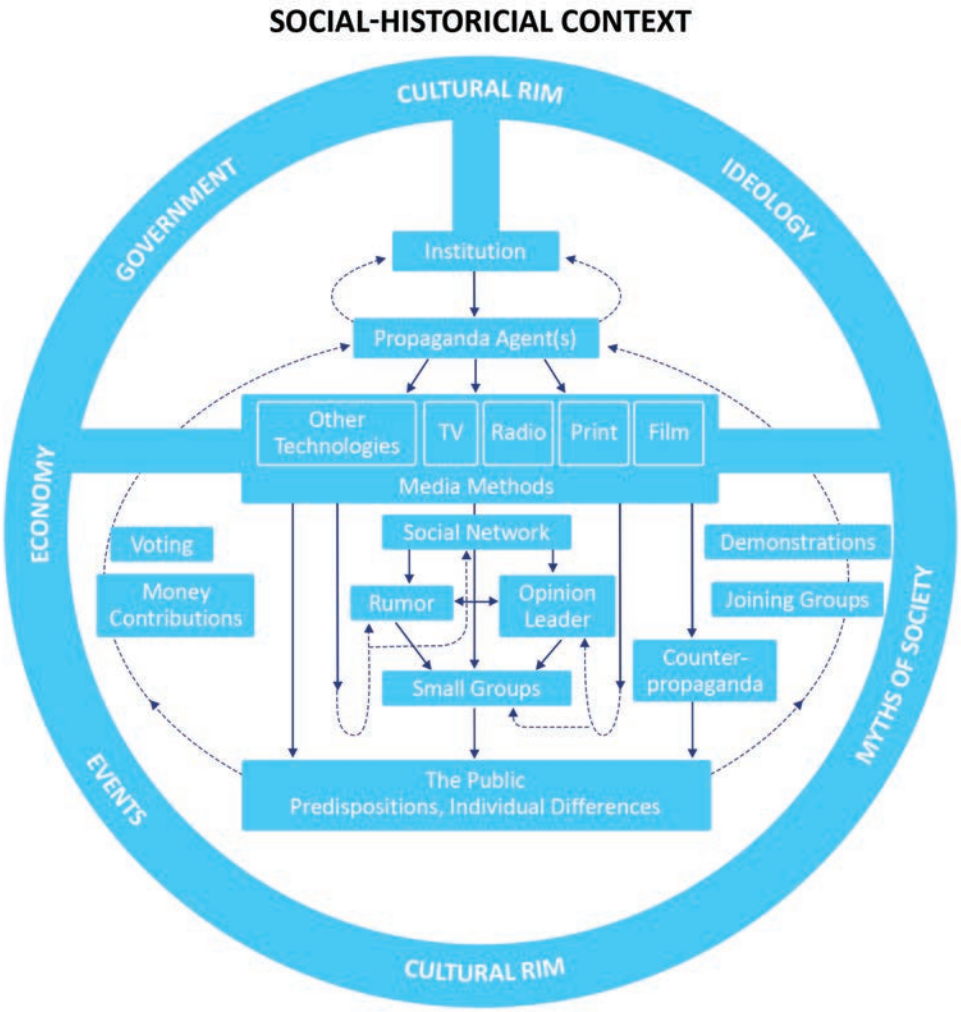
Patrząc przez pryzmat współczesnego społeczeństwa i środowiska informacyjnego, w którym ono funkcjonuje, można stwierdzić, że proces propagandy jest uwarunkowany wieloma czynnikami, takimi jak: aktywność propagandystów, media społecznego przekazu, dostęp do sieci Internet (w tym do mediów społecznościowych), organizacje rządowe i pozarządowe, grupy społeczne, systemy wartości, kultura, tradycje, systemy ekonomiczne, prawne i polityczne. Komunikaty wysyłane w propagandzie funkcjonują w szeroko postrzeganej obręczy kulturowej (ang. *cultural rim*), która jest determinowana kontekstem społeczno-historycznym (ang. *social-historical context*). Z tego względu nie można rozpatrywać propagandy w oderwaniu od uwarunkowań danego społeczeństwa. Funkcjonuje ono bowiem opierając się na swoich systemach wartości, kulturze, doświadczeniach, przekonaniach i historii. Propaganda, uwzględniająca powyższe aspekty, ma wpływ na kształt kultury, ale także kultura oddziałuje na kształt propagandy.

Na rysunku 1.12. przedstawiono uwarunkowania współczesnej propagandy, w którym uwidoczniono ścisłe powiązanie procesu propagandy ze społeczeństwem, na które jest ona ukierunkowana, zwłaszcza z jego społecznymi, historycznymi i kulturowymi uwarunkowaniami. Propagandyści w swoim przekazie uwzględniają (powinni uwzględnić) wszystkie aspekty dziedzictwa narodowego społeczeństwa, mające swoje odzwierciedlenie w stylu, sposobie i narracji przekazu. Tym samym identyfikowanie kampanii propagandowych wymaga uwzględnienia kontekstu społecznego, historycznego i kulturowego społeczeństwa, w którym była ona prowadzona.

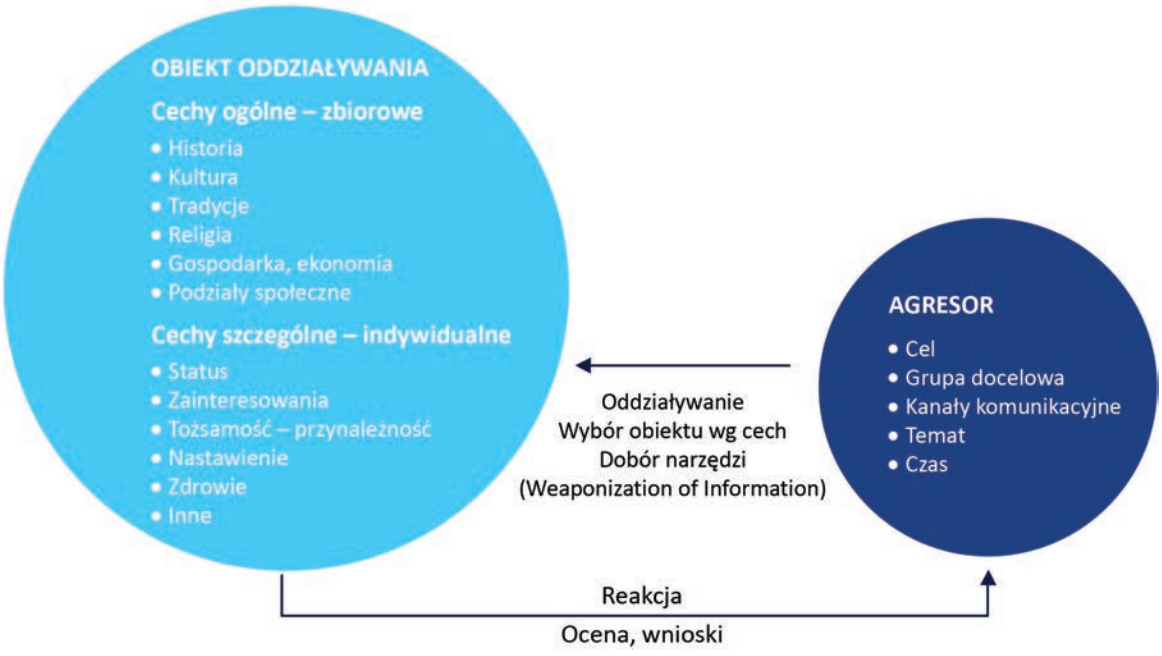
Propaganda najczęściej ukierunkowana jest w konkretną grupę społeczną, co wymusza uwzględnienie wielu innych czynników związanych z cechami tej grupy, takimi jak: zamożność, status społeczny, wykształcenie, zainteresowania, nastawienie, przynależność. Elementy propagandy celowanej przedstawiono na rysunku 1.13.

Kolejnymi aspektami propagandy wymagającym zidentyfikowania są jej źródło oraz stopień prawdziwości czy też zakłamania. Wyróżnia się trzy podstawowe rodzaje propagandy[52]: białą (ang. *overt or white*

[52] G.S. Jowert, V. O'Donnell, *Propaganda and persuasion*, Sage Publications, Washington D.C. 2006, s. 17.



Rysunek 1.12. Uwarunkowania współczesnej propagandy
Źródło: G.S. Jowert, V. O'Donnell, Propaganda and persuasion, Sage Publications, Washington D.C. 2006, s. 361.



Rysunek 1.13. Elementy propagandy celowanej
Opracowanie własne.

propaganda), szarą (ang. *gray propaganda*) i czarną (ang. *covert or black propaganda*). Pierwsza z nich, biała, to działania, w których zarówno źródło, jak i pochodzenie informacji są znane odbiorcom. To nic innego jak przekazanie oficjalnego stanowiska rządu, agencji rządowej czy też każdej innej organizacji w sposób jawny, przy założeniu, że przekazywane w nich informacje są podawane w sposób wybiórczy, z uwypukleniem sprzyjających stronie przekazującej i jednoczesnym pomijaniem faktów niewygodnych. W wypadku propagandy szarej źródło informacji nie jest znane, można jedynie domyślać się jego pochodzenia, zaś przekazywana w jej ramach informacja jest korzystna bądź też niekorzystna dla określonej grupy odbiorców, uwarunkowana celem działania propagandysty. Informacje są podawane w taki sposób, aby nosiły znamiona wycieku informacji, często w postaci nieoficjalnego stanowiska rządu czy też organizacji. Ostatni rodzaj propagandy – czarnej – jest z założenia budowany na manipulacji, kłamstwie i fałszu. Zarówno źródło informacji, jak i sama informacja są fałszywe. Celem tego typu działań jest uzyskanie w docelowej grupie odbiorców odpowiedniego efektu psychologicznego, polegającego na całkowitej zmianie postrzegania bieżącej sytuacji politycznej, społecznej, ekonomicznej, militarnej itp. Współcześnie czarna propaganda jest narzędziem powszechnie wykorzystywanym, chociażby przy okazji wyborów, referendów i innych ważnych dla danego społeczeństwa sytuacji, a środowiskiem jej rozprzestrzeniania jest cyberprzestrzeń.

Podobnie jak w przypadku omawianej wcześniej dezinformacji, także w odniesieniu do propagandy można wyróżnić dwie zasadnicze kategorie: propagandę taktyczną i strategiczną[53]. Są one związane z okresem ich prowadzenia i przyjętymi celami oddziaływania. Najczęściej formy te są wykorzystywane w trakcie operacji militarnych, ale ostatnio także w konfliktach hybrydowych. Propaganda taktyczna jest ukierunkowana bezpośrednio do wybranej grupy odbiorców, na przykład żołnierzy biorących udział w walce (operacji), celem wywarcia na nich odpowiedniego wrażenia, przekonania do własnych poglądów, zdemoralizowania i zdemotywowania do jakiegokolwiek działania czy też poświęceń. Jej oddziaływanie w czasie jest bezpośrednio związane z czasem prowadzenia operacji militarnej. Propaganda taktyczna związana może być z wywołaniem w społeczeństwie paniki ukierunkowanej na podejmowanie nieprzemyślanych działań np. wypłat gotówki z kont bankowych. Z kolei propaganda strategiczna jest ukierunkowana na osiągnięcie celów strategicznych, rozłożonych w długim przedziale czasu, sięgającym nawet kilkadziesiąt lat, a jej głównym celem jest zbudowanie nowej świadomości (nowego postrzegania otaczającej rzeczywistości) wśród grupy docelowej, zgodnej z przyjętym celem strategicznym.

W literaturze przedmiotu można znaleźć również inne rodzaje i formy propagandy. W zależności od rodzaju aktywności stron prowadzących kampanie propagandowe wyróżnia się[54] propagandę defensywną (ang. *defensive propaganda*) i ofensywną (ang. *offensive propaganda*). Pierwsza z nich jest wykorzystywana do wzmocnienia pozytywnego nastawienia społeczeństwa i akceptacji w stosunku do planów i przedsięwzięć realizowanych przez państwo. Drugi rodzaj propagandy – ofensywnej – jest stosowany w celu zmiany, niezgodnego z celami propagandystów, nastawienia społeczeństwa.

Z punktu widzenia celu kampanii propagandowej wyróżniamy propagandę[55]: konwersyjną *(*ang. *conversionary propaganda*), dzielącą (ang. *divisive propaganda*), scalającą (ang. *consolidation propaganda*) i przeciwpropagandę (ang. *counterpropaganda*). Głównym celem propagandy konwersyjnej jest konwersja, czyli zmiana świadomości, poglądów i lojalności jednostki w stosunku do danej grupy społecznej i ich przekierowanie na inną, pożądaną grupę społeczną. Propaganda dzieląca jest ukierunkowana na rozbicie jedności wybranej grupy społecznej (społeczeństwa). Chodzi w niej o stworzenie w grupie docelowej podziałów, a tym samym zmniejszenie jej siły oddziaływania. Odmienne cele charakteryzują propagandę scalającą, której głównym zadaniem jest likwidacja wszystkich podziałów i zjednoczenie społeczeństwa wokół wspólnej sprawy, wspólnych wartości. Z kolei przeciwpropaganda jest nastawiona na osłabienie lub też całkowite uniemożliwienie osiągnięcia celów propagandy stosowanej przez adwersarza.

Elementami propagandy są także *techniki,* za pomocą których jest ona prowadzona. Do najważniejszych z nich można zaliczyć[56]: zapewnienie (ang. *assertion*), owczy pęd (ang. *bandwagon*), naciąganie faktów (ang. *card stacking*), błyskotki (ang. *glittering generalities*), mniejsze zło (ang. *lesser of two evils*), doczepianie ogólników (ang. *name calling*), wskazywanie wroga (ang. *pinpointing the enemy*), ludowość (ang. *plain folks*), uproszczenie (*ang. simplification*), referencję (ang. *testimonials*), przenoszenie (ang. *transfer*).

Zapewnienie (*ang. assertion*) jest współczesną techniką propagandy powszechnie stosowaną

[53] P.M.A. Linebarger, *Psychological warfare…,* op. cit., s. 69.

[54] Ibidem, s. 70.

[55] Ibidem.

[56] Na podstawie materiałów uzyskanych przez autora w ramach przedmiotu *Foreign Propaganda, Perceptions, and Policy*, prowadzonego w semestrze jesiennym 2017 r. w The Institute of World Politics, Washington D.C.

w reklamie[57]. Przekazywane informacje mają entuzjastyczny, radosny, energiczny charakter, a treści w nich zawarte, niekoniecznie prawdziwe, odwołują się do przekonań i nastawienia odbiorców. Coś jest dobre, bo jest, bez żadnego odwoływania się do faktów. Za każdym razem, gdy reklamodawca stwierdzi, że jego produkt jest najlepszy, bez dostarczania naukowych dowodów, korzysta z techniki zapewnienia. Odbiorca informacji zgadza się z otrzymywanym przekazem bezrefleksyjnie, nie dążąc do ustalenia, jak jest naprawdę. Zapewnienie, choć dosyć łatwe do wykrycia, jest coraz częściej wykorzystywane w polityce do sterowania emocjami społecznymi, a narracja takiego przekazu jest, z natury rzeczy, budowana na fałszu i kłamstwie[58].

Owczy pęd (*ang. bandwagon*) jest jedną z najpowszechniejszych technik propagandy stosowaną zarówno w czasie pokoju, jak i wojny, i odgrywa bardzo ważną rolę we współczesnej inżynierii społecznej. Technika ta polega na apelowaniu do odbiorcy o podążanie za większością, która z pewnością ma rację. A skoro tak, to przyłączenie się do większości będzie tylko i wyłącznie z korzyścią dla jednostki. W propagandzie tego typu propagandysta zasadniczo stara się przekonać odbiorcę, że tylko jedna ze stron jest tą właściwą, ponieważ dołączyło się do niej więcej osób i z tego też względu tylko oni mają rację. Odbiorcy przekazów informacyjnych mają wierzyć, że skoro tak wielu ludzi dołączyło do większości, to zwycięstwo jest nieuniknione, a porażka niemożliwa. Przeciętny człowiek, zmuszony presją tłumu, zawsze chce być po zwycięskiej stronie. Przeciwdziałanie tej technice polega w głównej mierze na szczegółowym rozważeniu plusów i minusów przyłączania się do sugerowanej idei bez uwzględniania liczby osób, które już się do niej dołączyły[59].

Technika naciągania faktów (*ang. card stacking*) polega na przedstawianiu informacji w sposób wybiórczy, sprzyjający propagandystom, pomijając informacje dla nich negatywne. Technika ta, ze względu na swoją skuteczność, jest powszechnie stosowana w reklamie i polityce. Chociaż większość informacji przedstawionych przez propagandystę jest prawdziwa, to w przekazie pomija się to, co jest istotne dla sprawy i równocześnie niekorzystne dla propagandysty. Najlepszym sposobem radzenia sobie z naciąganiem faktów jest zdobycie informacji z różnorodnych źródeł[60].

Błyskotki (*ang. glittering generalities*) to technika wykorzystywana najczęściej w polityce, polegająca na używaniu słów mających pozytywne znaczenie dla poszczególnych odbiorców przekazu propagandowego, najczęściej bezpośrednio powiązane z systemem wartości obowiązującym w społeczeństwie. Użyte słownictwo jest przyjmowane bezrefleksyjnie, automatycznie, bez zastanowienia, tylko i wyłącznie dlatego, że dotyczy ważnego dla odbiorcy pojęcia. Słowa często używane w technice błyskotek to: bóg, honor, ojczyzna, wolność, niepodległość, suwerenność, miłość, demokracja. Głównym celem techniki jest zjednoczenie społeczeństwa wokół wspólnych wartości w chwilach trudnych i przełomowych. Niemniej jednak technika może być też nadużywana przez polityków na potrzeby walki politycznej i wygrania wyborów[61].

Technika mniejszego zła (*ang. lesser of two evils*) polega na przekonaniu odbiorców, że spośród wielu złych rozwiązań jedno z nich jest dobre (korzystne) i powinno być zaakceptowane przez społeczeństwo. Technika ta jest stosowana najczęściej w czasie wojny, w celu przekonania społeczeństwa o potrzebie poświęcenia i poniesienia niezbędnych ofiar. W czasie pokoju przekaz nie jest już taki jednoznaczny, a główny nacisk ukierunkowany jest na przekonanie społeczeństwa do przeprowadzenia niezbędnych, kosztownych społecznie reform, np. reformy emerytalnej, podatkowej lub walutowej. Winą za wszelkie trudy i wyrzeczenia związane z poświęceniem społeczeństwa obarczany jest wrogi kraj (w czasie wojny) lub wroga grupa polityczna (w czasie pokoju). Prezentowana idea jest przedstawiana jako jedyna opcja lub droga postępowania, którą należy wybrać, gdyż każde inne rozwiązanie jest złe.

Doczepianie ogólników (*ang. name calling*) występuje najczęściej w scenariuszach politycznych i wojennych, rzadko w reklamie. Polega na użyciu obraźliwego słownictwa, które niesie za sobą negatywną konotację przy opisie przeciwnika politycznego czy też militarnego. Propagandyści usiłują wzbudzić wśród opinii publicznej uprzedzenie do konkretnej grupy, nadając przeciwnikowi (oponentowi) taką nazwę, która źle się kojarzy społeczeństwu lub której nie lubi. Często nazwę taką nadaje się za pomocą sarkazmu i ośmieszania. Identyfikacja tej techniki polega w głównej mierze na oddzieleniu emocji od odbieranego przekazu informacyjnego.

Wskazywanie wroga (*ang. pinpointing the enemy*) jest techniką wykorzystywaną zarówno w czasie wojny, jak również w kampaniach politycznych i debatach społecznych. Jest to działanie ukierunkowane na przedstawienie osoby lub grupy jako wroga społecznego,

[57] Patrz rysunek 1.8.
[58] H. T. Conserva, *Propaganda Techniqes*, AuthorHouse, Bloomington 2003, s. 25-27.
[59] W. Garber *Propaganda Analysis—to what ends,* The American Journal of Sociology, Chicago 1942, s. 240.
[60] Ibidem s. 244.
[61] Ibidem s. 242

narodowego. Identyfikacja techniki polega na unikaniu postrzegania przekazu informacyjnego i kierowanych w nich oskarżeniach w kategoriach jednoznacznego dobra i zła.

Ludowość (*ang. plain folks*) to technika, która ma na celu przekonać opinię publiczną, że poglądy propagandysty odzwierciedlają poglądy zwykłego, prostego ludu i z tego względu działają na korzyść prostych ludzi. Propagandysta często stosuje akcent i charakterystyczne zwroty określonej grupy odbiorców, wspierając przekaz żartami, gestami i odpowiednim zachowaniem. Język użyty przez propagandystę, poprzez błędy wymowy, jąkanie się i ograniczone słownictwo, sugeruje jego szczerość i spontaniczność, tworząc iluzję niedoskonałości mówcy, swojskości. Technika ta występuje często w połączeniu z techniką błyskotek, przez co wzmacniany jest przekaz ukierunkowany na wspólne wartości. Najlepszym sposobem przeciwdziałania tej technice jest oddzielenie idei prezentowanych przez propagandystę od jego osobowości i wyuczonych technik wystąpień publicznych.

Uproszczenie (*ang. simplification*) jest w swej istocie zbieżne z techniką wskazywania wroga, z uwagi na częste dążenie do wyboru pomiędzy dobrem a złem. Technika ta jest wykorzystywana do manipulowania niewykształconymi odbiorcami, postrzegającymi świat przez pryzmat ulubionych kanałów informacyjnych, powielającymi otrzymane przekazy informacyjne w sposób bezrefleksyjny. Jest taka rzeczywistość, bo tak mówili w telewizji, tak wyczytałem w Internecie lub takie było kazanie. W walce z uproszczeniem niezbędne jest zbadanie innych występujących przekazów informacyjnych z różnorodnych kanałów komunikacyjnych[62].

Referencja (*ang. testionials*) to technika wykorzystywana najczęściej w czasie kampanii reklamowych i politycznych, polegająca na odniesieniu się do rekomendacji próbujących połączyć znaną lub szanowaną osobę z produktem, przedmiotem lub ideą. To odniesienie się do autorytetów (w tym pseudoautorytetów, takich jak celebryci, influencerzy, agenci wpływu) i przekonanie odbiorców, że jeżeli autorytet ma takie poglądy, to oni powinni mieć takie same, bez względu na fakty i okoliczności. Przeciwdziałanie tej technice polega na obiektywnej ocenie wszystkich wad i zalet przedmiotu, oferty, idei i wyciągnięcia bezstronnych wniosków, niepodyktowanych żadnymi względami subiektywnymi lub naciskami zewnętrznymi.

Ostatnią z wymienionych technik propagandy, stosowaną zarówno w polityce jak i podczas wojny, jest przenoszenie (*ang. transfer*). Technika ta polega na próbie stworzenia i przeniesienia autorytetu z jednej rzeczy (osoby, grupy społecznej) na inną rzecz (osobę, grupę społeczną), w celu uzyskania przychylności. Istotnego znaczenia w tym przypadku nabiera wykorzystanie symboli, które niosą za sobą konkretne znaczenie. Dlatego też politycy chętnie robią sobie zdjęcia na tle flagi narodowej, zyskując poparcie w propatriotycznej części społeczeństwa. W innym przypadku popierają palenie flag instytucji międzynarodowych np. Unii Europejskiej, zyskując poparcie wśród eurosceptyków i narodowców. To także robienie zdjęć z osobami będącymi autorytetami np. z papieżem. Technika transferu jest wykorzystywana w budowaniu negatywnego postrzegania organizacji poprzez doklejanie im łatek związanych z ideologią, która w danym społeczeństwie kojarzy się w sposób negatywny.

Skuteczna propaganda wymaga nieustannego wyciągania wniosków z przeszłości. Analiza historycznych przypadków kampanii propagandowych pozwala dostrzec, które z metod i narzędzi były skuteczne, w jakim środowisku społecznym propaganda była prowadzona, w jakim czasie i jakimi kanałami komunikacyjnymi odbywał się przekaz i co należy zmodyfikować, aby zmaksymalizować przekaz i tym samym skuteczność propagandy.

[62] H. T. Conserva, *Propaganda*..., op. cit., s. 74-76.

Cele realizowane w przekazach informacyjnych

Wskazanie celów realizowanych w oddziaływaniu informacyjnym wymaga zidentyfikowania, czym w swojej istocie jest cel działania i jakie podmioty go realizują. Zgodnie z zapisami słownikowymi, celem jest to, *do czego się dąży, co się chce osiągnąć*[63]. W prakseologii termin *cel* jest rozumiany jako zaplanowany lub zamierzony wynik każdego racjonalnego działania. Jest on wyznaczany przez podmiot działania i w zależności od przyjętego przez niego systemu wartości może być *stopniowalny* lub *niestopniowalny*[64]. W celu stopniowalnym określone są warunki jego osiągnięcia w kategoriach:

- ilości,
- jakości,
- miejsca,
- czasu.

Osiągnięcie lub nieosiągnięcie celu jest stopniowane według powyższych kategorii. Cel niestopniowalny oznacza, iż założono, że może być on, jako całość, osiągnięty lub nieosiągnięty, bez stanów pośrednich.

W definicjach celu bardzo często wymieniany jest podmiot działania, który w zależności od sposobu zorganizowania i jego umiejscowienia w systemie bezpieczeństwa jest postrzegany różnorodnie. Podmiotami realizującym cel mogą być zarówno poszczególni ludzie, społeczności, grupy formalne lub nieformalne, związki, stowarzyszenia, firmy, samorządy, służby, państwa, sojusze i inne niewymienione organizacje. Każda z nich ma swój system wartości, a tym samym swoje cele, które mogą być zarówno zbieżne, jak i całkowicie odmienne. Będą one pochodną rodzaju kooperacji, w której podmioty uczestniczą, ukierunkowanej na współdziałanie (cele zgodne, związane z zyskami) lub rywalizację i walkę (cele przeciwstawne, związane ze stratami).

W ujęciu Tadeusza Kotarbińskiego wyróżnia się kooperację pozytywną, identyfikowaną jako współpracę i kooperację negatywną, utożsamianą z walką. Podstawą takiej klasyfikacji jest zgodność (kooperacja pozytywna) lub niezgodność (kooperacja negatywna) celów działania podmiotów kooperujących. Z kolei Mirosław Sułek podzielił występujące kooperacje na trzy główne działy: współpracę, rywalizację i walkę[65]. Podstawą tego podejścia były formy stosunków międzyludzkich występujących w ekonomii. W tym ujęciu współpraca oznacza korzyści, jakie odnoszą wszystkie strony biorące udział w kooperacji. Mogą one mieć charakter zarówno materialny, jak i niematerialny, a najlepszym, najjaskrawszym przykładem współpracy jest rynek i wspominana już ekonomia[66]. W rywalizacji korzyści są postrzegane zgoła odmiennie. To, co najczęściej jest zyskiem dla jednej strony, jest równocześnie stratą dla strony drugiej, przy czym wartość zysku i straty jest tożsama. W wymiarze międzynarodowym przejawem rywalizacji jest dążenie państw lub innych podmiotów bezpieczeństwa do bycia potęgą światową i procentowy udział kooperantów w podziale zysków i stref wpływów. Jak podaje Mirosław Sułek, rywalizacja jest działalnością regulacyjną, zmierzającą do ustalenia proporcji pomiędzy współpracą a walką, a osią tej rywalizacji są stosunki sił[67].

Walka oznacza kooperację, w której wszystkie strony ponoszą czyste straty. Może być ona prowadzona w różnych sferach, na przykład na płaszczyźnie ekonomicznej, energetycznej, militarnej, informacyjnej czy chociażby ostatnio obserwowanej płaszczyźnie technologicznej. Logika takiego postępowania prowadzi do zwycięstwa najsilniejszego[68]. Mirosław Sułek zauważył, że współczesne stosunki międzynarodowe, ale także stosunki międzyludzkie i społeczne, są syntezą współpracy, rywalizacji i walki w różnych obszarach, z różnym nasileniem i zaangażowaniem. Nie można bowiem mówić tylko o absolutnej współpracy czy absolutnej walce[69].

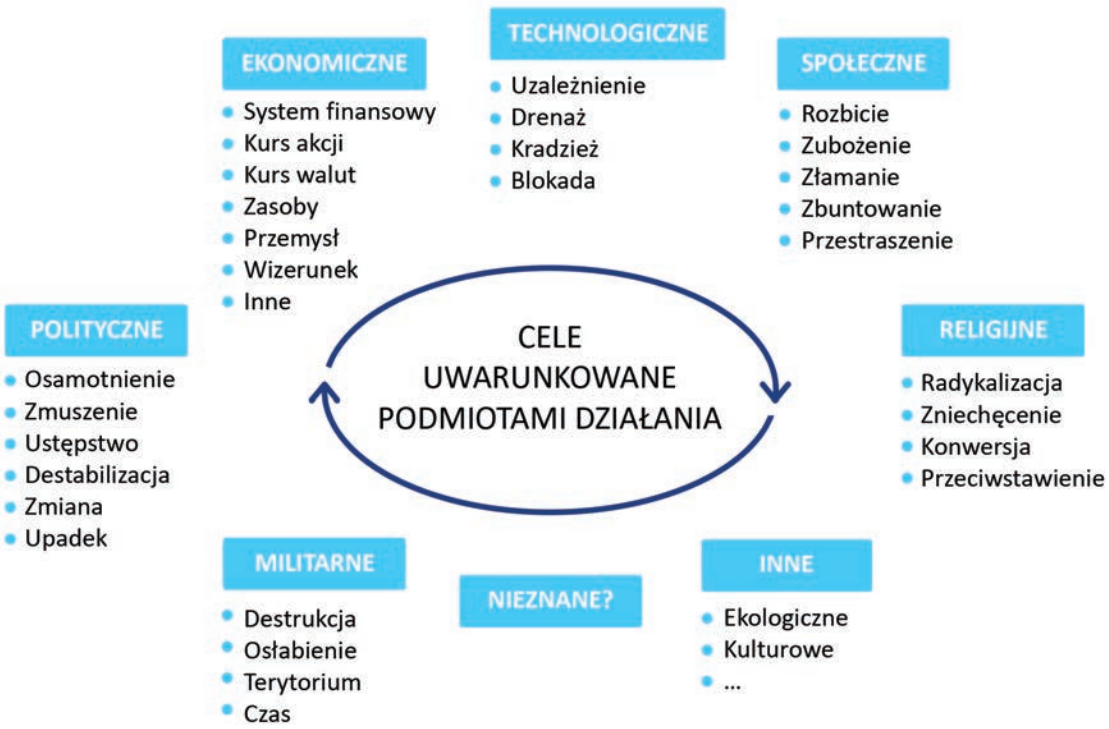
Cele wyznaczone przez podmioty rywalizujące i walczące mogą być różne, uwarunkowane możliwościami samych podmiotów i przyjętymi, tak jak wspomniano, systemami wartości. Dla podmiotu będącego państwem cele mogą wynikać z przyjętych strategii, doktryn i sposobów realizacji interesów narodowych. Większość państw prowadzi deklaratywną lub rzeczywistą defensywną politykę obronną, ukierunkowaną na zwiększenie bezpieczeństwa na drodze pokojowej poprzez rozbudowę potencjału obronnego, zawierania koalicji i sojuszy. Są też państwa, które realizują swoje cele, interesy narodowe na drodze agresywnej, poprzez rozwój zdolności ofensywnych, prowadzenie ofensywnych kampanii informacyjnych, destabilizację wybranych rejonów, generowanie podziałów, szantaż ekonomiczny, energetyczny, technologiczny czy też ostatecznie przez konflikt zbrojny. Do tego dochodzą różnorodne grupy interesów takich, jak separatyści, fundamentaliści, terroryści, lobbyści i thinktanki. Każda z tych grup może wyznaczać i realizować swoje cele, uwarunkowane posiadanym

[63] *Słownik języka polskiego*, t. I, Wydawnictwo Naukowe PWN, Warszawa 1993, s. 235.
[64] Por.: W. Bojarski, *Podstawy analizy i inżynierii systemów*, Państwowe Wydawnictwo Naukowe, Warszawa 1984, rozdz. 3.
[65] M. Sułek, *Trzy działy prakseologii*, „Rocznik Naukowy Wydziału Zarządzania w Ciechanowie Wyższej Szkoły Menadżerskiej w Warszawie", z. 12, t. II, Ciechanów 2008, s. 2, www.mises.pl, [11.09.2019].
[66] Ibidem.
[67] Ibidem, s. 3.
[68] Ibidem.
[69] Ibidem.

potencjałem. Uwagę powinno także skupić się na korporacjach międzynarodowych, szczególnie związanych z nowoczesnymi technologiami informacyjnymi. Ich zasoby ekonomiczne i informacyjne pozwalają na skuteczną rywalizację nawet z państwami, tym bardziej, że zawsze są wspierane przez rządy krajów będących ich głównym miejscem działalności. Tym samym stają się one podmiotami mogącymi skutecznie osiągać swoje cele ekonomiczne lub jakiekolwiek inne, poprzez generowanie podziałów, kreowanie trendów, unikanie opodatkowania, szkalowanie grup społecznych i partii politycznych, zarówno na poziomie lokalnym, jak również w skali globalnej. Ogólna klasyfikacja celów realizowanych w przekazach informacyjnych, ale także w rywalizacji i walce została przedstawiona na rysunku 2.1. Oczywiście klasyfikacja ta nie wyczerpuje zagadnienia ponieważ cele te, jak wcześniej wspominano, są pochodną podmiotu, który je realizuje, a tym samym niezwykle trudno jest wskazać wszystkie możliwe kierunki oddziaływania.

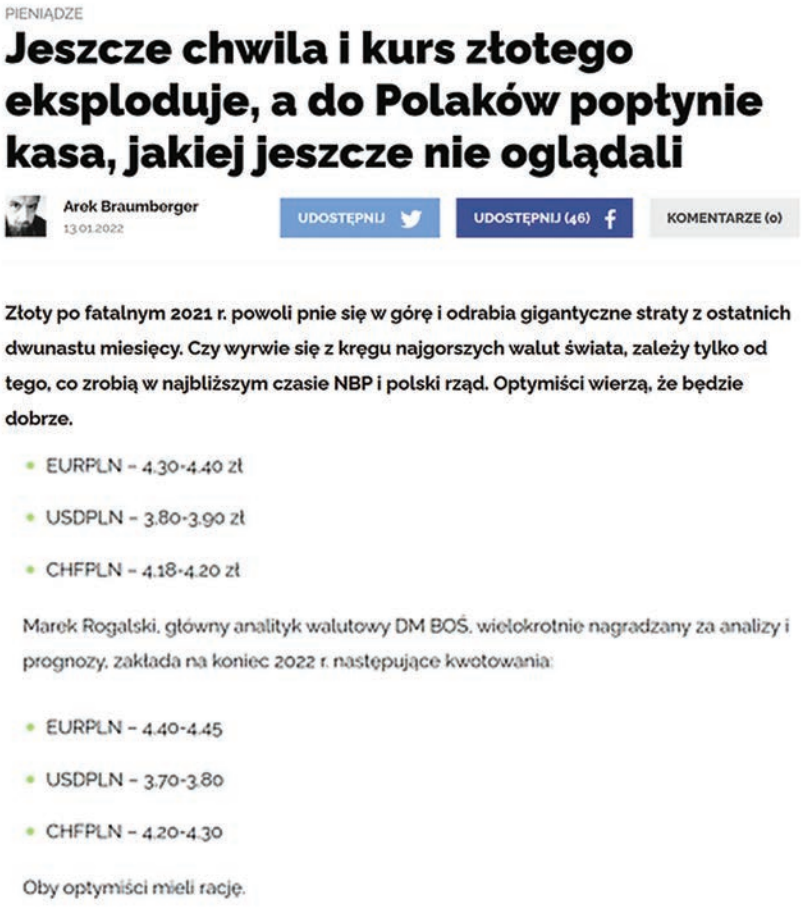
Przejdźmy zatem do sklasyfikowania celów wyznaczanych w kooperacji negatywnej. Na pierwszy plan wysuwa się *cel polityczny*, który jest pojmowany jako oczekiwany, pożądany efekt postępowania w sferze politycznej. To rezultat wzajemnych relacji (kooperacji pozytywnych, kooperacji negatywnych i rywalizacji) pomiędzy wszystkimi uczestnikami życia politycznego. Są nimi instytucje międzynarodowe, państwa, partie polityczne, społeczeństwa, elity, ośrodki władzy, formalne i nieformalne grupy nacisku. Działania związane z realizacją celów politycznych są ukierunkowane na wzmocnienie, utrzymanie lub osłabienie poszczególnych podmiotów biorących udział w polityce. W kooperacji negatywnej działania te zmierzają najczęściej do osamotnienia, zmuszenia, zdezawuowania, destabilizacji, zmiany i upadku.

Cele te są ukierunkowane na osłabienie lub wręcz zniszczenie podmiotu politycznego na drodze oddziaływania informacyjnego wspartego, w ramach efektu synergii działaniami, działaniami w innych obszarach np. blokadami ekonomicznymi, zerwaniem stosunków dyplomatycznych, sankcjami. Są one podyktowane własnymi interesami, przeciwstawnymi do interesów atakowanego podmiotu. Największe znaczenie odgrywa w tym wypadku dezinformacja i propaganda, ukierunkowane zarówno na obiekt oddziaływania (obiekt ataku), jak również na jego otoczenie (środowisko lokalne i międzynarodowe). Należy jednak pamiętać o tym, że mogą być wykorzystane także elementy oddziaływania informatycznego (cyberbroń) i kinetycznego (sabotaż, dywersja i skrytobójstwo), zgodnie z zasadą synergii, zespolenia działań ukierunkowanych na maksymalizację stopnia osiągnięcia przyjętych celów działania. Dla przykładu, droga do osiągnięcia celu, jakim jest zmiana lub upadek państwa, może być wielostopniowa i rozłożona w długim okresie. W pierwszej kolejności agresor będzie prowadził kampanie informacyjne ukierunkowane na społeczeństwo w celu jego



Rysunek 2.1. Cele realizowane w oddziaływaniu informacyjnym
Opracowanie własne.

skłócenia, wytworzenia coraz większych podziałów i budowania nastrojów niezadowolenia w stosunku do władzy i sytuacji międzynarodowej. Jednocześnie wśród społeczności międzynarodowej (regionalnej w otoczeniu państwa) będzie prowadzona kampania informacyjna ukierunkowana na osłabienie wizerunku atakowanego państwa i jego obywateli. Będą szerzone nieprawdziwe informacje na temat docelowego społeczeństwa, bazujące na stereotypach i uprzedzeniach. Faza takiego oddziaływania może trwać długie lata, do momentu, aż agresor uzna, że nadszedł odpowiedni czas do dalszej eskalacji, polegającej na wprowadzeniu elementów oddziaływania informatycznego i kinetycznego, kończąc na pełnowymiarowym konflikcie zbrojnym. Zniszczenie lub czasowe obezwładnienie kluczowych elementów infrastruktury krytycznej w połączeniu z oddziaływaniem kinetycznym, na przykład na decydentów mających autorytet w społeczeństwie, może być przysłowiowym zapalnikiem do wywołania masowych protestów, strajków, a nawet zamachu stanu. Wszystko zależy od siły oddziaływania agresora, odporności atakowanego państwa i reakcji społeczności międzynarodowej. A odporność ta jest tym większa, im większa jest świadomość społeczeństwa na temat charakteru współczesnych zagrożeń oraz im większy jest poziom kompetencji państwa do przeciwstawienia się tym zagrożeniom. Reakcja społeczności międzynarodowej jest kluczowa z punktu widzenia kosztów społecznych i ekonomicznych ponoszonych przez agresora. Opisany powyżej scenariusz eskalacji konfliktu był realizowany przez Rosję w stosunku do Ukrainy, a jego finalnym efektem jest rosyjska agresja zbrojna na Ukrainę. Należy podkreślić, że w przypadku konfliktu zbrojnego nieznany jest jego rezultat końcowy, a tym samym nieznane są koszty społeczne i ekonomiczne zarówno dla agresora, atakowanego, jak i społeczności międzynarodowej zaangażowanej we wsparcie zaatakowanego. Przy tego typu zagrożeniach, przy istotnym prawdopodobieństwie wybuchu konfliktu zbrojnego, wszelkie prognozy rozwoju sytuacji, zwłaszcza w obszarze finansów, mogą być obarczone błędami, co zobrazowano na rysunku 2.2. Poniższy przykład pokazuje, jak dynamiczny jest współczesny świat i jakie znaczenie dla prognoz mają *czarne łabędzie*. W przedstawionym przykładzie nie można się dopatrzeć uwzględnienia ryzyka konfliktu zbrojnego na Ukrainie, aczkolwiek prognoza dotyczy końca 2022 roku.



PIENIĄDZE

Jeszcze chwila i kurs złotego eksploduje, a do Polaków popłynie kasa, jakiej jeszcze nie oglądali

Arek Braumberger
13.01.2022

UDOSTĘPNIJ | UDOSTĘPNIJ (46) | KOMENTARZE (0)

Złoty po fatalnym 2021 r. powoli pnie się w górę i odrabia gigantyczne straty z ostatnich dwunastu miesięcy. Czy wyrwie się z kręgu najgorszych walut świata, zależy tylko od tego, co zrobią w najbliższym czasie NBP i polski rząd. Optymiści wierzą, że będzie dobrze.

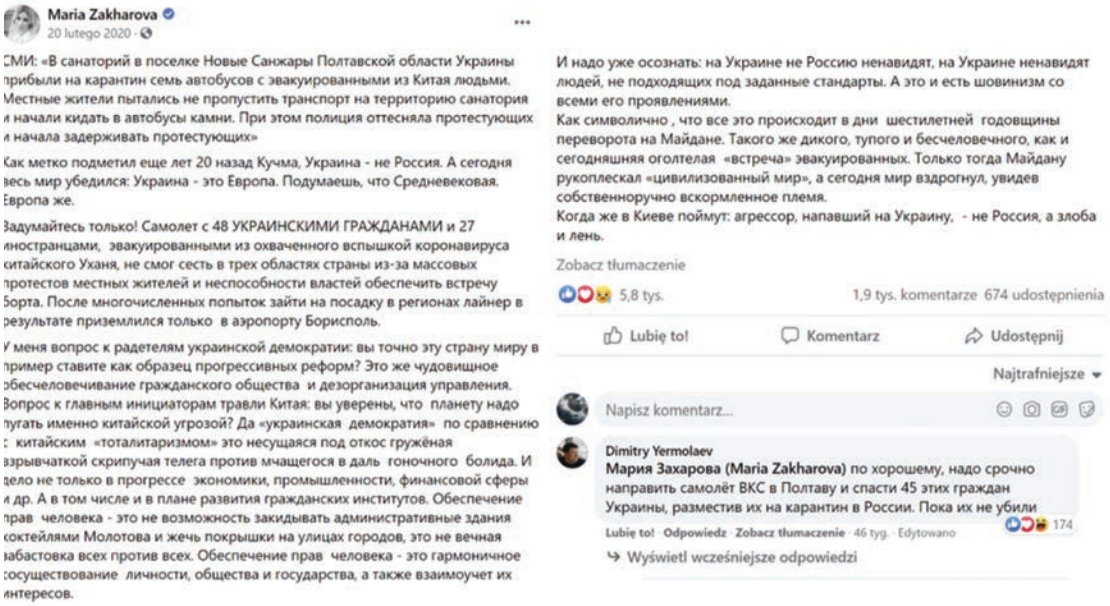
- EURPLN – 4.30-4.40 zł
- USDPLN – 3.80-3.90 zł
- CHFPLN – 4.18-4.20 zł

Marek Rogalski, główny analityk walutowy DM BOŚ, wielokrotnie nagradzany za analizy i prognozy, zakłada na koniec 2022 r. następujące kwotowania:

- EURPLN – 4.40-4.45
- USDPLN – 3.70-3.80
- CHFPLN – 4.20-4.30

Oby optymiści mieli rację.

Rysunek 2.2. Przykład prognoz kursu złotego z początku 2022 roku
Źródło: https://spidersweb.pl/bizblog/kurs-zlotego-waluty-2022/, [8.03.2022].



Rysunek 2.3. Przykład realizacji celu politycznego z wykorzystaniem portalu społecznościowego
Źródło: https://www.facebook.com/maria.zakharova.167/posts/10222164267245343, [12.01.2021].

Rysunek 2.4. Przykłady realizacji celu politycznego polegającego na zdezawuowaniu i osamotnieniu Ukraińców
Źródło: https://pl.sputniknews.com/20220102/rosja-wzywa-ue-do-potepienia-dzialan-ukrainskich-nacjonalistow-16906497.html, [1.02.2022]; https://demotywatory.pl/4885622/Banderowcy-napadnieci-przez-Rosje, [8.03.2022].

Na rysunkach 2.3. i 2.4. przedstawiono przykłady przekazu informacyjnego ukierunkowanego na cel polityczny związany z osłabieniem wizerunku Ukraińców w oczach Rosjan i społeczności międzynarodowej. Przekazy te bazują w głównej mierze na stereotypach. Pierwszy z nich został umieszczony na profilu społecznościowym rzeczniczki Ministerstwa Spraw Zagranicznych Rosji i związany był z zamieszkami, które wybuchły na Ukrainie w miejscowości Nowi Sanżary w lutym 2020 roku. Został on powielony między innymi przez polskojęzyczny portal pl.sputniknews.com, celem zwiększenia zasięgu oddziaływania informacyjnego na inne społeczeństwa, w tym przypadku na społeczeństwo polskojęzyczne[70]. Drugi przypadek dotyczy kreowania w społeczeństwie wizerunku Ukraińca jako faszysty i banderowca, co powinno wywoływać jednoznaczne negatywne konotacje i być wytłumaczeniem dla, jak to określił Prezydent Putin, demilitaryzacji i denazyfikacji Ukrainy. Same słowa demilitaryzacja i denazyfikacją są

[70] https://pl.sputniknews.com/swiat/2020022111965248-sputnik-to-sredniowiecze-rzeczniczka-msz-rosji-skomentowala-protesty-na-ukrainie/, [12.01.2021].

Rysunek 2.5. Przykłady antypolskiej propagandy
Źródło: https://pl.sputniknews.com/20210917/17-wrzesnia-data-ktora-wciaz-wywoluje-kontrowersje-16105896.html , [1.02.2022]; https://historia.wprost.pl/galerie/15375/3/agresja-zsrr-na-polske-w-oczach-sowieckiej-propagandy.html, [8.03.2022]; https://twitter.com/rusemb_pl/status/908712012947099650, [8.03.2022].

elementem antyukraińskiej propagandy w rosyjskojęzycznej przestrzeni informacyjnej i są politycznym zamiennikiem terminów wojna i agresja zbrojna.

Z podobnymi przekazami mamy do czynienia w przypadku tłumaczenia rosyjskiej napaści na Polskę we wrześniu 1939 roku.

W dobie rozwoju cyberprzestrzeni istotnego znaczenia nabierają cele technologiczne ukierunkowane na uzależnienie lub uniezależnienie, drenaż intelektualny, kradzież technologii lub ich blokadę. Cele te są wyraźniejsze, im bardziej krytyczna i uzależniająca jest technologia. Jaskrawym przykładem znaczenia posiadania technologii i zdolności produkcyjnych był wybuch pandemii koronawirusa i niezdolność krajów europejskich do produkcji podstawowych środków ochrony osobistej. Co więcej, widoczny jest w coraz większym stopniu drenaż intelektualny ukierunkowany na pozyskiwanie przez najbogatsze państwa świata elit intelektualnych innych państw. W tym przypadku wykorzystywany jest system wartościowania publikacji i przydzielania im odpowiednich punktów, co skutkuje z jednej strony podniesieniem prestiżu uczelni i samych naukowców, z drugiej jednak naraża państwo stosujące punktację dorobku naukowego na zmniejszenie potencjału naukowego, a tym samym na osłabienie gospodarcze i ekonomiczne. Państwa takie jak Polska nie są w stanie konkurować pod względem nakładów na naukę z państwami zachodnimi, tym samym ich pozycja w atrakcyjności zatrudnienia jest dużo niższa. Co więcej, umieszczanie w dostępie publicznym informacji na temat prowadzonych badań naukowych w obszarach technologii krytycznych i uzależniających, doprowadza do jeszcze większego drenażu intelektualnego i w perspektywie długookresowej działa na niekorzyść państwa.

Istotnego znaczenia nabiera również inwigilacja, szpiegostwo i związana z nimi kradzież technologii. Gromadzenie przez korporacje i agencje rządowe wrażliwych informacji o użytkownikach sieci, a są nimi dane osobowe, upodobania, zainteresowania, poglądy, kontakty interpersonalne, jest przyczyną intensywnego rozwoju zagrożeń, ukierunkowanych na manipulowanie percepcją, kreowanie postaw i poglądów, wpływanie, szantaż i dyskredytację, szerzenie niepokojów czy też wpływanie na wyniki wyborów i referendów. W 2013 roku Edward Snowden[71] ujawnił dokumenty dotyczące inwigilacji użytkowników sieci Internet, związane z programem cyberinwigilacji PRISM[72], polegającego na monitorowaniu na szeroką skalę serwisów społecznościowych, kont poczty elektronicznej czy też połączeń telefonicznych. Stany Zjednoczone, na terytorium którego znajdują się siedziby największych światowych firm usług internetowych, takich jak Google, Microsoft, Apple czy Facebook, z których korzystają użytkownicy na całym świecie, przechowywało i nadal przechowuje informacje o miliardach użytkowników sieci.

[71] https://edition.cnn.com/2013/09/11/us/edward-snowden-fast-facts/index.html, [11.12.2020]
[72] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, [11.12.2020]

Rysunek 2.6. Aktywność użytkowników aplikacji Strava w bazie wojskowej Bagram
Źródło: https://www.bbc.com/news/technology-42853072, [11.12.2020]

Kolejne doniesienia związane są z inwigilowaniem i śledzeniem użytkowników programów wspierających aktywność fizyczną. Przykładem może być aplikacja *Strava*, która zbierała dane o użytkownikach, a następnie na tej podstawie publikowano statystki aktywności, w postaci interaktywnej mapy *global heatmap*. Pod koniec stycznia 2018 roku zainteresowanie użytkowników mediów społecznościowych wzbudziła aktywność użytkowników aplikacji[73], w obszarach, które uznawane były za pustkowia, a które kojarzyły się z bazami wojskowym. Mapy te zawierały informacje dotyczące nie tylko położenia baz wojskowych, ale również informacje na temat poszczególnych użytkowników aplikacji. Przykład aktywności użytkowników aplikacji Strava w amerykańskiej bazie wojskowej w Afganistanie przedstawiono na rysunku 2.6.

Inwigilacja w cyberprzestrzeni jest także rodzajem szpiegostwa, zarówno gospodarczego, jak i państwowego, prowadzonego za pomocą wyrafinowanych narzędzi informatycznych. Graczami na tym polu są zarówno przedstawiciele biznesu, jak i państwa, a w obrębie ich zainteresowań są informacje dotyczące działalności gospodarczej konkurentów i stanowiące tajemnicę państwową. Inwigilacja jest związana także z podstawową działalnością państwa, ukierunkowaną na zapewnienie własnego bezpieczeństwa i bezpieczeństwa obywateli. W tym wypadku państwo stosuje narzędzia śledzące użytkowników cyberprzestrzeni, a zebrane informacje powinny być wykorzystywane wyłącznie do zwiększenia poziomu bezpieczeństwa. Najlepszym przykładem szpiegostwa gospodarczego jest kradzież planów samolotu F-35[74]. Na rysunku 2.7. przedstawiono samolot F-35 z jego chińskim odpowiednikiem J-31.

Przejawem rywalizacji na polu nowoczesnych technologii jest rozwijana przez Rosję koncepcja rosyjskojęzycznej sieci RUNet. Podejście do roli i znaczenia sieci Internet (cyberprzestrzeni) w Rosji zmieniło się diametralnie na przestrzeni ostatnich 10 lat. Z jednej strony dostrzeżono jej znaczenie dla rozwoju nowoczesnej gospodarki, z drugiej zaś uznano, że jest to środowisko niosące za sobą ogromne zagrożenia dla stabilności rządów. Co więcej uznano również, że cyberprzestrzeń jest częścią środowiska informacyjnego, wykorzystywanego do realizacji interesów narodowych, inwigilacji, szpiegostwa, kreowania postaw, idei i poglądów, środowiskiem, w którym przewagę technologiczną ma świat zachodni, a zwłaszcza Amerykanie. Uznano zatem, że sieć Internet powinna być podporządkowana administracyjnie bezpośrednio państwu, tak aby zapewnić w niej pełną kontrolę nad treściami w niej umieszczanymi. Podjęto kroki związane z uniezależnieniem się od technologii zachodnich i oparciu infrastruktury sieciowej na rodzimych rozwiązaniach. Znamiennym dla postrzegania roli cyberprzestrzeni w Rosji było podpisanie 5 grudnia 2016 roku przez Prezydenta Władimira Putina nowej Doktryny Bezpieczeństwa Informacyjnego Federacji Rosyjskiej. Jest to dokument przełomowy, ukazującym w nowym świetle rosyjskie podejście do bezpieczeństwa informacyjnego, wojny informacyjnej

[73] https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases, [11.12.2020]

[74] https://www.scmp.com/news/china/military/article/3025403/john-bolton-accuses-china-stealing-f-35-technology-make-stealth, [11.12.2020]

Rysunek 2.7. Amerykański samolot F-35 z jego chińskim odpowiednikiem J-31
Źródło: https://twitter.com/navalinstitute/status/1252246949627125760 , [11.12.2020]

i jej znaczenia dla historycznej i bieżącej polityki Rosji. Doktryna ta identyfikuje główne obszary przeciwdziałania operacjom ukierunkowanym przeciwko Rosji w ogólnie pojmowanym środowisku informacyjnym i wskazuje na konieczność ciągłego podnoszenia zdolności Rosji w przestrzeni informacyjnej poprzez – jak to określono – *doskonalenie systemu zapewnienia bezpieczeństwa sił zbrojnych* Federacji Rosyjskiej[75].

Analizy wykazały, że rosyjskie działania odnośnie sieci Internet ukierunkowane zostały na pełną jej kontrolę w granicach państwowych z jednoczesnym zachowaniem korzyści wynikających z zalet globalnej sieci. Jest to element prowadzonej przez Rosjan walki informacyjnej ukierunkowanej na panowanie we własnej inforsferze i wykorzystanie sieci do zdobywania informacji, ataków na infrastrukturę krytyczną, szerzenie dezinformacji i propagandy. Realizacja własnej, narodowej sieci RUnet odbywa się w trzech głównych obszarach: sekurytyzacja sieci w granicach państwa, panowanie nad wymianą informacji pomiędzy siecią RUnet a siecią globalną oraz pełna kontrola nad krytycznymi zasobami *rosyjskiego Internetu*[76].

Sekurytyzacja sieci w granicach państwa realizowana jest poprzez[77]:

- podniesienie rangi cyberbezpieczeństwa na poziom bezpieczeństwa państwa;
- scentralizowanie i znacjonalizowanie systemu ostrzegania o zagrożeniach w sieci;
- znacjonalizowanie norm technicznych oraz rozbudowa własnych technologii sieciowych (teleinformatycznych);
- stworzenie funkcji *wyłącznika sieci* (*ang. kill switch*) umożliwiającego odłączenie *rosyjskiego Internetu* od sieci globalnej.

Panowanie nad wymianą informacji pomiędzy siecią RUnet a siecią globalną ukierunkowane zostało na[78]:

- filtrowanie informacji;
- wprowadzenie przepisów dotyczących przechowywania informacji na terytorium Rosji;
- blokowanie geograficzne sieci.

Z kolei kontrola nad zasobami *rosyjskiego Internetu* realizowana jest poprzez[79]:

- zebranie informacji o operatorach telekomunikacyjnych i deweloperach informacji – stworzenie listy tak zwanych punktów wymiany ruchu;
- ustalenie pełnej listy adresów sieciowych oraz ich właścicieli;

[75] https://www.cybsecurity.org/pl/analiza-nowej-doktryny-informacyjnej-rosji/, [13.01.2021].
[76] I. Stadnik *Sovereign Runet: What does it mean … op. cit.*, s. 2.
[77] Ibidem.
[78] Ibidem, s. 9.
[79] Ibidem, s. 12.

- stworzenie wykazu systemów autonomicznych oraz danych osób, którym nadano identyfikatory sieciowe;

- określenie szczegółowych zasad routingu w sieci.

Znamiennym przykładem realizacji celu technologicznego jest także konflikt pomiędzy Stanami Zjednoczonymi a Chinami o firmę Huawei. W tym przypadku Stany Zjednoczone oskarżyły firmę Huawei o szpiegostwo gospodarcze i zakazały stosowania tych rozwiązań technologicznych w swoich sieciach teleinformatycznych. Znamiennym jest fakt, że Huawei jako pierwszy na świecie zaimplementował technologię 5G i tym samym uzyskał przewagę technologiczną nad Amerykanami.

Rysunek 2.8. Przykłady oskarżeń firmy Huawei o szpiegostwo
Źródło: https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack, [7.02.2022]; https://www.reuters.com/legal/transactional/huawei-accused-stealing-trade-secrets-spying-pakistan-2021-08-12 [7.02.2022]; https://www.nbcnews.com/politics/national-security/u-s-officials-using-huawei-tech-opens-door-chinese-spying-n1136956, [7.02.2022].

Kolejnym celem kooperacji negatywnej jest **cel ekonomiczny**. Jest on najczęściej związany z aktywnością podmiotu w sferze ekonomicznej (gospodarczej), jego zdolnością kredytową, ukierunkowaną na efektywność i maksymalizację zysków, ale także ze zwykłym oszustwem ukierunkowanym na szybki zysk kosztem nieświadomych obywateli. Dla podmiotów takich jak państwo cele ekonomiczne są podyktowane zrównoważonym rozwojem kraju, rozwojem gospodarki, bogaceniem się społeczeństwa, a jego wymiernymi znacznikami są: produkt krajowy brutto, dług publiczny, zdolność kredytowa, poziom inflacji, stosunek eksportu do importu, zamożność społeczeństwa. Sprostanie powyższym wyzwaniom wymusza na państwie posiadanie zasobów materiałowych, energetycznych, ludzkich, technologicznych, przemysłowych i finansowych. Tym samym w kooperacji negatywnej, ukierunkowanej na cele ekonomiczne, można oddziaływać między innymi na: zasoby, technologie, przemysł, system finansowy, walutę, wizerunek państwa, decydentów i wiele innych.

Istnieją państwa, których działalność w przestrzeni informacyjnej jest ukierunkowana na kradzież technologii, co pozwala im skutecznie rozwijać własną gospodarkę i powoduje znaczne oszczędności. W przedstawionym już przypadku kradzieży planów samolotu F-35 szacuje się, że Chiny zaoszczędziły co najmniej 5 miliardów dolarów i wiele lat niezbędnych do przeprowadzenia badań i uzyskania podobnych rezultatów. Należy przypuszczać, że działalność szpiegowska prowadzona w cyberprzestrzeni będzie w dalszym ciągu rozwijana, także w sektorze finansów, a informacje w ten sposób zdobyte mogą być wykorzystane do działania z pozycji dodatniej, wrogiego przejęcia lub dyskredytacji atakowanej instytucji.

Znane są także przypadki wrogiej działalności w stosunku do zasobów, mającej na celu uzależnienie

państwa na przykład od surowców energetycznych lub też nawet ich pozbawienie. Znamiennym przykładem są działania Rosji w stosunku do krajów europejskich, w tym Polski i Ukrainy. Niestety pomimo alarmujących apeli rządu polskiego do krajów zachodnich informujących o tym, że gazociąg Nordstreem 2 jest tylko i wyłącznie narzędziem polityki Rosji, certyfikacja gazociągu została wstrzymana dopiero po agresji Rosji na Ukrainę. Przykłady oddziaływania informacyjnego ukierunkowanego na pozytywne postrzeganie Rosji jako wiarygodnego partnera biznesowego gwarantującego Polsce bezpieczeństwo energetyczne przedstawiono na rysunku 2.9. Analizy wykazały, że cele realizowane w obszarze surowców strategicznych będą ukierunkowane w coraz większym stopniu na uran i lit, co związane jest z polityką klimatyczną Unii Europejskiej i osiągnięciem zero emisyjności.

Rysunek 2.9. Przykłady prorosyjskiego lobbowania energetycznego
Źródło: https://t.me/SputnikPolska/3686, [8.02.2022]; https://pl.sputniknews.com/20220120/ogromne-wydatki-na-import-surowcow-energetycznych-komu-polska-placi-najwiecej-17049038.html, [8.02.2022].

W odniesieniu do zasobów ludzkich sterowanie przekazem informacyjnym oczerniającym, dyskredytującym dane społeczeństwo, bazującym na stereotypach i uprzedzeniu, może być ukierunkowane na zniechęcenie potencjalnych emigrantów od rynku pracy atakowanego podmiotu. Z drugiej strony wywoływanie niepokojów społecznych może skutkować zwiększeniem emigracji zarobkowej, a tym samym pozbawieniem atakowanego rynku rąk do pracy. Rozpowszechnianie fałszywych informacji na temat sytuacji gospodarczej i ekonomicznej danego państwa może być ukierunkowane na obniżenie ratingów zdolności kredytowej państwa, co w perspektywie długookresowej może doprowadzić do jego głębokiej zapaści ekonomicznej i społecznej. Oczywiście można przytaczać wiele innych celów oddziaływania, niemniej jednak nie wpłynie to na konkluzję, że wroga działalność wymierzona w podstawy ekonomiczne innego podmiotu bezpieczeństwa wymaga czasu i przede wszystkim informacji, zarówno zdobytej, zmodyfikowanej, jak i celowo spreparowanej. Cyberprzestrzeń w tym wymiarze będzie odgrywała coraz większą rolę, z uwagi na:

- możliwość inwigilacji systemów informacyjnych strony przeciwnej,

- możliwość prowadzenia kampanii dezinformacyjnych,
- możliwość prowadzenia kampanii propagandowych,
- uzależnienie funkcjonalności gospodarki od technologii informacyjnych.

Przykłady działań ukierunkowanych na zasoby ludzkie przedstawiono na rysunku 2.10.

Rysunek 2.10. Przykłady oddziaływania informacyjnego w obszarze zasobów ludzkich
Źródło: https://www.economist.com/europe/2020/02/22/poland-is-cocking-up-migration-in-a-very-european-way, [9.03.2022]; https://demotywatory.pl/4813398/Mlodzi-wyszli-na-ulice-bo-maja-dosc-Ukraincow-na-rynku-pracy-w, [9.03.2022].

Wybuch wojny na Ukrainie uzmysłowił, jak współczesne społeczeństwo podatne jest na przekazy informacyjne i jaką rolę w tych przekazach odgrywają portale społecznościowe. Przykładem mogą być rozpowszechniane informacje o drastycznym ograniczeniu dostępności paliwa dla obywateli, zachowaniu rezerw dla wojska i całkowitym wstrzymaniu dostaw ropy naftowej z Rosji. Przekazy te wywołały panikę, przed stacjami ustawiały się długie kolejki samochodów, co w rezultacie doprowadziło do chwilowych braków w dostępności paliwa. Większość z tych przekazów związana była z działalnością prorosyjskich trolli internetowych, których działalność jest dobrze zorganizowana i ukierunkowana na realizację interesów Rosji[80].

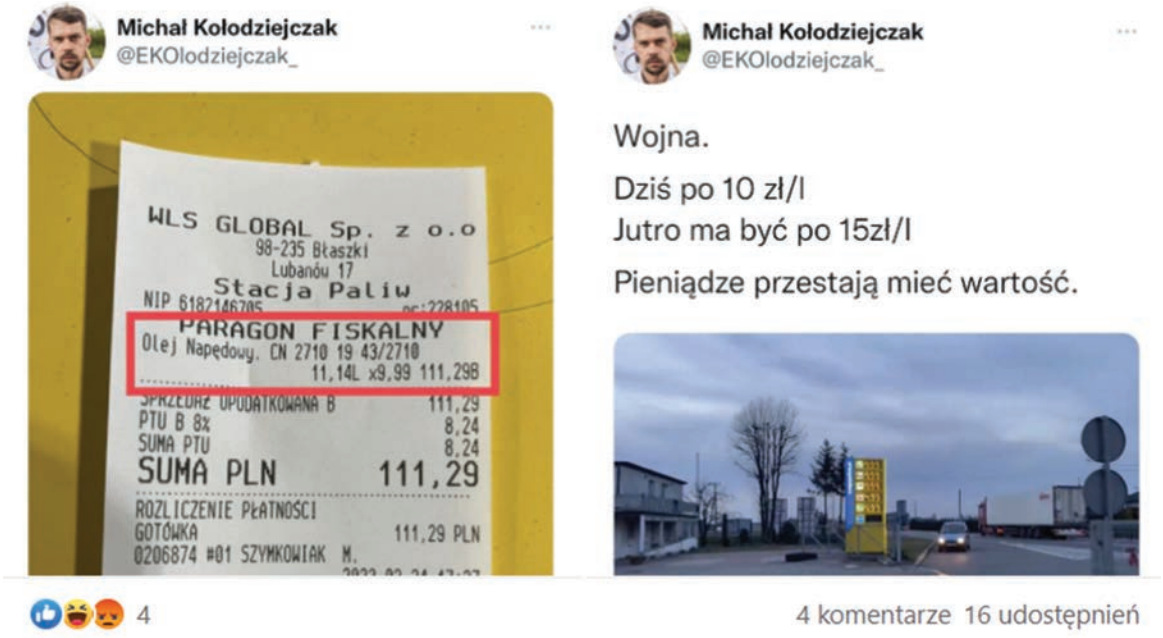
Znamiennym przykładem beztroski w przekazie informacji, powodującym panikę w społeczeństwie, jest post lidera Agrounii Michała Kołodziejczaka, który zamieścił na swoim profilu społecznościowym przekaz, zobrazowany na rysunku 2.11. Z uwagi na liczbę osób śledzących profil, przekaz był piorunujący i wywołał wykupienie paliwa na licznych stacjach w kraju. Autor przytoczonego wpisu prawdopodobnie nie zdawał sobie sprawy, jak wielkie zamieszanie wywoła.

W przestrzeni informacyjnej funkcjonują także przekazy ukierunkowane na zwykłe oszustwo. Doskonałym środowiskiem do realizacji tego typu działalności jest cyberprzestrzeń, zapewniająca anonimowość sprawcom i umożliwiająca dotarcie do szerokiego grona odbiorców. W przekazach tych najczęściej występuje odwołanie do autorytetów, pseudoautorytetów lub instytucji finansowych. Przekazy te oczywiście realizowane są bez ich zgody i wiedzy, i bazują na najprostszych ludzkich instynktach szybkiego wzbogacenia się, tak jak w omawianym w rozdziale pierwszym przypadku AmberGold. Co więcej, przekazy te są uwiarygodniane fałszywymi analizami finansowymi, do których zwykły użytkownik cyberprzestrzeni nie może merytorycznie się odnieść. Przykłady tego typu działalności przedstawiono na rysunku 2.12.

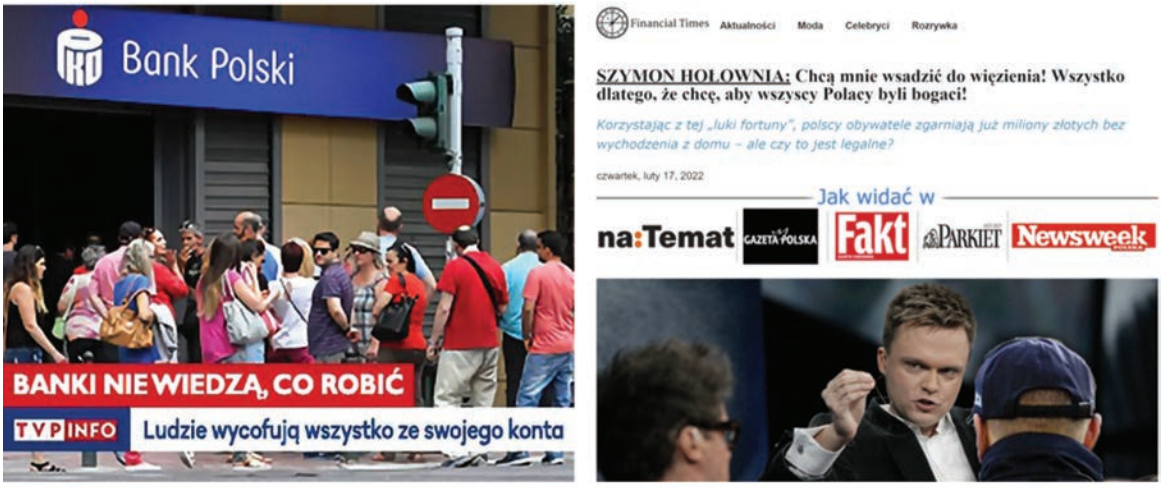
Analizy wykazały, że cyberprzestrzeń stała się doskonałym środowiskiem do oddziaływania w wymiarze ekonomicznym z wykorzystaniem ataków informatycznych. Można przytoczyć wiele przykładów tego typu zdarzeń, których efektem były istotne straty finansowe poniesione przez atakowane podmioty. Jednym z nich jest atak na sieć kasyn Sands w Las Vegas w lutym 2014 roku[81].

[80] https://alebank.pl/120-tys-fejkow-dziennie-w-polskim-internecie-od-rosyjskich-trolli/?id=403919&catid=25926, [9.03.2022].

[81] https://www.claimsjournal.com/news/national/2020/01/06/294849.htm, [12.01.2020].



Rysunek 2.11. Przykład wpisu powodującego niepokoje w społeczeństwie
Źródło: https://www.facebook.com/search/top?q=b%C5%82aszki%20paliwo%20ko%C5%82odziejczak, [3.03.2022].



Rysunek 2.12. Przekaz informacyjny ukierunkowany na oszustwo
Źródło: https://straitsmagazine.com/6FrKs3YM?utm_term=&utm_creative=582603230588&utm_campaign=16004223026&utm_position=-none&utm_network=d&utm_target=&utm_placement=demotywatory.pl&utm_match=, [15.02.2022]; https://wristdreamplane.com/?gclid=EAIaIQobChMIxczawNz59QIVTeuaCh1eKQ3qEAEYASAAEgKMG_D_BwE, [15.02.2022].

W jego wyniku właściciel kasyna poniósł straty finansowe szacowane na ponad 40 milionów dolarów. Atak ten umotywowany był w głównej mierze zemstą na właścicielu kasyna, Sheldonie Adelsonie, który na konferencji w Nowym Jorku zasugerował profilaktyczne zrzucenie bomby atomowej na irańskiej pustyni. Następnym znamienitym przykładem ataku, który doprowadził zarówno do strat finansowych, jak również ocenzurował w pewnym sensie przestrzeń publiczną w Stanach Zjednoczonych, był atak przeprowadzony na Sony Picture w listopadzie 2014 roku[82]. Atak związany był z zapowiedziami dystrybucji do kin filmu *The interwiew*, w którym w sposób prześmiewczy przedstawiono przywódcę Korei Północnej. W końcowym efekcie, film nie wszedł do powszechnej dystrybucji z uwagi na obawy związane z eskalacją zagrożeń i jawnymi groźbami strony północnokoreańskiej.

[82] https://www.bankinfosecurity.com/sony-pictures-cyber-attack-timeline-a-7710, [12.01.2021].

Ważnym celem w trakcie kooperacji negatywnej w cyberprzestrzeni jest także **cel społeczny**. W państwach demokratycznych to społeczeństwo jest tym czynnikiem, który kształtuje ustrój państwa i wybiera swoich przedstawicieli, a tym samym kształtuje prowadzenie polityki wewnętrznej i zagranicznej. Najogólniej rzecz ujmując, społeczeństwo poprzez akt wyboru decyduje, w którą stronę podąża państwo, jakie są jego priorytety i jak są one realizowane. Niestety, w coraz większym stopniu uwidaczniane są wpływy, na akt wyboru, na drodze negatywnego oddziaływania informacyjnego, umożliwiającego kreowanie fałszywej rzeczywistości, sprzyjającej stronie prowadzącej wrogą kampanię informacyjną. Cele realizowane w tego typu przekazach mogą mieć charakter polityczny, jak chociażby podczas wpływania na wyniki wyborów czy też referendów. Oddziaływanie negatywne na społeczeństwo może być ukierunkowane między innymi na: rozbicie, zubożenie, załamanie, zbuntowanie, przestraszenie lub zniechęcenie.

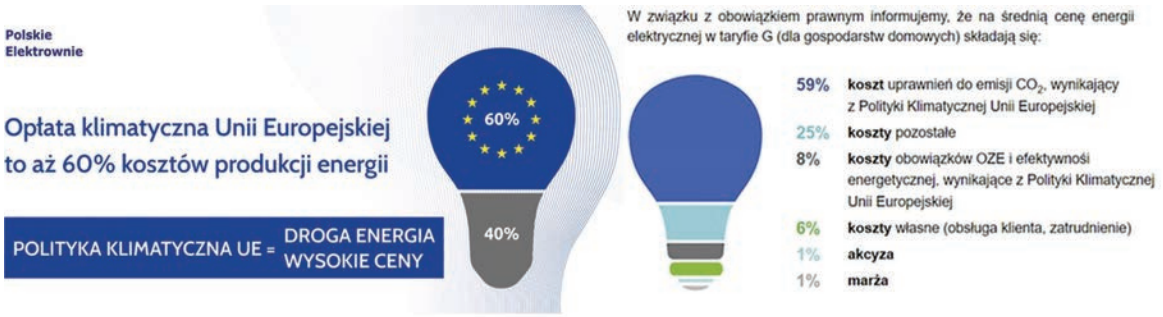
W myśl zasady dziel i rządź, działanie na rozbicie, zubożenie, załamanie, zbuntowanie, zniechęcenie i przestraszenie społeczeństwa jest podyktowane osłabieniem jego woli przeciwstawienia się wszelkim przeciwnościom i zagrożeniom. Łatwiej jest bowiem rywalizować ze społeczeństwem, które nie stanowi jedności, a rząd nie ma poparcia w całości społeczeństwa, nie może liczyć na jego poświęcenie i oddanie, szczególnie w sytuacjach kryzysowych. Pogłębianie i generowanie podziałów może mieć różne podłoże, zarówno światopoglądowe, kulturowe, ideologiczne, ale też ekonomiczne. Niejednorodne są drogi i sposoby takiego oddziaływania, lecz wspólny cel, zniszczenie spójności narodowej. Najczęściej mamy do czynienia z precyzyjnie przygotowaną i prowadzoną kampanią propagandową lub dezinformacyjną, rozłożoną w czasie, umożliwiającą osiągnięcie przyjętych celów strategicznych. Dodatkowo cyberprzestrzeń, stanowiąca istotny element przestrzeni informacyjnej, umożliwia prowadzenie kampanii informacyjnych w oderwaniu od uwarunkowań geograficznych, administracyjnych i czasowych, i jest tym bardziej skuteczna, im bardziej złożone i różnorodne jest społeczeństwo podmiotu oddziaływania. W przypadku podmiotów takich, jak chociażby Unia Europejska kampanie propagandowe będą coraz skuteczniejszym narzędziem generowania konfliktów pomiędzy nie tylko społecznościami danych państw, ale całymi narodami. Na rysunku 2.13. przedstawiono przykłady realizacji celu społecznego związanego z wytworzeniem wrogiego nastawienia do wybranych grup społecznych czy też narodowościowych.

Klasycznym przykładem dezinformacji ukierunkowanej na cel społeczny i być może także cel polityczny jest kampania informacyjna wymierzona w podstawy pakietu klimatycznego Unii Europejskiej. W tym przypadku bezpośrednim celem było zniechęcenie Polaków do samej Unii i poprawa wizerunku rządu po drastycznych podwyżkach cen energii elektrycznej w styczniu 2022 roku. W przedstawionych na

Rysunek 2.13. Przykład realizacji celu społecznego związanego z wytworzeniem wrogiego nastawienia do społeczności lub narodu

Źródło: https://pl.sputniknews.com/20200601/waszyngton-to-nie-moskwa-zdewastowano-pomnik-tadeusza-kosciuszki-sputnik-12510259.html/, [8.02.2022]; https://www.rt.com/sport/439208-jewish-cemetery-poland-sports-complex/, [8.02.2022].

rysunku 2.14. grafikach posłużono się techniką mieszania prawdy i kłamstwa. Z jednej strony w samych kosztach wytworzenia energii elektrycznej koszt emisji CO_2 wynosi około 60%, z drugiej jednak strony koszt CO_2 dla końcowego odbiorcy energii elektrycznej to już tylko około 23%. Plakaty te, rozmieszczane w całym kraju, jak również dostarczane w postaci grafik z rachunkami za prąd, stały się zarzewiem szeroko zakrojonej debaty publicznej dotyczącej kierunków zmian w polityce polskiego rządu i zagrożenia wyjścia Polski z Unii Europejskiej. Cel stojący za tego typu przekazem informacyjnym jest niezrozumiały. Jeżeli była to dezinformacja taktyczna, to była ona ukierunkowana na doraźną poprawę wizerunku rządu i prawdopodobne wcześniejsze wybory. W przypadku dezinformacji strategicznej, jej celem mogło być przygotowanie gruntu pod wyjście Polski ze struktur Unii Europejskiej. Wybuch wojny na Ukrainie w znaczny sposób odmienił bieżącą sytuację polityczną i zmienił postrzeganie i rolę Unii Europejskiej w polskim społeczeństwie, tym samym cele kampanii informacyjnej odeszły na dalszy plan.



Rysunek 2.14. Przykład dezinformacji techniką mieszania prawdy i kłamstwa
Źródło: https://zielona.interia.pl/polityka-klimatyczna/news-czy-naprawde-to-ue-odpowiada-za-drogi-prad-w-polsce-ekspert-,nId,5822893, [8.02.2022]; https://www.money.pl/gospodarka/polacy-placa-wiecej-za-prad-pis-mowi-ze-to-wina-unii-klamstwo-i-manipulacja-6735111051401952a.html, [8.02.2022].

Innym przykładem przekazów informacyjnych ukierunkowanych na zniechęcenie społeczeństwa do wybranej grupy osób, jest propaganda sugerująca, że społeczność LGBT odpowiada za promowanie pedofilii.

Rysunek 2.15. Przykłady propagandy wymierzonej w społeczność LGBT.
Źródło: https://konkret24.tvn24.pl/polska,108/srodowiska-lgbt-uznaly-pedofilie-za-nowa-orientacje-falszywe-grafiki-powrocily,937146.html, [8.02.2022].

Cel religijny jest bezpośrednio związany z atakiem na systemy wartości dominujące w danym społeczeństwie. Z jednej strony dąży się do radykalizacji poglądów, z drugiej do ich złagodzenia. To także przeciwstawienie wyznawców jednej religii przeciwko wyznawcom innej i dążenie do zwiększenia zasięgu własnej wiary poprzez działania ukierunkowane na zastraszenie lub konwersję. Wojny religijne zawsze były nieodzownym elementem historii ludzkości. Oczywiście ich charakter był często podyktowany nie tylko celem ideologicznym, lecz także czystą pragmatyką zdobycia władzy, zajęcia terenu, przejęcia zasobów, wzbogacenia się, jednak ich przebieg i zasięg zawsze były związane z poziomem rozwoju ludzkości. I chociaż można się zgodzić z poglądem, że ich współczesny wymiar może być także krwawy, jak w przypadku wojny toczonej przez tak zwane Państwo Islamskie, to coraz większą aktywność ugrupowań religijnych możemy obserwować w cyberprzestrzeni. Jest to doskonałe środowisko do szerzenia idei, znajdowania i pozyskiwania zwolenników i wyznawców, radykalizowania poglądów, szerzenia strachu i terroru. To także środowisko komunikacyjne, pozwalające na tworzenie organizacji rozproszonych, umożliwiające koordynowanie działań umotywowanych ideologicznie, wymierzonych zarówno w przeciwników religijnych, jak i w społeczeństwa bazujące na innych systemach wartości. W tę działalność wpisują się różnego rodzaju fundamentaliści religijni, stosujący jako sposób oddziaływania zamachy terrorystyczne. Na rysunku 2.16. przedstawiono przykłady klasycznej propagandy obrazkowej, z wykorzystaniem tak zwanych memów, wymierzonej w wyznawców judaizmu i katolików.

Rysunek 2.16. Przykład propagandy wymierzonej w katolików i wyznawców judaizmu.
Źródło: https://encyclopedia.ushmm.org/content/en/photo/nazi-anti-jewish-propaganda, [9.03.2022]; https://www.patheos.com/blogs/daffeythoughts/2016/02/the-washington-post-cries-bigotry-in-a-display-of-stunning-ignorance.html, [9.03.2022].

Pozostał do omówienia **cel militarny**, związany bezpośrednio z siłami zbrojnymi i ich zdolnością do prowadzenia działań. Cele militarne będą wynikały z przyjętych celów operacyjnych i strategicznych, roli i miejsca sił zbrojnych w systemie obronnym państwa. Mogą być one ukierunkowane zarówno na destrukcję zasobów przeciwnika, osłabienie jego potencjału, przejęcie lub utrzymanie terenu, zyskanie czasu, ochronę i osłonę własnych zasobów militarnych i cywilnych. Odbywać się to będzie za pomocą kampanii informacyjnych, oddziaływania informatycznego i kinetycznego, przy uwzględnieniu synergii z innymi rodzajami działań.

Carl von Clausewitz, odnosząc się do celów i środków walki, stwierdził, że *jeżeli wojna jest aktem przemocy, aby zmusić przeciwnika do wykonania naszej woli, to powinno zawsze chodzić jedynie i wyłącznie o powalenie wroga, to znaczy jego obezwładnienie*[83]. Do przeszkód stojących na drodze do osiągnięcia tego celu zaliczył trzy elementy: siły zbrojne, kraj i wolę przeciwnika. Określił on sposób postępowania z poszczególnymi elementami, mówiąc, że w przypadku sił zbrojnych działanie ukierunkowane powinno być na ich zniszczenie, doprowadzenie do stanu, w którym nie będą zdolne do dalszej walki; kraj należy zdobyć, z uwagi na to, że mogą być w nim tworzone nowe siły zbrojne; oraz złamać wolę przeciwnika, zmusić społeczeństwo do ustępstw, spełnienia żądań i całkowitego poddania.

[83] C. Clausewitz, *O wojnie*, Wydawnictwo Test, Lublin 1995, s. 27.

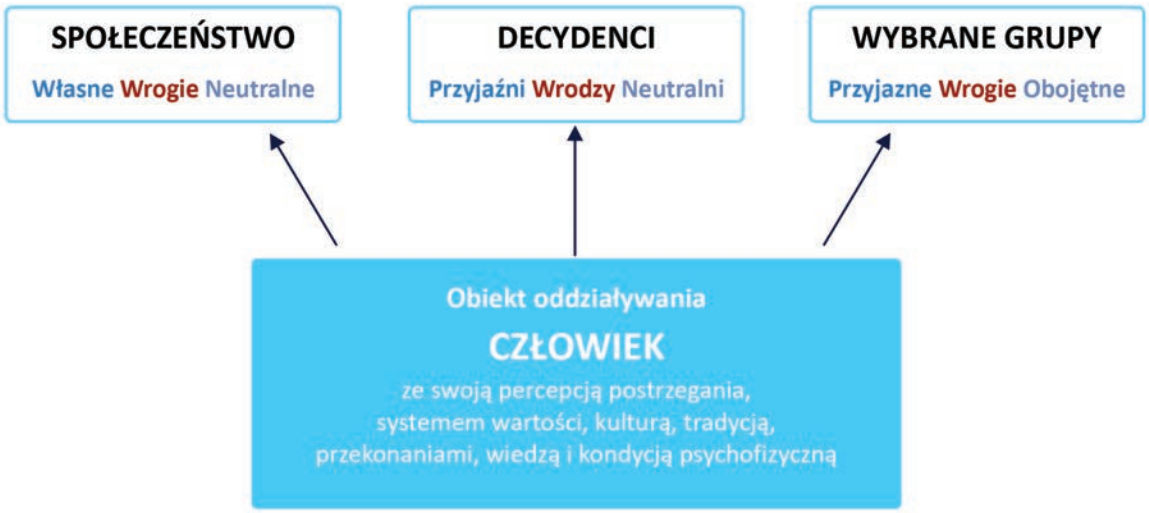
Ta swoista triada klasycznych elementów wojny była wyznacznikiem sposobu rozegrania wojen właściwie przez wieki. I zapewne nadal nią może być w odniesieniu do wybranych podmiotów prawa międzynarodowego. Jednak powinniśmy się zastanowić co będzie, jeżeli odwrócilibyśmy hierarchię wartości i na pierwszy plan wysunęli osłabienie lub nawet zniszczenie woli strony przeciwnej, oponenta? Czy zagwarantuje to osiągnięcie przyjętych celów działania? Czy należy zająć kraj, zniszczyć jego siły zbrojne, aby wygrać wojnę? Współczesne pojęcie wojny zostało rozmyte, a każdy konflikt zbrojny związany jest z ogromnymi kosztami ekonomicznymi i społecznym oraz niesie za sobą niepewność wyniku końcowego, także prawdopodobieństwo porażki.

Wziąwszy pod uwagę przedstawione wątpliwości, można przypuszczać, że sukces może być odniesiony poprzez zmianę priorytetów oddziaływania i ukierunkowanie go na ludzi, którzy decydują o funkcjonowaniu podmiotów, jakimi są państwa. Mają oni swoją percepcję postrzegania rzeczywistości, własne systemy wartości, kulturę, historię, tradycję, religię i przekonania. Na bazie tych uwarunkowań, wspartych sterowanymi przekazami informacyjnymi, można budować w społeczeństwie takie nastawienie i ogląd rzeczywistości, które będą sprzyjały osiągnięciu przyjętych celów działania. Przekaz informacyjny powinien być ukierunkowany zarówno na tych, którzy sprzyjają agresorowi, są jego przeciwnikami, ale także w swoich poglądach są neutralni i nie stanowią docelowego obiektu oddziaływania. Należy jednocześnie zaznaczyć, że w każdej grupie społecznej znajdują się jednostki, które mniej lub bardziej identyfikują się z poglądami prowadzącego agresywną kampanię informacyjną, co w znacznym stopniu ułatwia generowanie i tworzenie podziałów, mieszanie w umysłach, osłabienie woli przeciwstawienia się, pozbawienie zwolenników i przyjaciół.

Rysunek 2.17. Przykłady realizacji celów militarnych.
Źródło: https://web.archive.org/web/20200219153121/https://theduran.com/nato-top-military-officer-defender-20-is-facing-problems/, [9.02.2022]; https://www.mpolska24.pl/post/15402/dragon-17-czyli-najwieksza-kompromitacja-w-dziejach-mon-czesc-2, [9.02.2022]; https://www.fakt.pl/wydarzenia/polityka/kulisy-cwiczen-dragon-17-dramatyczna-sytuacja-wyposazenia-rezerwy/f309174, [9.02.2022].

Ostatecznym efektem oddziaływania będzie osamotnienie i obezwładnienie psychofizyczne obiektu oddziaływania, tym samym pozbawienie woli walki i zdolności skutecznego przeciwstawienia się zamiarom agresora. Skutkować to może całkowitym lub częściowym podporządkowaniem terytorium danego kraju interesom agresora, na przykład pod względem ekonomicznym lub energetycznym, włączenie go we własną strefę wpływów bez konieczności destrukcyjnego unieszkodliwiania jego sił zbrojnych. W takim schemacie postępowania siły zbrojne będą obezwładniane wieloetapowo poprzez stopniową likwidację przemysłu zbrojeniowego, spowolnienie modernizacji technicznej, brak reform struktur dowodzenia, rezygnację z poboru, tworzenia rezerw materiałowych i osobowych, zniszczenie wiarygodności w strukturach międzynarodowych. Przemoc zbrojna schodzi w tym wypadku na plan dalszy i jest niejako dopełnieniem, tym elementem, który jest ostatecznością. Oczywiście taki schemat postępowania jest możliwy wyłącznie w stosunku do podmiotów, które nie mogą zapewnić sobie pożądanego poziomu bezpieczeństwa, budowanego w oparciu o własne siły zbrojne, ale przed wszystkim w oparciu o wiarygodne sojusze militarne i międzynarodową współpracę gospodarczą. Na rysunku 2.17. przedstawiono przykłady oddziaływania informacyjnego ukierunkowanego na osłabienie wizerunku sił zbrojnych, zniechęcenie społeczeństwa do partycypowania w kosztach ich utrzymania i osłabienie zawartych sojuszy wojskowych.

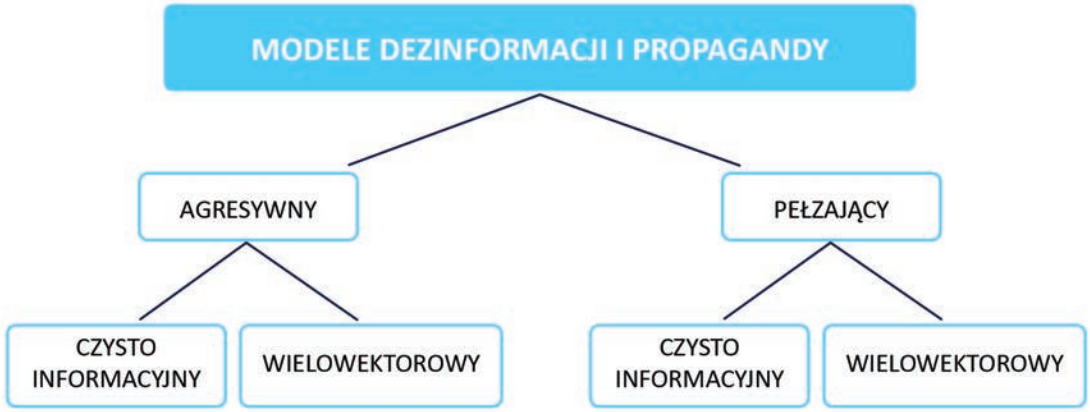
Kończąc tę część rozważań, należy podkreślić, że w kampaniach informacyjnych obiektami oddziaływania są ludzie, społeczeństwa, rządzące elity, podzieleni na trzy główne kategorie: przyjaciół, przeciwników i obserwatorów, co zaprezentowano na rysunku 2.18.



Rysunek 2.18. Priorytetowe obiekty oddziaływania w przekazach informacyjnych
Opracowanie własne

Modele dezinformacji i propagandy w sektorze bankowym

Rozpatrując dezinformację i propagandę przez pryzmat ich charakteru i sposobu realizacji można zaobserwować, że są to procesy, które mogą być realizowane według odmiennych modeli postępowania. Pierwszy model – **agresywny** – realizowany jest w krótkim czasie, a jego główny cel związany jest z bieżącą sytuacją na rynkach ekonomicznych lub też z szybką realizacją np. zysków. Działania te są łatwo identyfikowalne, a tym samym istnieje możliwość adekwatnej reakcji na zaistniałą sytuację. W drugim modelu – **pełzającym** – realizowane cele są rozłożone w czasie, często kilkunastoletnie, co w znacznym stopniu utrudnia identyfikację tego typu działań. Obserwacje wykazały, że zarówno w modelu agresywnym, jak i pełzającym, oddziaływanie może być **czysto informacyjne**, ograniczone do dezinformacji i propagandy, jak i **wielowektorowe** z dodatkowym wykorzystaniem narzędzi informatycznych. Modele te zostały przedstawione na rysunku 3.1.



Rysunek 3.1. Modele oddziaływania informacyjnego
Opracowanie własne

3.1. Model pełzający czysto informacyjny

Model maksymalizacji oddziaływania, widoczności i głównego przesłania narracji.

Ogólnym rezultatem tej kampanii informacyjnej jest ukształtowanie świadomości ofiary, wpływanie na jej postawy i zachowania, a w efekcie podjęcie przez nią niekorzystnych dla niej finansowych działań.

Wrogi podmiot będzie dysponował planem kampanii informacyjnej. Określi w nim ramy czasowe realizacji kampanii. Przydzieli niezbędny czas na: rozpoznanie grupy docelowej, dostępne lokalizacje, dostępne zasoby (infrastruktura, techniczne, osobowe, zabezpieczenia). Charakter i czas trwania takich przygotowań będzie zależał od poziomu przygotowania zarówno atakującego, jak i ofiary. Ustalone zostaną potrzeby informacyjne oraz kanały komunikacji. Odpowiedni czas trwania planowania będzie uzależniony od wielkości i różnorodności grupy docelowej, a także od złożoności systemu, który ma zostać zaatakowany. Po fazie rozpoznawczej opracowane zostaną odpowiednie narzędzia techniczne, komunikaty oraz metody prowadzenia kampanii.

Ustalone zostaną najlepsze sposoby przekazywania kluczowych wiadomości. Język i formaty zostaną dostosowane do odpowiedniej kultury z uwzględnieniem ogólnego poziomu umiejętności czytania i pisania, różnorodności używanych języków i odpowiednich obrazów, które reprezentują podstawowe wiadomości. Uwzględnione zostaną również takie czynniki, jak na przykład nieformalna terminologia używanej przez grupę przeznaczenia.

Określone zostaną odpowiednie kanały komunikacji do wykorzystania w kampanii informacyjnej. Odpowiednie kanały komunikacji będą brać pod uwagę kilka czynników, w tym preferencje komunikacyjne i zachowania w obrębie populacji docelowej; złożoność udostępnianych informacji oraz dostępny budżet i zasoby do realizacji. Preferowane kanały komunikacji często różnią się w zależności od wieku, grupy społecznej, pochodzenia etnicznego, poziomu umiejętności czytania i pisania, poziomu wykształcenia, znajomości i dostępu do technologii, płci, religii, niepełnosprawności lub innych cech i mogą się zmieniać w czasie. Wykorzystane zostaną preferowane i zaufane kanały komunikacji. Wybrane kanały muszą być do zaakceptowania przez populację docelową. Wykorzystane będzie wiele formatów, w tym form pisemnych, ustnych i obrazkowych. Wzmocniona zostanie wiarygodność przekazywanych komunikatów. Kampania informacyjna zaprojektowana będzie

w taki sposób, aby większość osób otrzymywała te same (lub podobne) informacje przynajmniej dwoma różnymi kanałami: poprzez media społecznościowe i zapowiedzi w postach internetowych. Komunikaty odnosić się będą do potrzeb informacyjnych, obaw i wrażliwości oraz populacji docelowej. Wykorzystane kanały zaś będą dostępne, skuteczne i dalekosiężne.

Wszystkie produkty informacyjne przed ich wykorzystaniem w kampanii informacyjnej, po opracowaniu i przetłumaczeniu kluczowych przesłań będą przetestowane z udziałem różnych grup wiekowych, społecznych, płciowych czy światopoglądowych w populacji docelowej. Dla zmniejszenia niepewności i wywoływania podejrzeń kluczowe komunikaty będą wystandaryzowane.

Ramy czasowe wdrożenia będą zależne w szczególności od takich czynników, jak:

- wielkość populacji;
- obszar geograficzny, który kampania musi objąć;
- złożoność komunikatów do przekazania;

W przypadku doraźnych działań, takich jak weryfikacje obejmujące rozproszoną lub mobilną populację z ograniczonym dostępem do kanałów komunikacyjnych, ramy czasowe będą dłuższe, biorąc pod uwagę dostępność populacji do otrzymywania informacji.

Kanały wykorzystywane w kampanii to:

- Poczta internetowa na prywatne lub służbowe skrzynki pocztowe.
- Media społecznościowe.
- Media masowego przekazu.
- Propagandowe lub dezinformacyjne strony internetowe.
- Lokalne lub globalne ogłoszenia publiczne.
- Metody audiowizualne.
- Materiały piśmiennicze, graficzne.
- Grupy dyskusyjne.
- Bezpośrednie spotkania.

Po zbudowaniu odpowiedniej świadomości ofiary mogą być podjęte różne działania w celu wyłudzenia środków finansowych. Jednym z takich działań może być włamanie się do poczty elektronicznej sprzedawcy, a następnie przekonanie klienta, że zmiana danych bankowych jest autentyczna i nakłonienie do przelania odpowiedniej sumy pieniędzy. Innym sposobem może być uzyskanie wymaganych danych zarówno do komputera, jak i danych dostępu do konta bankowego. Następnie włamanie się do systemu komputerowego firmy i dokonanie stosownych przelewów finansowych.

Aby wykryć „phishingowe" wiadomości e-mail w swojej skrzynce oraz zapewnić bezpieczeństwo organizacji i jej funduszy zaleca się:

- Zachować czujność.
- Podejmować działania proaktywne.
- Sprawdzać, czy wiadomość zawiera właściwy adres URL.
- Sprawdzać, czy adresy URL zawierają wprowadzającą w błąd nazwę domeny.
- Sprawdzać, czy wiadomość zawiera błędną pisownię i gramatykę.
- Zachować ostrożność, jeśli w wiadomości jest prośba o podanie danych osobowych.
- Zachować czujność, jeśli oferta wydaje się zbyt piękna, aby była prawdziwa.
- Dołożyć starań, aby nie zainicjować akcji.
- Zachować czujność, jeśli jesteś proszony o przesłanie pieniędzy na pokrycie wydatków.
- Zachować czujność, jeśli przekaz zawiera nierealistyczne groźby
- Zachować czujność, jeśli wiadomość wydaje się pochodzić z agencji rządowej
- Zachować czujność, jeśli coś po prostu nie wygląda dobrze.

3.2. Modele agresywne wielowektorowe

Wykorzystanie kontrowersyjnych tematów + podmiana stron www + atak DDoS.

Adwersarz może wykorzystywać w rzeczywistości opublikowane kontrowersyjne tematy, takie jak błędne prognozy ekonomiczne, do stałego pomniejszania kompetencji osób odpowiedzialnych za polski sektor finansowy. Kampania może ulec wzmocnieniu w momencie, gdy któryś ze znanych banków zacznie

prezentować informacje o potencjalnej niewypłacalności.

Wygenerowany wówczas przez wrogie państwo atak typu „haktywizm", polegający na masowej podmianie treści na stronach www banków, może promować tezy o upadku systemu finansowego w Polsce. Promowane w mediach społecznościowych podrobione wypowiedzi ekspertów, w tym z wykorzystaniem technologii „deep fake", sugerujące zasadność „run'u na bankomaty" mogą doprowadzić do źle prezentujących się w mediach kolejek po pieniądze oraz naturalnego wyczerpania zasobów gotówki. To jeszcze bardziej podgrzewać będzie atmosferę.

Jednocześnie przeprowadzony atak DDoS na strony bankowości elektronicznej, połączony ze zdecydowanym zwiększeniem zainteresowania ze strony klientów chcących sprawdzić stan środków, doprowadzić może do uniemożliwienia dostępu do systemów bankowych. Dalsze podbijanie zagadnienia będzie już wówczas mieć miejsce automatycznie.

Insider + zaszyfrowanie danych + phishing

W gorącym dla banku momencie, jak na przykład w okresie przedświątecznym, insider pracujący w banku, w wyniku szantażu lub przekupstwa, pomoże zorganizowanej grupie przestępczej w zaszyfrowaniu danych. Podejmowane w trakcie negocjacji okupu próby odtworzenia kończyć się będą niepowodzeniem, gdyż przestępcy uzyskają wcześniej stały dostęp do sieci wewnętrznej z wykorzystaniem nielegalnie wpiętego modemu i będą skutecznie torpedować wysiłki. Będzie to bardzo trudne do zidentyfikowania przez zespoły IT i bezpieczeństwa.

Fakt incydentu zostanie bezzwłocznie zidentyfikowany przez użytkowników, którzy nie będą w stanie korzystać ze zgromadzonych środków finansowych. W szczególności bolesne to będzie dla firm, które nie będą w stanie terminowo wypłacić wynagrodzenia. Narzekania prawdopodobnie będzie można bezzwłocznie zidentyfikować w mediach społecznościowych.

Przestępcy wykorzystają to do masowego rozsyłania pracownikom, zidentyfikowanym poprzez media społecznościowe, ukierunkowanego phishingu z oczekiwaną informacją, np. dotyczącą możliwości uzyskania zaliczki na poczet wynagrodzenia po zalogowaniu się na podrobionych przez przestępców stronach www – imitujących strony innych banków. Dzięki temu przestępcy masowo gromadzić mogą dane uwierzytelniające, dodawać kontrolowane przez siebie rachunki słupów jako zaufane oraz rozpoczynać kradzież środków finansowych.

W takiej sytuacji może nastąpić przerwanie funkcjonowania procesów w banku, można spodziewać się konieczności zapłaty okupu lub znacznych sum związanych z obsługą incydentu, można spodziewać się pogorszenia współpracy z firmami-klientami, a ich pracownicy stracą środki finansowe. Żal może przełożyć się na cały sektor, który nie był w wystarczający sposób odporny na zmasowane ataki.

Podmiana stron www + SIM swapping + BGP Highjacking

Absolutnie nieprawdziwa wiadomość o utracie płynności przez jeden z głównych banków zostanie umieszczona po **podmienieniu strony www** organizacji bankowej jak BFG czy ZBP – niewystarczająco zabezpieczonej i przetestowanej pod kątem bezpieczeństwa. Mimo, że szybko zostanie usunięta, zostanie wcześniej zarchiwizowana przez szereg internautów. Farma botów będzie podbijać temat uzupełniony o sugestie, że informacja zniknęła, gdyż została ujawniona przypadkowo i fatalna kondycja finansowa banku powinna pozostać tajemnicą. Powstałe na tej bazie teorie spiskowe będą zyskiwać coraz większą popularność. W odpowiednim momencie atakujący uzupełnią ją o kolejną nieprawdziwą informację, że bank planuje uniemożliwić wykonywanie przelewów. Powinno to spowodować masową chęć zalogowania się do bankowości online celem wykonania przelewu.

Równocześnie w wyniku ataku **SIM swapping** przestępcy spróbują wyprowadzić środki finansowe ze strony influencerów. Opisywane przez nich w mediach społecznościowych wzburzenie po kradzieży, samodzielnie podbijające zasięgi, dodatkowo przekona kolejnych klientów do próby transferu pieniędzy.

W tym momencie przestępcy przeprowadzą atak **BGP Highjacking,** by przekierować ruch na podrobioną, kontrolowaną przez przestępców stronę. Poddenerwowani internauci widząc podobny wygląd strony i widząc certyfikat TLS nie będą patrzeć na jego szczegóły, lecz bezzwłocznie będą próbować dokonać przelewów. To powinno pozwolić wyprowadzić znaczne sumy na rachunki kontrolowane przez przestępców.

Ponieważ oszukani internauci nie będą korzystać z nieprawdziwych odnośników, jak to ma miejsce w przypadku ataków phishingowych, lecz samodzielnie będą wpisywać adres banku w pasku przeglądarki, ich frustracja będzie narastać, prowadząc do gwałtownego zniszczenia wizerunku, co w związku z uszczupleniem środków finansowych banku naprawdę doprowadzić może do kryzysu.

Sposoby identyfikowania kampanii informacyjnych

Zwalczanie kampanii dezinformacyjnych jest zagadnieniem złożonym, stąd konieczne jest spojrzenie na nie z kilku perspektyw. *Reagowanie* na takie kampanie wchodzi w zakres odpowiedzialności zespołów Public Relations (PR), które powinny koncentrować się na bezzwłocznej reakcji na zdarzenie. Zmieniające się otoczenie i idące za tym inne oczekiwania klientów powodują, że szybkość reakcji może mieć większy wpływ niż kompletność odpowiedzi na zarzuty, oszczerstwa lub dezinformację.

W niniejszym rozdziale chcemy podkreślić kwestię *prewencji,* czyli zapobiegania takim kampaniom. Z jednej strony kampanie dezinformacyjne mogą być absolutnie nieprawdziwe i kłamliwe. W takiej sytuacji zaprezentowanie faktów odpowiednio szerokiej audiencji jest kluczowym sposobem reagowania, które nie powinno być szczególnie trudne, choć może zająć czas.

Zdecydowanie gorzej wyglądać będzie sytuacja w przypadku, gdy kampanie dezinformacyjne silnie opierać się będą na rzeczywistych zdarzeniach. Faktach, którym nie można zaprzeczyć, lecz które zostały przeinaczone i ukazane w fałszywym świetle. Im „ciekawsze" będzie rzeczywiste zdarzenie, które zostanie wykorzystane w kampanii, tym trudniej będzie organizacji walczyć z „łowcami teorii spiskowych". Coraz łatwiej się na nich natknąć w internecie i mają coraz większy wpływ na kształtowanie opinii publicznej. Takie rzeczywiste zdarzenia, będące przyczynkiem do zbudowania na ich podstawie kampanii dezinformacyjnych, określane będą jako *„prowokatory*".

4.1. Prowokatory kampanii dezinformacyjnych

Działania w zakresie dezinformacji mają przede wszystkim charakter wpisów w mediach społecznościowych, na portalach informacyjnych, wypowiedzi w tradycyjnych mediach czy też masowo przesyłanej korespondencji. Innymi słowy bardzo rzadko kojarzą się z cyberatakami. W niniejszym rozdziale chcemy zwrócić uwagę na to, że różnego rodzaju błędy, awarie oraz ataki mogą służyć za doskonałe *prowokatory*. Cyberataki mogą zostać wykorzystywane do uwiarygadniania nieprawdziwych i zmanipulowanych tez. Stąd też, w celu ograniczania dezinformacji, niezbędne jest jeszcze większe położenie nacisku na zwiększanie odporności systemów teleinformatycznych.

Autorzy chcą zwrócić uwagę, że zaproponowana na kolejnych stronach lista scenariuszy nie wyczerpuje zagadnienia. Niemniej na podstawie analiz znanych incydentów oraz obserwacji trendów uważamy, że są to zagadnienia, na które należy zwrócić szczególną uwagę. Jednocześnie jesteśmy świadomi, że niektóre z podawanych przykładów mogą być umieszczone w kilku z opisywanych kategorii. Związane jest to z tym, że przestępcy, po sforsowaniu zabezpieczeń, mają wiele możliwości dalszych działań. Przykłady umieszczaliśmy więc w najbardziej charakterystycznych kategoriach.

4.1.1. Ataki odmowy dostępu

Ataki typu „Distributed Denial of Services" (**Ataki DDoS**) są powszechnie stosowanym narzędziem wykorzystywanym w przypadku nieuczciwej konkurencji, do szantażu, a także jako narzędzie destrukcyjne. W zależności od rodzaju polegają na generowaniu zmodyfikowanych pakietów, które mogą wysycić łącze lub też generowaniu zapytań tak bardzo obciążających serwery, że zaprzestaną one pracy. We wszystkich przypadkach skutkiem ataku jest uniemożliwienie dostępu użytkowników do istotnych zasobów. Przeprowadzenie ataku jest tanie oraz wymaga stosunkowo niewielkich umiejętności technicznych. Zazwyczaj nie są długotrwałe, choć nie ma technicznych przeszkód, by trwały całymi dniami.

Długotrwały atak – lub krótszy, ale realizowany w dobrze dobranym momencie – może zostać wykorzystany do potwierdzenia tez rozgłaszanych przez adwersarzy. Bardzo dobrze tym samym mogą służyć poparciu tez o niewypłacalności czy o zamknięciu banku w związku z aferami finansowymi. To może skutkować panicznymi ruchami klientów. Trzeba bowiem pamiętać, że takie ataki są bezzwłocznie widoczne dla społeczeństwa i tym samym najprawdopodobniej zostaną bezzwłocznie wychwycone przez media i nagłośnione. Zmasowane zainteresowanie sprawą przez zaniepokojonych klientów dodatkowo spotęguje atak DDoS.

4.1.2. Modyfikacja systemów bankowych

Udane **włamania do systemów bankowych** są rzadkie, lecz kilkakrotnie miały już miejsce w polskiej historii. Niewykluczone tym samym, że podobny incydent ponownie będzie mieć miejsce. Gdy większe z banków mają swoje zabezpieczenia przygotowane na bardzo wysokim poziomie, mniejsze nie mają tak potężnych środków finansowych, by budować kilkudziesięcioosobowe zespoły eksperckie. Stąd pojawiają się oszczędności, które mogą negatywnie wpłynąć na bezpieczeństwo banku. Włamanie, którego skutkiem byłoby ujawnienie informacji, ich modyfikacja lub przerwanie ciągłości funkcjonowania systemów, może z kolei stać się przykładem uwiarygodniającym tezy stawiane przez adwersarzy.

Szczególnie należy w tym momencie zwrócić uwagę na ryzyko ataku typu **„supply chain"**, czyli ataku wykorzystującego zasoby należące do innego – zaufanego partnera. Organizacje, w tym banki, bardzo często korzystają z pomocy

podwykonawców, z którymi wymieniają się na bieżąco danymi, niekoniecznie stanowiącymi tajemnicę bankową. W zdecydowanej większości przypadków znacznie łatwiej będzie przestępcom przełamać zabezpieczenia takich podmiotów. W przypadku, gdy mają one zestawione tunele VPN, otwiera to przestępcom drogę do sieci wewnętrznej banku.

Specyficznym rodzajem modyfikacji systemów bankowych jest **zaszyfrowanie danych** w celu wymuszenia okupu czy zniszczenia. Niekiedy działania te są wykonywane przez zorganizowane grupy przestępcze, bywają jednak motywowane politycznie.

Ujawnione rzeczywiste próby przełamania bezpieczeństwa systemów bankowych, zakończone modyfikacją danych, mogą bezpośrednio popierać potencjalne tezy agresorów o słabości całego systemu bankowego, bardzo utrudniając jakąkolwiek możliwość rzetelnej obrony.

4.1.3. Ujawnianie poufnych informacji wewnętrznych

Banki posiadają w swoich systemach informatycznych informacje pozwalające bezpośrednio lub pośrednio wnioskować na temat działalności prominentnych osób oraz ważnych organizacji. Mogą to być na przykład informacje o wychodzących i przychodzących przelewach, dokumenty przekazywane w związku z procedurami AML, wnioski kredytowe. Mogą one w nieautoryzowany sposób opuścić systemy informatyczne w wyniku celowego ataku, ale również w przypadku błędu pracowników (np. testowania nowych wersji systemów z wykorzystaniem danych produkcyjnych) lub ich skopiowania przez osobę z wewnątrz organizacji (tzw. „insidera"). Takie nieautoryzowane **ujawnianie poufnych informacji wewnętrznych** może być wykorzystywane do dyskredytacji klientów lub samych instytucji finansowych, które, jak pokazują wycieki, niekiedy nie w pełni przestrzegają własnych kodeksów etycznych i obowiązujących przepisów prawa. Informacje mogą być ujawniane w całości lub też pojedynczo w celu realizacji wcześniej założonych celów.

Przy tej okazji chcemy zwrócić uwagę na szczególny problem z tzw. „**insiderami**", czyli osobami z wewnątrz. Pracownicy organizacji posiadają często nadmierny dostęp do danych w organizacji – szczególnie widoczny przez pryzmat nieprecyzyjnie zarządzanych dostępów do współdzielonych dysków i folderów. Czy to kierując się przesłankami etycznymi, czy finansowymi, czy nawet zemstą – pracownicy i współpracownicy potrafią publikować bardzo niewygodne dane, świadomie łamiąc przepisy dotyczące ochrony tajemnicy bankowej. Ich działanie szczególnie jest potęgowane przez tendencję do przechowywania danych latami – na wszelki wypadek. Łatwo dostępne archiwa potrafią być pomocne, ale w ręku przestępcy stają się niezmiernie groźne. Takie osoby z wewnątrz potrafią też czy to w wyniku groźby, czy chęci osiągnięcia korzyści finansowej współpracować z przestępcami w różnym zakresie.

Masowe ujawnienie informacji finansowych będzie bardzo boleśnie odczuwalne przez klientów banku. Każdy z „bohaterów" poczuje się bezpośrednio dotknięty. Liczyć się więc należy z bardzo silną negatywną reakcją, skierowaną w stronę banku jako instytucji, a być może nawet bezpośrednio jego przedstawicieli. Należy się również spodziewać teorii spiskowych powstałych dookoła zagadnienia permanentnej inwigilacji.

4.1.4. Przejmowanie kont klientów

Fałszywe bramki płatności czy strony banków, mimo że w ostatnich miesiącach są zauważalnie mniej „popularne" wśród cyberprzestępców, co roku prowadzą do utraty środków finansowych przez tysiące osób. Pojawiają się fale ataków typu **phishing**, które przekierowują klientów na oszukańcze strony lub instalują szkodliwe oprogramowanie typu RAT (ang. remote access trojan). Szkodliwe oprogramowanie może też być rozpowszechniane przez niebezpieczne strony www, wykorzystując tzw. technikę **wodopoju.** Niezaktualizowane stacje robocze internautów, łącząc się z popularną stroną (np. portalem finansowym), mogą zostać zainfekowane, ujawniając przestępcom dane uwierzytelniające do systemów bankowych.

Bardzo niepokojącym zjawiskiem jest coraz szybciej się rozpowszechniający „Caller ID spoofing" (tzw. **CLI Spoofing**). Mimo, że wymaga indywidualnego podejścia do każdej przyszłej ofiary, skuteczność ataków bywa potężna. Oszustwo podlega na modyfikowaniu tekstu wyświetlającego się nieświadomej ofierze na telefonie komórkowych, tak by wskazywał zaufane źródło, jak KNF, ZBP, BIK czy dział bezpieczeństwa banku. Atakujący wywierają wówczas presję na ofierze, by zainstalowała któryś ze znanych programów wspierających zdalny dostęp (np. Anydesk czy VNC), a po uzyskaniu zdalnego dostępu kradną oszczędności życia. W takich przypadkach ofiara bezpośrednio może winić bank, którego to „pracownik" dokonał kradzieży, lub też rozpowszechniając tezę, że bank dopuścił do „shakowania" swojego systemu i przestępcy dzwonili z wewnętrznej infrastruktury banku. Podobnie jak w poprzednim scenariuszu, ofiary często mogę być przekonane o braku własnej winy.

Jeszcze inny scenariusz masowego przejmowania danych uwierzytelniających związany może być z przejęciem ruchu internetowego wykorzystując **BGP Hijacking**.

Zdarzenia polegające na nieprawidłowym rozgłoszeniu adresów IP zdarzają się kilkaset razy w roku. W większości przypadków dzieje się to przypadkowo, niemniej należy wiedzieć, że taki celowy atak mógłby być bardzo szkodliwy, gdyż istniałaby możliwość wystawiania prawdziwych certyfikatów SSL/TLS, co po podstawieniu spreparowanej witryny banku mogłoby doprowadzić do masowego wycieku danych uwierzytelniających.

Ostatnim z tematów, który wydaje się niezbędny do zasygnalizowania w tej sekcji jest **„SIM swapping"**, czyli przejmowanie numerów telefonicznych należących do bardziej majętnych osób oraz wykorzystywanie ich do podszywania się pod rzeczywistych klientów – użytkowników aplikacji bankowych. Mimo, że zagadnienie to ma swoje źródła w oszukiwaniu operatorów telekomunikacyjnych, to sektor finansowy jest de facto władny, by się przed nimi ochronić, modyfikując procesy wewnętrzne oraz wymuszając inny przepływ informacji z operatorami telefonii komórkowej.

Ponieważ w znacznej części opisanych powyżej spraw widoczne są przynajmniej pewne zaniedbania po stronie użytkowników, banki niekoniecznie mogą być skłonne do uwzględniania ich reklamacji. Z oczywistych powodów potrafi to prowadzić do frustracji poszkodowanych, przekonanych o niesprawiedliwości, a to może być z łatwością rozpowszechnione i wzmocnione. Takie negatywnie nastawione grupy poszkodowanych łatwiej będzie zmanipulować i przekonać do wspierania działań agresora.

4.1.5. Podmiana stron www

Mimo, że **podmiana stron www** (tzw. „defacement") zazwyczaj kojarzona jest ze stosunkowo niegroźnym zjawiskiem haktywizmu, może jednak prowadzić do znacznych niepokojów społecznych. Może to bowiem dotyczyć zarówno pojedynczych banków, jak i większych grup czy zrzeszeń. Niekiedy wręcz na masową skalę. Zazwyczaj haktywizm dotyczy kwestii politycznych lub światopoglądowych, jednak łatwo można wyobrazić sobie scenariusze, w których na stronach banków i instytucji finansowych pojawiać się będą oszczercze informacje na temat stanu polskiej gospodarki.

Mimo, że podmiana witryny internetowej nie wydaje się szczególnie groźna, może zostać wykorzystana do ośmieszenia i zdyskredytowania organizacji finansowych, doprowadzając nawet do widocznych ruchów personalnych. To z kolei może nawet mieć wpływ na prowadzoną politykę organizacji.

4.1.6. Manipulowanie inwestorami

Możliwość inwestowania w akcje na praktycznie całym świecie ułatwiła grupom oszustów organizowanie się. Na zamkniętych forach i grupach „inwestorzy" organizują się, by **manipulować kursem akcji spółek giełdowych**. Z jednej strony dysponują zauważalnym kapitałem, z drugiej strony mogą starać się wprzęgać w działania nieświadomych inwestorów. Wykorzystują do tego fikcyjne porady inwestycyjne czy „spreparowane wycieki", które mają sugerować spodziewane wzrosty lub spadki kursów.

Zazwyczaj tego typu działania mają na celu zwiększanie zysku zorganizowanych grup. Jednak można sobie również wyobrazić scenariusz, w którym celem będzie nie zysk, lecz osłabienie poszczególnych spółek lub nawet sektorów gospodarki.

Zjawiskiem, na które również warto zwrócić uwagę, są **oszustwa inwestycyjne**. Masowe wycieki adresów e-mail mogą stanowić doskonałą pomoc dla oszustów poszukujących łatwowiernych osób, pragnących szybkiego zarobku. Rozsyłanie wskazówek inwestycyjnych może pomóc przestępcom kraść pieniądze, sprzedawać nic niewarte instrumenty lub manipulować kursem akcji. Będzie to tym łatwiejsze, gdy ujawnione w przypadku wycieku adresy e-mail będą pochodziły z serwisów zajmujących się finansami i inwestycjami. Przestępcy będą wówczas mieć możliwość szybkiego dotarcia do potencjalnej grupy docelowej.

O tym, jak masowe jest pragnienie szybkich pieniędzy, świadczy skala afer finansowych, które mieliśmy w Polsce. Analiza tych i podobnych, lecz mniejszych, zdarzeń jednoznacznie pokazuje, że bardzo łatwo jest wykorzystywać te tematy do punktowania prawdziwych bądź fałszywych słabości nadzoru nad polskim systemem finansowym. Jak pokazały doświadczenia z ostatnich lat, agresja osób poszkodowanych kierowana jest w znacznym stopniu w kierunku organów nadzoru, podważając ich kompetencje.

4.1.7. Wykorzystanie kontrowersyjnych tematów

Świat XXI wieku łaknie sensacji, co też skwapliwie jest wykorzystywane przez media czy różnej maści influencerów. Sensacyjne lub kontrowersyjne wiadomości mogą również posłużyć do uwiarygadniania tez stawianych przez specjalistów od dezinformacji. Kontrowersje dotyczące płynności poszczególnych banków, korupcji i nieprawidłowości w organach nadzoru, niewłaściwie wyliczanych wskaźników gospodarczych itp. mogą być rozdmuchiwane i podsycane. Można sobie jednak równie dobrze wyobrazić sytuację kreowania zupełnie fikcyjnych „newsów". Warto zauważyć, że zbyt późne lub nieumiejętne próby sprostowania fałszywych wiadomości również mogą być wykorzystane przez atakujących, uwiarygadniając tezy o próbie „ukrycia prawdy" sprzed społeczeństwem.

4.2. Narzędzia prewencyjne

Organizacje sektora finansowego są znane z tego, że stosują najbardziej skuteczne z zabezpieczeń technicznych, informatycznych i organizacyjnych. Nieustanny rozwój cyberprzestępczości determinuje jednak konieczność stałego doskonalenia rozwiązań i wyszukiwania odpowiedzi dla przyszłych zagrożeń.

W niniejszym rozdziale Autorzy zwracają uwagę na wybrane zabezpieczenia znane ze świata IT, które mogą wykazać swoją skuteczność również w przypadku zwalczania dezinformacji. Równocześnie proponują rozwiązania, które jeszcze nie są powszechnie stosowane, lecz warte są rozważenia. Spodziewać się bowiem należy nieustającego, znacznego wzrostu zarówno ilości ataków, jak i poziomu ich wyrafinowania. A takie ataki mogą z powodzeniem służyć do uwiarygadniania praktycznie dowolnych działań dezinformacyjnych wymierzonych w polski system bankowy.

Zaproponowane rozwiązania zostały zmapowane na *prowokatory* opisane w poprzednim podrozdziale. Tym samym łatwiej będzie, bazując na bieżącym stanie zabezpieczeń w bankach, ustalić oczekiwany priorytet wdrażania zabezpieczeń, jak również wskazać dodatkowe obszary wymagające weryfikacji w ramach prowadzonych audytów wewnętrznych i kontroli.

O sile systemu bankowego świadczy bowiem jego wielowarstwowa struktura. Zabezpieczenia powinny być codziennym elementem pracy pracowników, powinny stać się integralną częścią procesów operacyjnych. Ich skuteczność powinna być zapewniana zarówno przez kierowników liniowych, jak również przez wyspecjalizowane działy zajmujące się różnymi aspektami zapewniania bezpieczeństwa. Skuteczność takiego nadzoru powinna być weryfikowana przez audyt wewnętrzny przekazujący kierownictwu banku rzetelne informacje o kondycji podmiotu. A całokształt mechanizmów nadzorczych powinny okresowo weryfikować zewnętrzne kontrole potwierdzające zgodność z ustanowionymi regulacjami.

Tabela 4.1. Narzędzia przeciwdziałające wybranym scenariuszom

Zabezpieczenie / Scenariusz	System AntyDDoS	Testy penetracyjne	Utwardzenie konfiguracji ruterów i urządzeń brzegowych	Web Application Firewall (WAF)	Segmentacja sieci wewnętrznej	Walidacja tras (ROV)	Monitoring reputacji	Silne przeglądy bezpieczeństwa	Budowanie świadomości	Utwardzanie procesów wewnętrznych	Monitoring podziemia przestępczego
Atak DDoS	X	X	X	X				X			**X**
Włamanie do systemów bankowych		X	X	X	X		X	X			**X**
Atak „supply chain”		X	X		X			X		X	**X**
Zaszyfrowanie danych		X	X	X	X		X	X	X	X	**X**
Wodopój		X		X			X	X			**X**
Ujawnianie poufnych informacji wewnętrznych								X	X	X	
Insider		X			X			X		X	
Phishing					X		X	X	X	X	**X**
Caller ID spoofing									X	X	**X**
BGP Highjacking			X			X					
SIM swapping									X	X	
Podmiana stron www		X	X	X			X	X			**X**
Manipulacja kursem akcji spółek giełdowych									X		**X**
Oszustwa inwestycyjne									X		
Wykorzystanie kontrowersyjnych tematów									X		

Opracowanie własne

4.2.1. Systemy AntyDDoS

Systemy AntyDDoS są wdrożone w zdecydowanej większości, jeżeli nie we wszystkich polskich bankach. Rosnący wolumen ataków przekraczający coraz częściej Gbps wymaga jednak tego, by systemy te były wdrożone poprawnie. Zabezpieczenia przed tym rodzajem ataków zostały ostatnio opisane w dokumencie „Dobre praktyki w zakresie przeciwdziałania atakom DDoS”[84] wydanym przez CSIRT Komisji Nadzoru Finansowego (KNF). Wdrażając ochronę należy uwzględniać zaproponowane w raporcie priorytety uwzględniające charakterystykę wykupionych łącz internetowych. Szczególną uwagę chcemy zwrócić na wskazywane w tym dokumencie kwestie potrzeby ochrony przed atakami aplikacyjnymi (czyli tzw. ataki warstwy 7). W przyszłości spodziewać się należy znacznego wzrostu zaawansowania tych ataków.

Skuteczność wdrożonych rozwiązań należy okresowo weryfikować, aby – jak w przypadku innych usług – mieć pewność, że spełniają pokładane nadzieje. Wykonuje się to podczas **testów rozwiązań AntyDDoS**, które polegają na przeprowadzaniu kontrolowanego ataku. W tym momencie podkreślić jednak należy pominiętą w dokumencie KNF kwestię rzetelnego zdefiniowania maksymalnych akceptowalnych czasów niedostępności chronionych usług, które mają bezpośredni wpływ na koszt. Zapewnienie dostępności systemów bankowych na poziomie 100% jest praktycznie niemożliwe. Niemniej oczekiwana średnia dostępność oraz maksymalne czasy niedostępności powinny zostać określone i monitorowane.

4.2.2. Testy penetracyjne

Wykonywanie testów penetracyjnych powinno być standardem w bankach, gdyż jest zdefiniowane w dokumencie „Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach”[85] Komisji Nadzoru Finansowego. Gdy większe z banków są w tym obszarze bardzo dobrze zorganizowane, w mniejszych prace potrafią ograniczać się jedynie do identyfikacji podatności. Można zaobserwować też niekiedy znaczne problemy z późniejszym wdrażaniem rekomendacji.

Testy penetracyjne powinny obejmować swoim zakresem systemy bankowości elektronicznej i poszczególne interface z innymi systemami i organizacjami, zabezpieczenia brzegu sieci (w tym VPN), skuteczność segmentacji sieci wewnętrznej, poprawność zabezpieczenia aplikacji w sieci wewnętrznej, serwerów i stacji roboczych. W większych z organizacji potwierdza się niekiedy też skuteczność detekcji, czyli weryfikuje, czy symulowane ataki zostały poprawnie zidentyfikowane przez stosowane systemy monitoringu.

Autorzy pragną podkreślić, że oprócz identyfikacji błędów konfiguracyjnych i podatności, które skutkować mogą utratą integralności i poufności, wykorzystując testy penetracyjne, można identyfikować również ryzyka dotyczące dostępności aplikacji webowych – weryfikując odporność udostępnionych usług na wysycenie zasobów, czyli na ataki typu DoS (Denial of Service).

4.2.3. Utwardzanie konfiguracji ruterów i urządzeń brzegowych

Standardowa konfiguracja urządzeń bardzo często pełna jest obszarów, które mogą zostać niewłaściwie wykorzystane. Stąd tak istotne staje się bazowanie na standardach utwardzania konfiguracji (tzw. hardeningu). Instalując niezbędne poprawki, wyłączając niepotrzebne usługi, zmieniając standardowych użytkowników itp. można utrudnić atak.

Skuteczność przeprowadzonego utwardzania weryfikuje się przy okazji testów penetracyjnych. Standardy konfiguracji lub wręcz standardowe obrazy, potrafią bardzo uporządkować infrastrukturę.

4.2.4. Web Application Firewall (WAF)

Rozwiązania klasy WAF mają na celu identyfikowanie oraz powstrzymywanie ataków na aplikacje webowe. Autorzy pragną zwrócić przy tej okazji uwagę na kilka kwestii. Przede wszystkim na potrzebę zapewnienia stałej współpracy pomiędzy zespołami zajmującymi się rozwojem chronionych aplikacji a osobami utrzymującymi to zabezpieczenie. Rozwiązania te spełniają pokładane nadzieje wyłącznie, gdy zmiany stron www są bezzwłocznie odwzorowane w konfiguracji systemu WAF. W przypadku gdy funkcjonalności będą rozwijane szybciej, w sposób niezsynchronizowany z zabezpieczeniami, WAF gwałtownie obniża swoją skuteczność. Należy też podkreślić, że systemy WAF, tak jak i inne systemy bezpieczeństwa, w szczególnych okolicznościach można ominąć. Ważne tym samym, by nie były one jedyną linią obrony i by chroniona infrastruktura była poprawnie utwardzona.

Warto zauważyć, że rozwiązania WAF mogą stanowić kolejną warstwę ochrony przed aplikacyjnymi atakami DDoS.

[84] https://www.knf.gov.pl/knf/pl/komponenty/img/Dobre%20praktyki%20w%20zakresie%20przeciwdzia%C5%82ania%20atakom%20DDoS_77247.pdf

[85] https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf

4.2.5. Segmentacja sieci wewnętrznej

Wdrożenie odseparowanych podsieci stanowi podstawowy sposób ograniczenia zasięgu udanych ataków i tym samym ich skutków. Należy liczyć się z tym, że przestępcom uda się prędzej czy później sforsować zabezpieczenia brzegowe – czy w wyniku wykorzystania podatności, oszukania pracownika, wprowadzenia „insidera" czy wtargnięcia bokiem wykorzystując infrastrukturę gorzej zabezpieczonego podwykonawcy (tzw. atak „supply chain"). Aby zminimalizować związane z tym szkody i zyskać więcej czasu na identyfikację takiego zdarzenia należy unikać tzw. „płaskich sieci", które umożliwiają atakującemu swobodne przechodzenie pomiędzy urządzeniami końcowymi czy podsieciami (tzw. „lateral movement"). Przemyślane relacje zaufania, wymuszane na wewnętrznych urządzeniach sieciowych, bardzo skutecznie ograniczą skalę ataku. A logowanie i monitorowanie tego typu ruchu pozwoli zidentyfikować atak, zanim poczyni nieodwracalne szkody.

4.2.6. Walidacja tras (ROV)

Walidacja tras BGP jest stosunkowo nowym mechanizmem stosowanym przez niektórych operatorów telekomunikacyjnych. Polega na podpisywaniu adresów IP z wykorzystaniem infrastruktury klucza publicznego, co utrudnia próby masowego przejęcia ruchu. Mimo, że rozwiązania chroniące przed atakami na protokół BPG wciąż są rozwijane, pierwsze skuteczne mechanizmy zostały opracowane w ramach międzynarodowej inicjatywy MANRS[86]. Mimo, że nie są jeszcze znane Autorom przypadki wykorzystania przejętego w ten sposób ruchu, znane są przypadki nieautoryzowanego przejęcia całej komunikacji internetowej przychodzącej do niektórych z banków.

4.2.7. Monitoring reputacji

Pewne wskaźniki sugerujące, że organizacja może być w nadchodzącym czasie narażona na incydent, można zidentyfikować stosując różne formy monitoringu reputacji. Weryfikacja baz z wyciekami danych uwierzytelniających pod kątem haseł należących do banku pozwala na zablokowanie ataków wykorzystujących udostępnione w internecie zasoby – szczególnie to może być istotne w momencie, gdy skradzione zostaną dane uwierzytelniające administratorów.

Bieżąca obecność w internetowym podziemiu, z wykorzystaniem usług typu Threat Hunting pozwala na wcześniejsze informacje o TTP (ang. Tools, Technics & Procedures) grup przestępczych szczególnie zainteresowanych sektorem finansowym i tym samym bieżące tworzenie nowych reguł korelacyjnych.

Może się wreszcie zdarzyć, że podsłuchanie rozmowy toczonej na którymś z forów pozwoli zidentyfikować, że organizacja będzie stanowić następny cel ataku i tym samym się na niego przygotować. Są to bardzo rzadkie sytuacje, niemniej zdarzają się. Z kolei monitorowanie rejestrowanych domen czy wystawianych certyfikatów TLS jest w stanie pomóc we wcześniejszej identyfikacji kampanii phishingowych.

W sytuacji, gdy wiele czynności wykonywanych w Internecie przez banki jest na bieżąco śledzone przez grupy przestępcze, należy zdaniem Autorów co najmniej rozważyć śledzenie również i przestępczej działalności.

4.2.8. Silne przeglądy bezpieczeństwa

Kompleksowe i regularne przeglądy wydają się być najskuteczniejszym sposobem przeciwdziałania atakom – pod warunkiem rzetelnego wdrażania późniejszych rekomendacji. W najbardziej namacalny sposób wykazują swoją wartość podczas doskonalenia infrastruktury wewnętrznej, niemniej można je wykorzystać do doskonalenia ochrony przed wszystkimi scenariuszami omawianymi w niniejszym raporcie. W każdym bowiem przypadku mogą pomóc w doskonaleniu reakcji na niepokojące zdarzenia – niezależnie czy dotyczyć będzie ono banku czy jego klientów i innych interesariuszy. Ważne jednak, by na bieżąco zasilały rejestry ryzyk i tym samym były zarządzane w sposób uporządkowany.

Zagadnieniem, które warto w tym momencie zaznaczyć, jest rekonesans cyberbezpieczeństwa, przeprowadzany niekiedy przy okazji testów penetracyjnych. Usługa polega na spojrzeniu na organizację okiem przestępcy i zidentyfikowanie obszarów, które pomogłyby w przeprowadzeniu udanego cyberataku. Taka analiza dodatkowo pomoże organizacji w identyfikacji słabych punktów.

4.2.9. Budowanie świadomości

Znaczna część cyberataków ma swój początek w niewystarczającej czujności klientów i pracowników. Mając świadomość tego faktu banki powinny nałożyć szczególny wysiłek, by docierać do możliwie szerokich grup społecznych z przekazami dotyczącymi tego jak wykrywać ataki, jak im przeciwdziałać oraz jak reagować w sytuacji, gdy jednak będą mieć miejsce.

Stąd płynie potrzeba kontynuacji wysiłków w tym zakresie i promowania najlepszych praktyk. Komunikacja powinna przybierać różne formy. Nie powinna

[86] https://www.manrs.org/

być nachalna, by nie zniechęcać do zapoznawania się z jej treścią. Powinna być prowadzona przez poszczególne banki, jak również w sposób scentralizowany przez organizacje takie jak ZBP. Powinna być prowadzona także z wykorzystaniem innych podmiotów jak fundacje i stowarzyszenia. Powinna uwzględniać osoby wykształcone i niewykształcone, seniorów i młodzież.

To, co jednak wydaje się najważniejsze, to promowanie dobrych praktyk poprzez dawanie dobrego przykładu. Szyfrowanie przez banki dokumentów bardzo słabymi hasłami jak numer Pesel; stosowanie w komunikacji trudnych do natychmiastowego zweryfikowania QR kodów i skrótowców; wysyłanie komunikatów sms zawierających linki, które trudno zweryfikować; niejasne sposoby potwierdzania tożsamości dzwoniących konsultantów – wszystkie tego typu zbyt często obserwowane sytuacje degradują wysiłki osób odpowiedzialnych za bezpieczeństwo. Jeśli bowiem „normalną" praktyką stosowaną w komunikacji przez banki jest przekonywanie do klikania w każdy link w sms czy wiadomości e-mail lub też konieczność podania szczegółowych danych osobowych w sytuacji, gdy niespodziewanie zadzwoni do nas konsultant z nową ofertą, nie można się dziwić skuteczności tego typu działań w wykonaniu przestępców.

4.2.10. Utwardzanie procesów wewnętrznych

Utwardzenie procesów wewnętrznych jest najbardziej skutecznym z zabezpieczeń, jakie można sobie wyobrazić. Pozwala zmniejszać prawdopodobieństwo pomyłek i skutków awarii. Pozwala również szybciej wykrywać i lepiej reagować na ewentualne ataki.

Banki są coraz bardziej zależne od usług firm telekomunikacyjnych. Stąd wydaje się właściwe zapewnienie coraz silniejszej współpracy w zakresie zwalczania cyberprzestępczości. Wzajemna wymiana informacji o niebezpiecznych stronach i adresach IP może pomóc chronić użytkowników poprzez blokowanie przestępców, podobnie zresztą jak informowanie o wykrywanych kampaniach phishingowych i ich blokowanie po stronie operatora telekomunikacyjnego. Wymiana informacji o wydanych duplikatach kart SIM może z kolei pomóc w zwalczaniu ataków typu SIM swapping. Współpraca z operatorami wykorzystującymi technologię ograniczającą CLI spoofing oraz uporządkowanie procesu weryfikacji konsultantów może pomóc ograniczać zjawisko ataków na BGP.

Te z procesów biznesowych, które mogą skutkować ujawnieniem bardzo cennych informacji, jak również stratami finansowymi, warto rozbudowywać o mechanizmy podwójnej weryfikacji ograniczając możliwość konfliktu interesów. Szczególnie tutaj trzeba zwrócić uwagę na skuteczność procesu nadawania uprawnień. Przede wszystkim w przypadku wertykalnych lub horyzontalnych awansów istnieje duże prawdopodobieństwo popełnienia błędu o istotnych konsekwencjach. Niepełne odebranie poprzednich praw dostępu może umożliwiać ominięcie podwójnej weryfikacji.

Podobnie rosnące zagrożenie widzimy ze strony różnych podwykonawców posiadających dostęp do cennych danych lub dostęp do sieci wewnętrznej banku. To z ich strony można spodziewać się najgroźniejszych w skutkach ataków. To zwiększa jeszcze bardziej potrzebę położenia szczególnego nacisku na poprawność tworzenia kopii zapasowych (również zasobów przetwarzanych w chmurach obliczeniowych) i ich odseparowanie od środowisk produkcyjnych, na zdolność zarządzania ciągłością biznesową oraz umiejętność odtwarzania po katastrofie.

Możliwości doskonalenia procesów można szukać również, a może przede wszystkim, w procesach obsługi klienta. Przykładowo wiele kradzieży środków finansowych z kont wykorzystuje mechanizm, podczas którego wyłudzane są dane uwierzytelniające i kody jednorazowe, by dodać rachunki należące do przestępców do „odbiorców zaufanych". Wprowadzenie mechanizmu „zamka czasowego", który nie będzie zezwalał na to, by bezzwłocznie po dodaniu zaufanego odbiorcy, transferować na to konto większych sum zapobiegnie wielu nieszczęściom i tym samym będzie pozytywnie wpływać na reputację banków. Coraz bardziej zaawansowane wydają się również możliwości płynące z systemów zautomatyzowanej analizy behawioralnej użytkowników systemów online.

4.2.11. Monitoring podziemia przestępczego

Przestępcy zazwyczaj działają w zamkniętych grupach, starając się możliwie chronić informacje na swój temat, jak i te dotyczące przyszłych celów. Ale nie zawsze tak jest. Szczególnie w przypadku haktywizmu, chociaż również w przypadku oszustw inwestycyjnych, można niekiedy zidentyfikować zbliżające się zagrożenie.

Równocześnie usługi typu Cyber Threat Intelligence są w stanie przekazać dość aktualne informacje na temat aktualnych wskaźników kompromitacji (tzw. IoC – Indicator of Compromise) dających namacalne informacje o tym, jak rozpoznać nowe ataki. Dodatkowo, w ramach tego typu usług, można otrzymywać raporty dotyczące działalności oraz technik stosowanych przez najbardziej interesujące z grup przestępczych.

W niniejszym podrozdziale zgromadzono szereg najlepszych praktyk z zakresu cyberbezpieczeństwa. Mimo, że wydawać się to może pobocznym zagadnieniem, tak nie jest. Kampanie dezinformacyjne, by być bardziej skuteczne, powinny być oparte na rzeczywistości. Taką iskrę mogą stanowić różnego rodzaju cyberincydenty. Dowodzą słabości organizacji, są ciekawe i dla osób postronnych i dla mediów, łatwo mogą być pokazane w kontekście różnych teorii spiskowych. Odpowiednio podsycone, cyberincydenty mogą doprowadzić do irracjonalnych zachowań i dewaluacji zaufania do poszczególnych banków lub wręcz całego sektora.

4.3. Reagowanie na kampanie dezinformacyjne

Zagrożenia zdecydowanie należy niwelować w pierwszych etapach, zanim dojdzie do niekontrolowanej eksplozji negatywnych emocji i potencjalnie dalszych działań dezinformacyjnych. Stąd pojawia się potrzeba bieżącego monitorowania mediów, w tym portali społecznościowych. Kampanie dezinformacyjne oraz dyskusje wyolbrzymiające znaczenie *prowokatorów* mogą bowiem pojawiać się w różnych – niekiedy dość przypadkowych – źródłach. Należy więc być obecnym we wszystkich miejscach, w których mogą rozwijać się dyskusje na temat *prowokatorów*.

Bardzo istotna więc będzie przy tym możliwość szybkiego **zidentyfikowania zdarzenia**: czy to wykorzystując API, samodzielnie tworzone „crawlery" przeczesujące dane medium, czy też wykorzystując dane już zindeksowane przez przeglądarki. Wsparciem dla skutecznej identyfikacji będą również narzędzia do ustalania emocji w stylu wypowiedzi. Kluczową umiejętnością nowej – zmieniającej się funkcji PR będzie tym samym umiejętność sprawnego wykorzystywania tych narzędzi i poprawnego dobierania takich parametrów, jak progi istotności.

Umiejętność wyważonego, lecz jednocześnie zdecydowanego i błyskawicznego reagowania na niepokojące zdarzenia z każdym miesiącem staje się coraz bardziej istotna. Klienci żądają natychmiastowych odpowiedzi i nie mają najmniejszych oporów, by publicznie piętnować organizacje, które reagują opieszale. Potrafią też sprawnie organizować znaczne grupy strasząc bojkotem i niszcząc mozolnie budowaną reputację. To, jak pokazano wcześniej, może być wykorzystane do szerzenia dezinformacji. Wydaje się więc, że w nadchodzących latach niezbędne może stać się stałe monitorowanie różnych mediów społecznościowych oraz zapewnienie reakcji na bardziej czy mniej zasadne zarzuty w trybie 24x7x365. Należy się wręcz spodziewać, że to prędkość reakcji – przynajmniej w zakresie przyjęcia zgłoszenia, będzie kluczowym czynnikiem, co stoi w sprzeczności z możliwością kompleksowej analizy i udzieleniem wyczerpującej odpowiedzi. Jednocześnie należy zwracać uwagę na potrzebę indywidualnego traktowania interesantów. Czasy szablonowych odpowiedzi bezpowrotnie minęły. Jednak z pomocą mogą przyjść boty, które można skonfigurować do wspomagania pracy zespołów PR – przynajmniej w zakresie pierwszej reakcji na zgłoszenie. Mogą one bowiem **zarejestrować zdarzenie** oraz **przekazać spersonalizowaną odpowiedź.**

Dopiero po tego typu pierwszej reakcji organizacja może zyskać czas na dalsze weryfikacje. Pierwszym krokiem powinna być **weryfikacja istotności** pod kątem określenia **potencjału masowości**, czyli sprawdzenia, czy miejsce opublikowania informacji lub zaangażowane osoby wskazują na duże prawdopodobieństwo tego, że zdarzenie zostanie nadmiernie nagłośnione. To, czy będzie ono podbijane coraz mniej zależy bowiem od tego, czy bazuje ono na prawdziwej sytuacji, czy jest w pełni fałszywe. W tym kroku weryfikować należy również, czy zagadnienie jest podbijane przez rzeczywiste osoby czy farmy botów. W sytuacji, gdy temat nie zdobędzie popularności, możliwe, że nastąpi jego wyciszenie, więc poza monitorowaniem sytuacji może się zdarzyć, że nie będą potrzebne dalsze czynności i nastąpi **koniec obsługi** zdarzenia.

Gdy spodziewać się jednak należy narastającego zainteresowania tematem i powiększania zasięgów, potrzebne staje się rozpoczęcie dalszych analiz. W pierwszym kroku proponujemy przeprowadzić **analizę prowokatorów**, czyli identyfikację informacji będących postawą do wysnuwanych oszczerstw lub teorii, na podstawie których można będzie potwierdzić, czy **kampania bazuje na rzeczywistych zdarzeniach**, czy jest w pełni zmyślona. W drugim przypadku powinno nastąpić zdecydowane **przekazanie odpowiedzi** ze sprostowaniem i żądaniem zaprzestania rozpowszechniania dezinformacji.

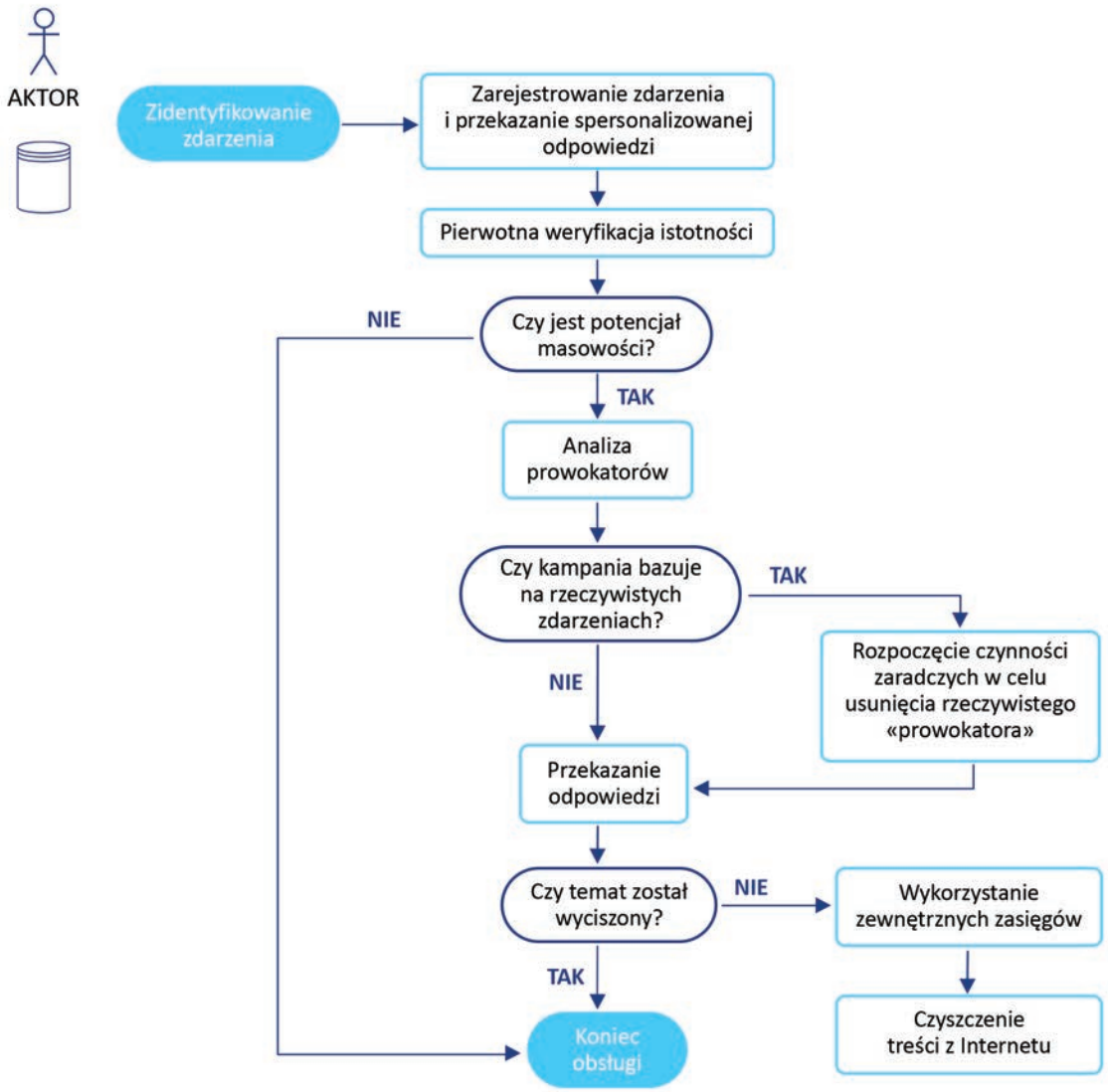
Jednak gdy zdarzenie jest pokłosiem rzeczywistego incydentu, niezbędna staje się aktywacja zespołów zadaniowych, które **rozpoczną czynności zaradcze zmierzające do usunięcia rzeczywistego prowokatora**. Następnie należy **przekazać odpowiedź** z przeproszeniem i merytorycznym wyjaśnieniem sytuacji.

Przekazanie odpowiedzi może okazać się skuteczne, stąd należy zweryfikować, **czy temat został wyciszony**. Jeśli tak, to oznacza, że potencjalna kampania dezinformacyjna została zniszczona w zarodku. Jeśli nie, potrzebne będą dalsze działania, wśród których

wymienić należy **wykorzystywanie zewnętrznych zasięgów**. Mogą w tym być wykorzystywane również inne – konkurencyjne organizacje, które również mogłyby stać się przedmiotem podobnej kampanii i oczekiwałyby wówczas rewanżu. Zdecydowanie w tego typu działania niwelujące należy zaangażować również organizacje zrzeszające, jak ZBP czy KNF. Można nawet rozważyć wykorzystywanie influencerów w przypadku kampanii mających naprawdę masowy zasięg. W takich bowiem przypadkach trzeba będzie zareagować nie tylko prostując dezinformacje blisko źródła, ale również w innych miejscach, w których temat może dopiero być duplikowany. A w tym pomocne będzie możliwe precyzyjne sprofilowanie populacji powiększającej zasięgi, by oddziaływać na całą „bańkę informacyjną", w ramach której funkcjonuje.

W szczególnych wypadkach można zacząć stosować techniki mające na celu **czyszczenie treści z internetu**. Może to mieć postać utrudniania odszukania informacji poprzez różne przeglądarki internetowe, czy współpracę z dostawcami treści – również za pośrednictwem kancelarii prawniczych – w celu skasowania nieprawdziwych informacji.

Przedstawiony opis postępowania przedstawiony został na rysunku 4.1.



Rysunek 4.1 Proces reagowania na kampanie dezinformacyjne
Opracowanie własne

Na zakończenie chcemy podkreślić, że banki i organizacje funkcjonujące w sektorze bankowym powinny przygotować się do przeorganizowania obecnej funkcji PR. W coraz większej ilości przypadków – szczególnie tych związanych z dezinformacją – należy spodziewać się konieczności współpracy z innymi organizacjami – zarówno w kwestii identyfikacji, jak i reagowania na tego typu przypadki. Ze względu na koszty samodzielna troska o wizerunek będzie coraz mniej opłacalna. Coraz bardziej interesujące mogą więc być modele scentralizowane, w tym usługi świadczone przez podmioty sektora bankowego oraz firmy komercyjne.

Skuteczne współdziałanie wielu organizacji i zespołów PR w sytuacji poważnego kryzysu wizerunkowego, wymagać będzie przećwiczenia różnych scenariuszy, co zgodnie z naszą wiedzą nie miało jeszcze w Polsce miejsca. Stąd rekomendujemy rozpoczęcie prac, w rezultacie których przygotowane i przeprowadzone zostaną ćwiczenia reakcji na zmasowaną kampanię dezinformacyjną atakującą polski sektor finansowy.

Propozycja narzędzi do zwalczania kampanii informacyjnych

Powszechna adaptacja najnowszych technologii w telekomunikacji znacząco zmieniła sposób tworzenia i konsumpcji wiadomości. Obecna sprawność sieci i systemów teleinformatycznych oraz wszelkich innych systemów telekomunikacyjnych (np. tych, w których źródłem jest telewizja) zachęca odbiorców informacji do jak najszybszego pozyskiwania jak największej ilości (czasem wręcz sensacyjnych) informacji kosztem sprawdzania faktów i weryfikacji źródeł. Niestety wielorakie zalety wolności słowa i komunikacji bezpośredniej są przyćmione przez nadużywanie cyberprzestrzeni do rozpowszechniania niedokładnych lub wprowadzających w błąd wiadomości.

Jednym z przedmiotów badań prowadzonych w ramach niniejszego projektu jest wroga kampania informacyjna. Dlatego dla porządku terminologicznego niniejszego opracowania przyjęto, iż wroga kampania informacyjna to całokształt uzgodnionych co do celu, zadań, miejsca i czasu operacji informacyjnych prowadzonych przez wrogi podmiot państwowy lub niepaństwowy dla osiągnięcia jego celu strategicznego. Ze względu na swoją istotę wrogie kampanie informacyjne stanowią istotne wyzwanie dla współczesnego sektora bankowego. Jak podaje Beata Tarczydło społeczeństwo jest jedynie informowane, natomiast wnioski konsumenci wyciągają sami[87]. Zatem, jeśli wroga kampania informacyjna jest bardzo dobrze przygotowana i przeprowadzona, wpłynie na świadomość społeczeństwa, które podejmie niepożądane, często nieracjonalne lub chaotyczne działania.

Kampanie informacyjne nie są niczym nowym. Przecież wojenna propaganda prowadzona jest do wywierania wpływu na opinię publiczną przeciwko przeciwnikowi. Jednak rozwój teleinformatyczny społeczeństw przyczynił się do wykorzystania Internetu i mediów społecznościowych do rozpowszechniania kampanii informacyjnych w sektorze finansowym.

Rozdział ten poświęcony został sposobom identyfikowania kampanii informacyjnych, narzędziom oraz technikom pomagającym w weryfikacji i sprawdzaniu faktów oraz pomagających odbiorcom, czytelnikom wiadomości filtrować i eliminować wątpliwe lub wręcz szkodliwe informacje.

5.1. Kampania informacyjna – uwarunkowania środowiskowe

Źródła informacji mają istotny wpływ na ludzi. Ostatnie kilka lat pokazuje, że środki masowego przekazu mogą być skutecznie wykorzystywane do rozpowszechniania dezinformacji. Co więcej, eksperymenty społeczne pokazują, że ludzie często wierzą w niepotwierdzone wiadomości i je rozpowszechniają.

Zdefiniujmy operację informacyjną. Operacja informacyjna to zespół wydarzeń informacyjnych (wiadomości w Internecie i mediach, komentarze na portalach społecznościowych, forach itp.), których celem jest zmiana opinii publicznej na temat konkretnego obiektu (osoby, organizacji, instytucji, kraju, itp.).

W czasie kampanii informacyjnych duże znaczenie dla wzmocnienia fałszywego przekazu mają konta w sieciach społecznościowych, które istotnie wpływają na sieć społecznościową. Dlatego należy zidentyfikować właśnie te konta, które odgrywają istotną rolę w operacjach wpływu.

Kampanie informacyjne mogą być wykrywane, identyfikowane i oceniane przy wykorzystaniu technik sztucznej inteligencji (ang. artificial intelligence, skrót AI), w szczególności za pomocą uczenia maszynowego (ang. *machine learning*), czyli algorytmów, które automatycznie będą budowały model matematyczny na podstawie danych związanych z podejrzaną aktywnością, np. interakcjami konta z zagranicznymi mediami. Innym ważnym aspektem mającym znaczenie dla analiz są używane przez takie konta języki. Takie podejście pozwoli wykrywać wrogie konta, które są aktywne w różnych kampaniach informacyjnych. Pozwoli również na klasyfikowanie tych kont internetowych w mediach społecznościowych w przydatne taksonomie[88].

W ostatnich latach coraz powszechniejsze stało się manipulowanie informacjami w Internecie, ponieważ sponsorowane przez państwo kampanie informacyjne mają na celu wpływanie na zachowania ludzi oraz ich polaryzację poprzez masowe skoordynowane działania.

[87] B. Tarczydło, *Kampania społeczna w teorii i praktyce*, AGH, Kraków, źródło: https://www.ue.katowice.pl/fileadmin/_migrated/content_uploads/19_B.Tarczydlo_Kampania_spoleczna_w_teorii_i_praktyce.pdf, [19.02.2022].

[88] Por. https://www.ll.mit.edu/r-d/projects/reconnaissance-influence-operations, [04.03.2022].

5.2. Narzędzia do walki z dezinformacją w Internecie

Rozwój Internetu i pojawienie się mediów społecznościowych fundamentalnie zmieniły ekosystem informacyjny, dając społeczeństwu bezpośredni dostęp do większej ilości informacji niż kiedykolwiek wcześniej. Jednak często odróżnienie właściwych informacji od treści niskiej jakości lub fałszywych jest prawie niemożliwe. Oznacza to, że fałszywe lub celowo wprowadzające w błąd informacje w sektorze bankowym, których zadaniem jest osiągnięcie celu gospodarczego lub politycznego szerzą się, rozprzestrzeniając dalej i szybciej w Internecie niż kiedykolwiek w innym formacie.

Jednym z elementów operacji czy kampanii informacyjnej jest dezinformacja[89]. Ważne zatem staje się wykrywanie i identyfikowanie dezinformacji i jej źródeł.

W ramach inicjatywy Countering Truth Decay[90] i przy wsparciu Fundacji Hewlett, RAND zidentyfikował i scharakteryzował szereg narzędzi internetowych opracowanych przez organizacje non-profit i organizacje społeczeństwa obywatelskiego w celu zwalczania dezinformacji w Internecie. Narzędzia te zostały stworzone, aby pomóc poruszać się w dzisiejszym wymagającym środowisku informacyjnym[91].

Narzędzia wykorzystywane do wykrywania przybierają różne formy, od witryn internetowych opartych na ludzkich mechanizmach sprawdzania faktów, po aplikacje wykorzystujące sztuczną inteligencję do wykrywania botów. Narzędzia pogrupowano w kilka kategorii, z których niektóre należą do wielu kategorii. Podział kategorii jest następujący:

Wykrywanie botów/spamu

Narzędzia te mają na celu identyfikację automatycznych kont na platformach mediów społecznościowych. Do tej kategorii zaliczono:

- Bot Sentinel,
- Botometer,
- Hoaxy (Observatory on Social Media)[92].

Bot Sentinel. Jest to opracowana w 2018 roku darmowa platforma opracowana do wykrywania i śledzenia trollbotów i niewiarygodnych kont na Twitterze. Stworzona została w celu wsparcia użytkowników informacji w walce z dezinformacją i ukierunkowanym nękaniem. Bot Sentinel wykorzystuje uczenie maszynowe i sztuczną inteligencję do badania konta na Twitterze, klasyfikowania go jako godnego zaufania lub niewiarygodnego oraz identyfikowania botów. Następnie przechowuje te konta w bazie danych, aby codziennie śledzić każde konto. Deweloperzy wykorzystują gromadzone dane do badania wpływu botów i ich propagandy na dyskurs oraz do badania sposobów przeciwdziałania rozprzestrzenianiu się botów i rozpowszechnianych przez nie informacji. Klasyfikowanie niewiarygodnych kont to proces ręczny. Analitycy przeglądają setki tweetów i retweetów podczas procesu oceny. Jeśli konto ma dużą liczbę obserwujących i wysoki odsetek wprowadzających w błąd lub niepoprawnych merytorycznie tweetów, może zostać uznane za niewiarygodne. To narzędzie koncentruje się zarówno na treści, jak i na procesie. Bezpośrednio ocenia informacje (np. uwierzytelnianie zdjęcia), ale także ocenia sposób wytwarzania i rozpowszechniania informacji. Bot Sentinel zwalcza dezinformację, identyfikując, tagując i śledząc boty oraz klasyfikując niewiarygodne konta. Identyfikacja botów zapewnia użytkownikom informacji możliwość rozróżnienia między treściami automatycznymi i ludzkimi. Oflagowując niewiarygodne konta, narzędzie dostarcza również użytkownikom informacji o jakości i wiarygodności informacji, w tym przypadku konkretnie na Twitterze. Konta oceniane są na podstawie wyniku od 0% do 100% – im wyższy wynik, tym większe prawdopodobieństwo, że konto zaangażuje się w ukierunkowane nękanie, toksyczne trollowanie lub stosuje oszukańcze taktyki opracowane w celu wywołania podziału i chaosu. System potrafi poprawnie klasyfikować konta z dokładnością do 95%. Ta platforma do śledzenia botów nie jest powiązana z RAND. Jest własnością i jest zarządzana przez Bot Sentinel Inc. Adres owej platformy to: https://botsentinel.com/#.

Istnieją różne rodzaje botów na Twitterze. Podobnie jak ogólny wynik bota, każdy wynik typu bota opisuje, jak bardzo konto działa jak określony rodzaj konta. Obecnie mamy sześć typów:

[89] Zob. M. Wrzosek, *Dezinformacja jako komponent operacji informacyjnej*, Akademia Obrony Narodowej, Warszawa 2005.

[90] Zanikanie Prawdy to termin, którego RAND Corporation (ang. *Research ANd Development*) – amerykański think tank i organizacja badawcza non-profit, pierwotnie sformowana dla potrzeb Sił Zbrojnych Stanów Zjednoczonych – używa w odniesieniu do malejącej roli faktów, danych i analiz w dyskursie politycznym i obywatelskim oraz w procesie stanowienia polityki. Zanikanie Prawdy charakteryzuje się czterema trendami: rosnącą niezgodą na fakty i dane; zacieraniem się granicy między opinią a faktem; rosnącą względną ilością opinii w porównaniu z faktami oraz malejącym zaufaniem do instytucji, które były postrzegane jako autorytatywne źródła informacji faktycznych.

[91] https://www.rand.org/research/projects/truth-decay/fighting-disinformation.html, [04.03.2022].

[92] https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html#q=&typeOfTool=Bot%2Fspam+detection&typeOfTool=Codes+and+standards, [14.03.2022].

- Echo-komora: konta, które angażują się w grupy śledzące oraz udostępniają i usuwają treści polityczne w dużej ilości
- Fałszywy obserwujący: boty zakupione w celu zwiększenia liczby obserwujących
- Finansowe: boty, które publikują za pomocą cashtagów
- Zadeklarowane przez siebie: boty z botwiki.org
- Spamer: konta oznaczone jako spamboty z kilku zbiorów danych
- Inne: różne inne boty uzyskane z ręcznych adnotacji, opinii użytkowników itp.

Botometer. Jest opracowanym w 2014 roku internetowym programem, który wykorzystuje uczenie maszynowe do klasyfikowania kont na Twitterze jako botów lub ludzi. Analizuje cechy profilu, w tym znajomych, strukturę sieci społecznościowej, aktywności czasowe, język oraz nastroje.

Botometer jest algorytmem uczenia maszynowego przeznaczonym do obliczania wyniku, w którym niskie wyniki wskazują prawdopodobne konta ludzkie, a wysokie wyniki wskazują prawdopodobne konta botów. Narzędzie to wyświetla ogólny wynik bota (w skali 0–5) wraz z kilkoma innymi wynikami, które stanowią miarę prawdopodobieństwa, że konto jest botem. To narzędzie ma na celu zwalczanie dezinformacji poprzez identyfikowanie botów (częstych źródeł dezinformacji) i ich zawartości, ostatecznie pomagając użytkownikom interpretować i oceniać informacje. Botometer powstał w wyniku współpracy Instytutu nauk o sieciach Uniwersytetu Indiany (ang. *Indiana University Network Science Institute*, skrót IUNI) oraz Centrum badań sieci złożonych i systemów (ang. *Center for Complex Networks and Systems Research,* skrót CNetS).

Hoaxy. Jest opracowanym w ramach projektu *Observatory on Social Media* w 2016 roku w ramach współpracy Instytutu nauk o sieciach Uniwersytetu Indiany oraz Centrum badań sieci złożonych i systemów narzędziem internetowym, które wizualizuje rozpowszechnianie artykułów w Internecie. Hoaxy wyszukuje twierdzenia i weryfikację faktów od 2016 r. Śledzi udostępnianie linków do historii ze źródeł o niskiej wiarygodności i niezależnych organizacji weryfikujących fakty. Oblicza również wynik bota, który jest miarą prawdopodobnego poziomu automatyzacji. W obszarze funkcjonalnym Hoaxy pozostaje badanie i lepsze zrozumienie, w jaki sposób informacje są udostępniane w Internecie. Narzędzie to pomaga zidentyfikować wpływ określonych mediów społecznościowych na dyskurs publiczny. Koncentruje się na treści. Bezpośrednio ocenia informacje, takie jak np. autentyczność zdjęcia.

Kody i standardy

Dotyczy to wszystkich narzędzi, które ustanawiają nowe normy, zasady lub najlepsze praktyki w celu zarządzania zbiorem procesów lub kierowania postępowaniem i zachowaniem. W większości prezentowanych tu narzędzi kodeksy i standardy mają na celu ochronę przed dezinformacją lub informacjami mylnymi. Do tej kategorii zaliczono:

- Certified Content Coalition
- International Fact Checking Network (IFCN) Codes and Principles
- Journalism Trust Initiative
- Pro-Truth Pledge
- The Trust Project Indicators

Certified Content Coalition czyli koalicja certyfikowanych treści. Jest to założona w 2018 roku inicjatywa mająca na celu promowanie standardów wśród wydawców mediów internetowych i certyfikację wydawców spełniających te standardy. Wydawcy, którzy są certyfikowani, otrzymają i będą wyświetlać certyfikat cyfrowy. Narzędzie to koncentruje się na procesie. Ocenia sposób tworzenia i rozpowszechniania informacji. Ma na celu ograniczenie dezinformacji poprzez poprawę praktyk dziennikarskich i standardów dotyczących jakości i przejrzystości informacji wśród dziennikarzy, wydawców i innych osób zaangażowanych w przestrzeń medialną.

International Fact Checking Network (IFCN) Codes and Principles czyli kodeksy i zasady międzynarodowej sieci kontroli faktów. Jest to założona w 2015 roku inicjatywa stworzona w celu promowania sprawdzania faktów w dziennikarstwie. Częścią tego jest stworzenie Kodeksu Zasad IFCN, który może pomóc w ustaleniu standardów metod sprawdzania faktów. IFCN organizuje również staże, szkolenia i konferencje. Dobre praktyki dziennikarskie w zakresie sprawdzania faktów przed przekazywaniem do publicznej wiadomości informacji znacznie wpłyną na stabilność zachowania się klientów banków. Narzędzie to podobnie jak Certified Content Coalition koncentruje się na procesie. Ocenia sposób tworzenia i rozpowszechniania informacji.

Journalism Trust Initiative, czyli inicjatywa zaufania dziennikarskiego. Jest to założona w 2018 roku

inicjatywa promująca zaufanie do dziennikarstwa poprzez opracowywanie odpowiednich standardów. Przedsięwzięcie to realizowane jest poprzez robocze porozumienie Europejskiego Komitetu Normalizacyjnego powszechnie określane skrótem CWA (ang. *CEN Workshop Agreement*, gdzie CEN od ang. *European Committee for Standardization*) stanowiące dokument referencyjny oraz udział mediów, rad prasowych i innych zainteresowanych stron w warsztatach tematycznych.

Narzędzie to koncentruje się na promowaniu dziennikarstwa godnego zaufania i ograniczaniu dezinformacji poprzez opracowywanie standardów przejrzystości, metod dziennikarskich i etyki. Celem tego narzędzia jest wypracowanie standardów, które mogą być wykorzystywane jako mechanizm samoregulacji, a docelowo mogłyby prowadzić do procesów certyfikacji mediów. Standardy te mogą być wykorzystywane nie tylko przez dziennikarzy i opinię publiczną, ale także przez sektor bankowy.

The Pro Truth Pledge, czyli zobowiązanie do prawdy. Jest to założona w 2016 roku inicjatywa mająca na celu zachęcanie do zachowań zgodnych z prawdą. Jest to zobowiązanie oparte o dzielenie się prawdą, jej honorowaniu i zachęcaniu do niej.

Narzędzie to opiera się na strategiach nauk behawioralnych, takich jak zmiana bodźców, zarządzanie reputacją, nudging[93] i ponowne zachęcanie, aby stworzyć normę przeciwko rozpowszechnianiu i tworzeniu dezinformacji. Narzędzie to ma również na celu zbudowanie społeczności skupionej na promowaniu i ochronie faktów i danych.

The Trust Project Indicator, czyli wskaźnik zaufania projektu. Założona w 2016 roku wspólna inicjatywa kilku firm informacyjnych, która opracowuje standardy mające na celu zwiększenie przejrzystości w dziennikarstwie. W ramach projektu opracowano następujące *wskaźniki zaufania*: najlepsze praktyki, wiedza ekspercka autora/reportera, rodzaj pracy, cytaty i odniesienia, metody, źródła lokalne, zróżnicowane głosy, informacje zwrotne, które można wykorzystać. Organizacje informacyjne będą umieszczać te wskaźniki w swoich artykułach.

Narzędzie to ma na celu walkę z dezinformacją poprzez wykorzystanie wskaźników do wzmacniania wysokiej jakości dziennikarstwa i pomagania użytkownikom w unikaniu źródeł niższej jakości, które mogą zawierać błędne informacje lub dezinformację.

[93] Teoria Nudge to koncepcja z zakresu ekonomii behawioralnej, teorii politycznej i nauk behawioralnych, która proponuje pozytywne wzmocnienia i pośrednie sugestie jako sposoby wpływania na zachowania i decyzje grup lub jednostek, źródło: https://en.wikipedia.org/wiki/Nudge_theory, [14.03.2022].

Ocena wiarygodności

Narzędzia oceny wiarygodności przyznają ocenę lub ocenę poszczególnym źródłom na podstawie ich dokładności, przejrzystości, jakości i innych miar wiarygodności. Do tej kategorii zaliczono:

- Disinformation Index,
- FakerFact,
- KnowNews,
- MediaBias Ratings,
- Misinformation Detector,
- NewsCheck Trust Index,
- Newstrition,
- OpenSources,
- The Factual,
- Trusted Times[94].

Disinformation Index, czyli Globalny Indeks Dezinformacji (GID) jest to utworzone w 2018 roku narzędzie internetowe, które ocenia serwisy informacyjne na podstawie „prawdopodobieństwa wystąpienia dezinformacji w danym serwisie medialnym".

Indeks zawiera ratingi ryzyka dezinformacji dla serwisów informacyjnych na rynkach medialnych całego świata. Oceny ryzyka są neutralne, niezależne i przejrzyste. Oceny dokonywane są na poziomie witryny. Stanowią one bezstronny „złoty standard" do oceny ryzyka dezinformacji. GID i jego ratingi są bezstronne i niepolityczne[95]. Ocena ryzyka GID opiera się na zidentyfikowanych przez ekspertów „flagach" dezinformacji, które mogą być połączone, aby pomóc w dokładnej i bezstronnej ocenie ryzyka domeny informacyjnej. Ocena ryzyka strony jest określana na podstawie automatycznej i ręcznej oceny. GID tworzy ratingi ryzyka dla domen informacyjnych na każdym rynku medialnym.

Indeks składa się z czterech filarów:

Struktura: Ten filar jest zautomatyzowany i analizuje różne metadane oraz sygnały obliczeniowe domen informacyjnych. Wykorzystuje on sztuczną inteligencję, która została opracowana na podstawie próbki 20 000 znanych domen dezinformacyjnych.

[94] https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html#q=&typeOfTool=Credibility+scoring, [02.05.2022].
[95] https://disinformationindex.org/the-index/, [19.02.2022].

Treść: Ten filar ręcznie ocenia różne „flagi" dezinformacji dla artykułów opublikowanych w określonej domenie. Obejmują one wiarygodność artykułu, sensacyjność, mowę nienawiści i bezstronność. Ocena ta opiera się na anonimowym przeglądzie 10 losowo wybranych artykułów o największej liczbie udostępnień w danej domenie. Przegląd jest dokonywany przez badacza, a źródło artykułów nie jest mu ujawniane.

Operacyjność: Ten filar ocenia podstawowe polityki, standardy i zasady, których domeny przestrzegają, aby zapewnić zaufanie i wiarygodność. Flagi dezinformacji pochodzą z uniwersalnego standardu, który został ustanowiony przez Journalism Trust Initiative (JTI). Filar ten koncentruje się na konflikcie interesów oraz integralności operacyjnej i odpowiedzialności danej witryny. Niezależny badacz sprawdza, czy dana witryna stosuje zasady zgodne z JTI. Ostatecznie wyniki będą oparte na informacjach przekazywanych przez witryny w ramach standardu JTI.

Kontekst: W tym filarze oceniane są praktyki związane z reputacją, wiarygodność i rzetelność domeny informacyjnej. Flagi dezinformacji są oceniane przez niezależnych ekspertów w badaniu przeprowadzonym wśród respondentów z całego spektrum politycznego.

Narzędzie to jest skoncentrowane na treści. Bezpośrednio ocenia informacje, takie jak np. autentyczność zdjęcia. Wykorzystuje ocenę i punktację jakości źródła (na podstawie dokładności, obiektywności itp.), aby kierować czytelników do informacji o wyższej jakości, a nie do informacji o niskiej jakości. Indeks został opracowany przy udziale Technicznej Grupy Doradczej składającej się z ośmiu członków z całego świata.

FakerFact jest opracowanym w 2018 roku narzędziem wykorzystującym sztuczną inteligencję, które ocenia cel i cechy informacji. Ocenia m.in. agendę, dziennikarstwo, wiki, opinię, satyrę. Narzędzie nie ocenia artykułu jako prawdziwego lub fałszywego, ale raczej podaje ocenę celu i obiektywności.

FakerFact stworzono po to, by pomóc lepiej zrozumieć to, co czytamy. Swobodny przepływ informacji ułatwia niektórym autorom mieszanie mniej wiarygodnych historii z artykułami opartymi na faktach. Zbyt wiele z tego, co można przeczytać i dowiedzieć się z Internetu, nie zawsze służy ustaleniu, co jest prawdą, czy dzieleniu się wiedzą. Zamiast skupiać się tylko na faktach, niektóre artykuły koncentrują się bardziej na wykorzystaniu naturalnych ludzkich reakcji na sposób, w jaki informacje są prezentowane, a nie na tym, co te informacje przekazują. FakerFact umożliwia wykrycie, kiedy artykuł koncentruje się na dzieleniu się wiarygodnymi informacjami, a kiedy na manipulowaniu czytelnikiem lub wpływaniu na niego za pomocą środków innych niż fakty. FakerFact jest narzędziem pozwalającym na wyodrębnienie z tekstu tylko faktów.

FakerFact zakłada, że najlepszym sędzią odróżniającym prawdę od fikcji jest sam czytający dany artykuł. Zadaniem tego narzędzia jest uważne przeanalizowanie tekstu i poinformowanie czytającego, jakiego rodzaju jest to artykuł. Czy artykuł jest stronniczy, czy też zawiera wyważoną ocenę? Czy artykuł jest napisany w taki sposób, że skupia się na faktach, czy też jest napisany w celu przekazania zmanipulowanych informacji? Czy styl pisania wykorzystuje manipulacyjną perswazję, czy też jest napisany w sposób, który dostarcza informacji umożliwiających wyciągnięcie własnych wniosków? Jeśli coś w artykule wydaje się podejrzane, narzędzie poinformuje, że jest podejrzane, a czytającemu pozostawi decyzję o poszukaniu innych wiarygodnych i rzetelnych źródeł informacji, które skupiają się na faktach[96].

KnowNews to narzędzie, które jest rozszerzeniem przeglądarki opracowanym w ramach inicjatywy Media Monitoring Africa Initiative w 2017 roku. Klasyfikuje ono strony informacyjne na podstawie ich wiarygodności. Strony są klasyfikowane jako wiarygodne, podejrzane lub nieoceniane. Narzędzie to należy do kategorii narzędzi dynamiczne wykrywających fałszywe wiadomości. Pomaga sprawdzić, czy dana witryna oferuje wiarygodne wiadomości, czy też nie należy jej ufać i jest niewiarygodna. Aby określić, czy strona z wiadomościami jest wiarygodna, czy nie w KnowNews stosuje się ustalone kryteria. Twórca KnowNews, czyli Media Monitoring Arica jest niezależną organizacją non-profit, która promuje wolność mediów, jakość mediów i etyczne dziennikarstwo[97]. Podmiotami finansującymi te narzędzie są m.in.: Facebook, Open Society Foundation for South Africa i Google.

Media Bias/Fact Check, (MBFC) jest założoną w 2015 roku przez Dave'a Van Zandta niezależną platformą internetową, która ocenia stronniczość, dokładność faktograficzną i wiarygodność źródeł medialnych. MBFC określa stronniczość źródeł medialnych i poziom ogólnego raportowania faktów poprzez połączenie obiektywnych środków i subiektywnej analizy przy użyciu naszej określonej metodologii. Dave Van Zandt jest głównym redaktorem źródeł. Wspomaga go grupa wolontariuszy i płatnych wykonawców, którzy prowadzą badania dla wielu źródeł wymienionych

[96] https://counteringdisinformation.org/index.php/interventions/fakerfact, [19.02.2022].
[97] https://chrome.google.com/webstore/detail/know-news/bmlfbcipfpdohbhhlkibdiacikbpaofm, [19.02.2022].

na tych stronach. MBFC oferuje również okazjonalne sprawdzanie faktów, oryginalne artykuły na temat stronniczości mediów oraz codzienne publikacje sprawdzające fakty z całego świata. Obecnie w bazie danych MBFC znajduje się ponad 4400 źródeł medialnych i dziennikarzy, a ich liczba stale rośnie.

MBFC jest jednocześnie platformą edukującą społeczeństwa na temat stronniczości mediów i oszukańczych praktyk informacyjnych. MBFC cieszy się zaufaniem głównych mediów i organizacji IFCN (ang. *International Fact-Checking Network*) zajmujących się sprawdzaniem faktów. Świadczy o tym fakt, że często powołują się na nich takie źródła, jak USA Today, Reuters Fact Check, Science Feedback czy Washington Post. Media Bias/Fact Check był również wykorzystywany jako źródło do badań przez Uniwersytet Michigan i Massachusetts Institute of Technology[98].

W tym miejscu należy wyjaśnić, iż International Fact-Checking Network (IFCN) jest organizacją, która monitoruje trendy w sprawdzaniu faktów, zapewnia zasoby szkoleniowe oraz organizuje coroczną konferencję na temat sprawdzania faktów pod nazwą #GlobalFact. Jej celem jest promowanie najlepszych praktyk w zakresie kontroli faktów oraz zapewnienie miejsca do współpracy pomiędzy osobami sprawdzającymi fakty na całym świecie. IFCN posiada Kodeks Zasad, który został opracowany w 2016 roku. Do zasad tych zalicza się:

1. Zobowiązanie do bezpartyjności i uczciwości
   W ramach tej zasady sprawdzane są fakty, przy zastosowaniu tego samego standardu dla każdej kontroli faktów. Bez koncentrowania się na sprawdzaniu faktów po żadnej ze stron. Stosowana jest ta sama procedura przy każdym sprawdzaniu faktów i w efekcie wnioski formułowane są przez dowody. W myśl tej zasady nie są popierane ani nie są zajmowane stanowiska polityczne w sprawach, które są sprawdzane.

2. Zobowiązanie do przejrzystości źródeł
   Zasada ta zapewnia użytkownikom możliwość samodzielnej weryfikacji ustaleń IFCN. Podawane są wszystkie źródła na tyle szczegółowo, aby czytelnicy, jeśli będą chcieli, mogli powtórzyć pracę analityczną, z wyjątkiem przypadków, w których mogłoby być zagrożone osobiste bezpieczeństwo źródła. W takich przypadkach podawane jest możliwie jak najwięcej szczegółów.

3. Zobowiązanie do przejrzystości finansowania i organizacji
   Zachowywana jest przejrzystość w zakresie źródeł finansowania. W przypadku otrzymania funduszy od innych organizacji, zachowywana jest dbałość o to, aby nie miały one wpływu na wnioski zawarte w raportach. Szczegółowo opisywane jest przygotowanie zawodowe wszystkich kluczowych osób w organizacji oraz wyjaśniana jest struktura organizacyjna i status prawny. Wyraźnie wskazywany jest czytelnikom sposób, w jaki mogą się kontaktować z organizacją.

4. Zobowiązanie do przejrzystości metodologii
   Wyjaśniana jest metodologia, według której są wybierane, badane, pisane, redagowane, publikowane i poprawiane analizy faktów. Czytelnicy są zachęcani do nadsyłania informacji do sprawdzenia i są transparentni w kwestii tego, dlaczego i w jaki sposób sprawdzają fakty.

5. Zobowiązanie do otwartej i uczciwej korekty
   Sygnatariusze publikują swoją politykę korekt i skrupulatnie jej przestrzegają. Poprawiają w sposób jasny i przejrzysty, zgodnie z polityką poprawek, starając się w miarę możliwości zapewnić czytelnikom możliwość zapoznania się z poprawioną wersją[99].

Kolejnym sposobem identyfikacji dezinformacji w Internecie jest *śledzenie dezinformacji*. Narzędzia wykorzystywane do identyfikacji dezinformacji koncentrują się na treści wiadomości. Bezpośrednio oceniają informacje, takie jak np. autentyczność zdjęcia. Narzędzia te śledzą lub badają przepływ i rozpowszechnienie dezinformacji. Mają na celu bezpośrednie identyfikowanie i zwalczanie dezinformacji poprzez zapewnianie użytkownikom oceny dokładności i wiarygodności informacji oraz oznaczanie, a następnie poprawianie wszelkich fałszywych lub wprowadzających w błąd informacji. Narzędzia dostarczają czytelnikom wskazówek, które pomagają im odróżnić źródła informacji wysokiej i niskiej jakości.

Jednym z takich narzędzi jest detektor dezinformacji (ang. *Misinformation Detector*) *BitPress*. Jest to utworzone w 2018 roku internetowe narzędzie typu „zdecentralizowany protokół zaufania", które zostało zaprojektowane do śledzenia wiarygodności wiadomości w przejrzysty sposób. Narzędzie mierzy zaufanie poprzez analizę treści i tego, z czym jest ona związana, tworząc sieć rozpowszechniania treści w organizacjach medialnych. Wszystkie źródła mediów otrzymują rankingi zaufania. A zatem powiązanie między treścią a określonymi źródłami może wpływać na rankingi zaufania innych źródeł. Narzędzie obejmuje usługi sprawdzania faktów,

[98] https://mediabiasfactcheck.com/about/, [20.02.2022].

[99] https://ifcncodeofprinciples.poynter.org/know-more/the-commitments-of-the-code-of-principles, [02.05.2022].

wykorzystując połączenie metod sprawdzania faktów przez człowieka i technologii blockchain.

NewsCheck Trust Index jest opracowanym w 2017 roku narzędziem, wykorzystywanym na platformie internetowej NewsCheck[100]. Za pomocą tego narzędzia można przeprowadzić ocenę wiarygodności wiadomości. Narzędzie łączy technologie teleinformatyczne (blockchain[101]) i analizę wykonywaną przez ludzi w celu identyfikacji i zwalczania fałszywych wiadomości. Posiada system zarządzania i dostarczania treści, które są uznawane za godne zaufania dla odbiorców. NewsCheck Truck Index jest częścią platformy NewsCheck i stanowi zbiór standardów dziennikarskich, które służą do przejrzystej weryfikacji informacji. Narzędzie to identyfikuje również stronniczość[102].

Newstrition to opracowane w 2018 r. rozszerzenie przeglądarki, które dostarcza informacji o źródłach wiadomości i ocenia dokładność samej historii wiadomości. Ułatwia oddzielenie prawdziwych wiadomości od „śmieci". Proces ten działa dzięki interaktywnej etykiecie dołączanej do wszystkich wiadomości online. Newstrition® to intuicyjne narzędzie do sprawdzania faktów i oceniania wiadomości. Bezpłatnie do użytku niekomercyjnego, można korzystać z aplikacji mobilnej Newstrition, strony internetowej oraz rozszerzeń dla przeglądarek Chrome i Firefox[103].

OpenSources to opracowana w 2017 roku internetowa baza danych źródeł informacji, które zostały przeanalizowane pod kątem ich reputacji w zakresie tworzenia wiarygodnych wiadomości. Baza danych klasyfikuje strony internetowe jako: Fake News, Satire, Extreme Bias, Conspiracy Theory, Rumor Mill, State News, Junk Science, Hate News, Clickbait, Proceed with Caution, Political oraz Credible[104].

The Factual to opracowana w 2016 roku aplikacja mobilna i rozszerzenie do przeglądarki, które oceniają treści informacyjne na podstawie „zakresu i jakości źródeł", „ekspertyzy dziennikarza", „opiniotwórczego charakteru użytego języka" i „historycznej reputacji widoku". Aby zmierzyć jakość treści, ocenia je w skali 0-100. Jest ona w większości zautomatyzowana. Narzędzie ocenia jakość wiadomości na podstawie różnorodności źródeł, doświadczenia autorów, używanego języka itp. Identyfikuje również źródła wyższej jakości.

The Factual to algorytm, który codziennie ocenia ponad 10 000 artykułów informacyjnych pod względem ich zawartości informacyjnej. Na podstawie tych danych The Factual oferuje pięć produktów, dzięki którym można uzyskać najbardziej rzeczowe wiadomości:

Newsletter – dzięki pomocy ludzkich redaktorów, którzy sprawdzają algorytm, The Factual produkuje codzienny newsletter z najbardziej treściwymi artykułami z całego spektrum na najmodniejsze tematy.

Strona internetowa – strona, która pokazuje na bieżąco aktualne tematy, grupując tysiące powiązanych artykułów, pozwalając na filtrowanie według różnych kryteriów.

Aplikację na iOS i Androida – łączy codzienny biuletyn informacyjny i stronę internetową The Factual w jedną prostą aplikację, dzięki której można szybko pozostać na szczycie ważnych trendów informacyjnych.

Rozszerzenie Chrome – rozszerzenie przeglądarki, które robi dwie rzeczy: (1) ocenia, jak bardzo treściwy jest każdy artykuł informacyjny oraz (2) umieszcza oceny artykułów bezpośrednio w kanałach Twittera i Facebooka.

IsThisCredible.com – prosta strona internetowa umożliwiająca uzyskanie oceny każdego znalezionego artykułu informacyjnego lub wyszukanie najbardziej rzeczowych wiadomości na dowolny temat[105].

Trusted Times opracowane w 2017 roku rozszerzenie przeglądarki, które klasyfikuje fake news i nierzetelne treści. Wykorzystuje uczenie maszynowe, aby dostarczyć dodatkowych informacji o artykułach, w tym o stronniczości i szczegółach dotyczących tego, kto jest opisywany pozytywnie, a kto negatywnie. Może klasyfikować artykuły jako fałszywe, niewiarygodne, zweryfikowane lub należące do głównego nurtu mediów; przedstawiać podsumowania zweryfikowanych treści; identyfikować ważne tematy; identyfikować potencjalną stronniczość; identyfikować historyczną stronniczość reporterów oraz historyczną stronniczość konkretnej witryny. Do przedstawiania wiarygodności stron internetowych wykorzystywane są ikony. Jest to jedyne rozszerzenie, które pomaga zidentyfikować stronniczość (jeśli taka istnieje) w każdym artykule informacyjnym, wykorzystując sztuczną inteligencję i zaawansowane algorytmy uczenia maszynowego.

[100] https://www.newscheck.com, [03.05.2022].
[101] Blockchain, czyli łańcuch bloków jest współużytkowanym, niezmienialnym rejestrem. Sprzyja budowie zaufania, ponieważ stanowi współdzielony rejestr prawdziwych informacji. Dane wiarygodne w oczach wszystkich użytkowników pomagają wykorzystywać inne nowe technologie, które radykalnie zwiększają efektywność, przejrzystość i skuteczność działań, https://www.ibm.com/pl-pl/topics/what-is-blockchain, [05.05.2022].
[102] https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/newscheck-trust-index.html[05.05.2022].
[103] https://our.news/how-it-works/?main, [05.05.2022].
[104] https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/opensources.html, [05.05.2022].
[105] https://www.thefactual.com, [5.05.2022].

Wykorzystując zaawansowane algorytmy uczenia maszynowego, przedstawia również dodatkową analizę każdego artykułu informacyjnego, aby pokazać ewentualną stronniczość reportera i źródła wiadomości. Dzięki temu można przeczytać każdą wiadomość jak profesjonalista.

Trusted Times różni się od innych wykrywaczy fake newsów, ponieważ:

- Przegląda największy wybór serwisów informacyjnych oraz blogów w Stanach Zjednoczonych.
- Jest to jedyne rozszerzenie, które umożliwia niezależne traktowanie każdego dziennikarza i artykułu informacyjnego – w przeciwieństwie do klasyfikowania całej gazety pod względem sympatii politycznych jako „lewicowej, centrowej lub prawicowej".
- Identyfikuje, czy artykuł jest fałszywy, niewiarygodny, zweryfikowany czy jest wiadomością głównego nurtu mediów.
- Przedstawia podsumowanie zweryfikowanych i mainstreamowych artykułów informacyjnych.
- Skanuje artykuł w celu zidentyfikowania ważnych i istotnych tematów i zagadnień poruszanych w artykule informacyjnym.
- Jest jedynym rozszerzeniem przedstawiającym analizę stronniczości artykułu lub sentymentu do danego tematu.
- Jest jedynym rozszerzeniem zapewniającym analizę historyczną stronniczości reportera w odniesieniu do wspomnianego tematu.
- Jest jedynym rozszerzeniem o analizę historyczną stronniczości strony internetowej w stosunku do wspomnianego tematu.

Trusted Times uznaje, że każda organizacja informacyjna, taka jak New York Times czy Politico składa się z setek reporterów, z których każdy ma unikalną perspektywę, wbudowany schemat/stronniczość, pomysły lub styl pisania.

Trusted Times wykorzystuje zaawansowane algorytmy uczenia maszynowego do analizy języka każdego artykułu, który odzwierciedla opinię lub nastawienie autora do danego tematu.

W ten sposób dziennikarz o unikalnych przekonaniach lub możliwej agendzie z jakiegokolwiek powodu zostaje zdemaskowany jako stronniczy w stosunku do tematu lub osoby, nawet jeśli pracuje w organizacji informacyjnej znanej z własnego politycznego odchylenia, tj. lewicy, prawicy lub neutralności.

Trusted Times jest idealny dla wszystkich, którzy poszukują wiarygodnego źródła informacji pozwalającego odróżnić sprawdzalne i wiarygodne źródło wiadomości opartych na faktach[106].

Disinformation tracking

Narzędzia te śledzą lub badają przepływ i rozpowszechnienie dezinformacji. Do tej kategorii zaliczono:

- BotSlayer
- Facebook Political Ad Collector
- Hamilton 2.0
- Hoaxy (Observatory on Social Media)
- Iffy Quotient
- Information Operations Archive
- Twitter Trails
- Who Targets Me

BotSlayer to opracowana w 2018 roku aplikacja, która pomaga śledzić i wykrywać potencjalne manipulacje informacjami rozprzestrzeniającymi się na Twitterze. Narzędzie zostało opracowane przez Obserwatorium Mediów Społecznych na Uniwersytecie Indiana (to samo laboratorium, które stworzyło Botometr i Hoaxy).

BotSlayer nie jest narzędziem do wykrywania i usuwania prawdopodobnych botów z listy obserwatorów lub znajomych na Twitterze. BotSlayer może być wykorzystywany na przykład do wykrywania w czasie rzeczywistym nowych skoordynowanych kampanii bez wcześniejszej wiedzy o tych kampaniach. System można łatwo zainstalować i skonfigurować w chmurze, aby monitorować aktywność botów wokół stałego zapytania zdefiniowanego przez użytkownika. Wystarczy klucz do aplikacji deweloperskiej Twittera, aby pobierać dane z interfejsu API Twittera.

BotSlayer wykorzystuje algorytm wykrywania anomalii do oznaczania hashtagów, linków, kont i mediów, które są trendy i wzmacniane w skoordynowany sposób przez prawdopodobne boty. Pulpit nawigacyjny pozwala użytkownikom badać tweety i konta

[106] https://addons.mozilla.org/pl/firefox/addon/trustedtimes/, [09.05.2022].

powiązane z podejrzanymi kampaniami za pośrednictwem Twittera, wizualizować ich rozprzestrzenianie się za pomocą Hoaxy oraz wyszukiwać powiązane obrazy i treści w Google.

BotSlayer został zaprojektowany jako platforma crowdsourcingowa: w zamian za bezpłatną usługę system dostarcza anonimowe dane do naszego laboratorium w celu przeprowadzenia badań, w sposób zgodny z warunkami i wytycznymi Twittera. Dane te będą pomocne w badaniu i wczesnym wykrywaniu zjawisk manipulacji w mediach społecznościowych[107].

Facebook Political Ad Collector

Facebook Political Ad Collector jest opracowanym w 2017 roku narzędziem pokazującym użytkownikom reklamy w ich kanałach na Facebooku i identyfikującym, które z nich mają charakter polityczny, indoktrynujący. Pokazuje również użytkownikom reklamy polityczne skierowane do innych użytkowników. Wszystkie zebrane reklamy polityczne są umieszczane w publicznie dostępnej bazie danych.

Narzędzie to ma dwa cele. Po pierwsze, ma dostarczyć użytkownikom więcej informacji na temat targetowania reklam w Internecie. Dzięki temu ludzie stają się bardziej świadomi istnienia reklam i dezinformacji, a przez to bardziej odporni na nie. Po drugie, narzędzie buduje bazę danych reklam politycznych i targetowania, której celem jest wywarcie presji na duże firmy, by te zmieniły swoje praktyki w zakresie przejrzystości i sposobu obsługi reklam politycznych.

Narzędzie to jest rozszerzeniem do przeglądarki umożliwiającym udostępnianie danych o kanałach społecznościowych użytkownikom informacji w celu zwiększenia przejrzystości.

Obecnie projekt Facebook Political Ad Collector nosi nazwę Ad Observer i jest narzędziem crowdsourcingowym, którego zadanie to zbieranie reklam z kanałów informacyjnych użytkownika na Facebooku, aby umożliwić dziennikarstwo śledcze i badania.

Projekt jest prowadzony przez Online Political Ads Transparency Project na Uniwersytecie Nowojorskim. Wcześniej projekt był prowadzony przez Quartz, The Globe and Mail oraz ProPublica.

Gdy użytkownik zaloguje się na Facebooku, narzędzie zbiera reklamy wyświetlane w news feedzie użytkownika. Narzędzie nie gromadzi żadnych informacji umożliwiających identyfikację użytkownika[108].

Hamilton 2.0

Hamilton 2.0 to opracowane w 2017 roku narzędzie mające na celu identyfikację i walkę z dezinformacją poprzez podnoszenie świadomości na temat trwających, wspieranych przez państwo operacji informacyjnych, które mogą, ale nie muszą zawierać fałszywe lub zmanipulowane informacje. Agreguje ono informacje promowane przez rosyjski rząd i wspierane przez państwo media, aby zidentyfikować trendy i taktyki stosowane w celu wywarcia wpływu na zachodnich odbiorców na platformach mediów społecznościowych.

Hamilton 2.0 to internetowy pulpit nawigacyjny, który w czasie rzeczywistym dostarcza informacji o rosyjskiej propagandzie i dezinformacji w sieci. Odbywa się to poprzez śledzenie setek powiązanych z Rosją kont na Twitterze, które są związane z wpływaniem na informacje w Stanach Zjednoczonych i Europie. Narzędzie zapewnia analizę narracji i tematów promowanych przez rosyjski rząd i wspierane przez państwo media na Twitterze, YouTube, w telewizji i na sponsorowanych przez państwo portalach informacyjnych.

Hamilton 2.0 to projekt Alliance for Securing Democracy przy German Marshall Fund of the United States. Zawiera zbiorczą analizę narracji i tematów promowanych przez rosyjskich, chińskich i irańskich urzędników państwowych i finansowane przez państwo media na Twitterze, YouTube, sponsorowanych przez państwo portalach informacyjnych oraz poprzez oficjalne komunikaty prasowe i stenogramy publikowane przez ministerstwa spraw zagranicznych tych krajów. Tablica zawiera również niewielką kolekcję kont Twitterowych globalnych mediów w celach porównawczych. Hamilton Search to nowa wyszukiwarka Tweetów i narzędzie do wyszukiwania danych, które ma uzupełnić możliwości wyszukiwania Hamiltona 2.0.

Celem tego narzędzia jest zwiększenie naszej wiedzy na temat koncentracji i rozprzestrzeniania się wspieranych przez państwo komunikatów rządowych na różnych nośnikach informacji. Hamilton 2.0 będzie nadal rozwijany i wzbogacany o nowe funkcje. Dzięki temu projektowi badacze zajmujący się kampaniami informacyjnymi państw narodowych i szerszym ekosystemem informacyjnym będą mieli więcej możliwości[109].

Hoaxy (Observatory on Social Media)

Hoaxy (Observatory on Social Media) jest opracowanym w 2016 roku narzędziem mającym na celu identyfikację i walkę z dezinformacją poprzez podnoszenie świadomości na temat różnych kampanii

[107] https://osome.iu.edu/tools/botslayer, [09.05.2022].
[108] https://chrome.google.com/webstore/detail/ad-observer/enliecaalhkhhihcmnbjfmmjkljlcinl, [10.05.2022].
[109] https://securingdemocracy.gmfus.org/hamilton-dashboard/, [27.04.2022].

dezinformacyjnych oraz sposobów rozprzestrzeniania się fałszywych informacji w sieci. Ma to sprawić, że społeczeństwo będzie bardziej świadome dostępnych informacji i lepiej przygotowane do poruszania się w ekosystemie informacyjnym.

The Observatory on Social Media (OSoMe, wymawiane jako awe-some) to wspólny projekt Centrum Badań Sieci i Systemów Złożonych (CNetS) w Luddy School, Szkoły Mediów oraz Instytutu Nauk Sieciowych (IUNI) na Indiana University. OSoMe łączy naukowców i dziennikarzy w badaniu roli mediów i technologii w społeczeństwie oraz budowaniu narzędzi do analizy i przeciwdziałania dezinformacji i manipulacji w mediach społecznościowych.

Hoaxy to narzędzie internetowe, które wizualizuje rozprzestrzenianie się artykułów w sieci. Hoaxy wyszukuje twierdzenia i fact-checking sięgające wstecz do 2016 roku. Śledzi udostępnianie linków do historii ze źródeł o niskiej wiarygodności i niezależnych organizacji sprawdzających fakty. Oblicza również wynik bota, który jest miarą prawdopodobnego poziomu automatyzacji. Ogólnie rzecz biorąc, IU Observatory on Social Media jest zainteresowane badaniem i lepszym zrozumieniem sposobu, w jaki informacje są udostępniane w sieci. Interesuje się również tym, jak media społecznościowe wpływają na dyskurs publiczny.

Hoaxy otrzymał nagrodę National Science Foundation, grant James S. McDonnell Foundation na systemy złożone oraz grant zalążkowy od Lilly Endowment. Badania nad wykrywaniem botów społecznościowych były częściowo wspierane przez DARPA SMISC[110].

Iffy Quotient to narzędzie internetowe, które wykorzystuje NewsWhip[111] do przeszukiwania Facebooka i Twittera oraz identyfikacji adresów URL, o których wiadomo, że są stronnicze lub często podają fałszywe informacje. Narzędzie oblicza następnie odsetek adresów URL na każdej stronie, które są „iffy"[112] lub znane z podawania fałszywych lub wprowadzających w błąd informacji. Iffy Quotient to wskaźnik określający, w jakim stopniu treści pochodzące ze stron „iffy" zostały wzmocnione na Facebooku i Twitterze.

Center for Social Media Responsibility przy University of Michigan School of Information opracowało sposób mierzenia postępów platform medialnych w wypełnianiu ich obowiązków publicznych. Termin iffy używany jest w celu opisania stron, które często publikują dezinformację. Kategoryzacja stron oparta jest o nieprecyzyjne kryteria i błędne ludzkie oceny. Od początku 2016 roku publikowana jest internetowa tablica, która przedstawia iloraz Iffy Quotient. Tablica umożliwia dokonywanie porównań w czasie i między platformami[113].

Information Operations Archive

Information Operations Archive (Archiwum Operacji Informacyjnych) to opracowane w 2018 roku narzędzie, które stanowi archiwum publicznie dostępnych i przypisywanych danych ze znanych internetowych operacji informacyjnych pochodzących z publicznych i nieusuniętych tweetów na Twitterze i Reddicie przypisywanych podmiotom rosyjskim i irańskim. Archiwum składa się obecnie z ponad 10 milionów wiadomości pochodzących ze sponsorowanych przez państwo rosyjskie i irańskie operacji wpływu na Twitterze i Reddicie.

Zbiory danych wykorzystywane w Archiwum Operacji Informacyjnych obejmują zarchiwizowane informacje, które są udostępniane na Twitterze i Reddit od 2018 roku. Poniżej znajdują się szczegółowe informacje na temat aktualnie dostępnych zbiorów danych.

Archiwum przechowuje te zbiory danych zarówno do wykorzystania przez badaczy, którzy chcą zrozumieć i opracować reakcje na dezinformację przeciwnika, jak i do eksploracji przez ogół społeczeństwa. Wiedza na temat konkretnych kampanii dezinformacyjnych oraz praktyk stosowanych przez podmioty rozpowszechniające dezinformację może sprawić, że użytkownicy będą bardziej odporni na przyszłe operacje informacyjne.

Twitter

Zbiory danych obejmują wszystkie publiczne, nieusunięte tweety i media (np. zdjęcia i filmy) z kont, które zdaniem Twittera są powiązane z operacjami informacyjnymi prowadzonymi przez państwo. Tweety usunięte przez tych użytkowników przed ich zawieszeniem (które nie są uwzględnione w tych zbiorach danych) stanowią zazwyczaj mniej niż 1% ich ogólnej aktywności. Zbiory danych Twittera są utrzymywane przez Twittera.

Nie wszystkie konta, które Twitter zidentyfikował jako powiązane z tymi kampaniami, aktywnie

[110] https Iffy Quotient://hoaxy.osome.iu.edu, [27.04.2022].
[111] NewsWhip to jedyna platforma monitorująca media w czasie rzeczywistym, która przewiduje historie i tematy, które będą miały znaczenie w nadchodzących godzinach, dając specjalistom ds. komunikacji jasność potrzebną do podejmowania szybkich i pewnych decyzji.
[112] Iffy jest przymiotnikiem. Nieformalnie oznacza, że coś jest niepewne, w jakiś sposób nie jest dobre, gorsze, nieodpowiednie, niedopuszczalne, niedoskonałe, niepewne.
[113] https://csmr.umich.edu/projects/iffy-quotient/, [27.04.2022].

tweetowały, dlatego liczba kont reprezentowanych w zbiorach danych może być mniejsza niż całkowita liczba kont. Zbiory danych Twittera są utrzymywane przez Twittera.

Reddit

Swój raport przejrzystości za rok 2017 wraz z listą 944 kont, co do których administratorzy strony podejrzewają, że należą do Rosyjskiej Agencji Badań Internetowych Reddit opublikował 11 kwietnia 2018 roku. Ten zbiór danych zawiera 944 konta. Reddit na razie udostępnia listę kont, ale po pewnym czasie ich zawartość zostanie usunięta z Reddita. Reddit robi to, aby umożliwić moderatorom, śledczym i opinii publicznej samodzielne zapoznanie się z historią kont[114].

Twitter Trails

Twitter Trails to opracowane w 2014 roku narzędzie internetowe, które wykorzystuje algorytm do analizy rozprzestrzeniania się danej historii i reakcji użytkowników na nią. Narzędzie mierzy rozprzestrzenianie się historii i sceptycyzm wyrażany przez użytkowników.

Algorytm mierzy, jak szeroko rozprzestrzeniła się wiadomość i jak sceptyczni są użytkownicy co do jej prawdziwości. Mierząc zachowanie tłumu, algorytm TwitterTrails pozwala badać doniesienia i określać, czy wydają się one prawdziwe, czy fałszywe[115].

Who Targets Me

Who Targets Me jest opracowanym w 2017 roku narzędziem pozwalającym użytkownikom stworzyć anonimowy profil, a następnie gromadzić informacje o ogłoszeniach politycznych i innych, które widzą wraz z informacjami o tym, dlaczego to właśnie do nich kierowane są te reklamy. Narzędzie może dostarczyć użytkownikom statystyk na temat tego, kto lub co skierował do nich reklamy i wykorzystuje te informacje do tworzenia bazy danych kierowanych do nich reklam. Wtyczka Who Targets Me została obecnie zainstalowana przez ponad 50 000 użytkowników na całym świecie w ponad 100 krajach i 20 językach[116].

Narzędzie to ma dwa cele. Po pierwsze, ma dostarczyć użytkownikom więcej informacji na temat targetowania w sieci. Dzięki temu ludzie mogą stać się bardziej świadomi reklam i dezinformacji, a przez to bardziej odporni na nie. Po drugie, narzędzie buduje bazę danych na temat reklam politycznych i targetowania, co ma na celu wywarcie presji na duże firmy technologiczne, by zmieniły swoje praktyki w zakresie przejrzystości i sposobu traktowania reklam politycznych[117].

Weryfikacja

Dotyczy to narzędzi sprawdzających fakty, które mają na celu sprawdzenie dokładności informacji lub autentyczności zdjęć i filmów. Do tej kategorii można zaliczyć:

- Captain Fact
- ClaimBuster
- CrossCheck
- Duke Videofactchecking Tool
- Emergent
- Exifdata
- Exiftool

Captain Fact to opracowana w 2015 roku internetowa kolekcja narzędzi przeznaczonych do zespołowej weryfikacji treści internetowych. Obejmuje rozszerzenie przeglądarki, które zapewnia nakładkę wideo na filmy internetowe ze źródłami i informacjami kontekstowymi, a także ikony pokazujące wiarygodność na podstawie głosów użytkowników. Posiada również „platformę dyskusyjną", która umożliwia omawianie poszczególnych punktów. Choć obecnie projekt koncentruje się na wideo, trwają prace nad narzędziem, które zapewni podobną nakładkę na artykuły[118].

ClaimBuster to opracowane w 2017 roku internetowe, zautomatyzowane narzędzie do sprawdzania faktów na żywo, opracowane przez University of Texas at Arlington. Narzędzie opiera się na przetwarzaniu języka naturalnego i uczeniu nadzorowanym (na podstawie zbioru danych zakodowanych przez człowieka) w celu identyfikacji informacji prawdziwych i fałszywych[119].

CrossCheck opracowane w 2017 r. narzędzie do identyfikacji, badania i korygowania fałszywych informacji, umożliwiając jednocześnie zlokalizowanie informacji opartych na faktach. CrossCheck to inicjatywa współpracy w ramach FirstDraft News, która koncentruje się na weryfikacji. Rozpoczęła się ona przed wyborami we Francji, a newsroomy i firmy technologiczne

[114] https://www.io-archive.org/#/, [27.04.2022].
[115] http://twittertrails.com/, [29.04.2022].
[116] https://whotargets.me/en/about/, [29.04.2022].
[117] https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/who-targets-me.html, [29.04.2022].
[118] https://captainfact.io/, [29.04.2022].
[119] https://idir.uta.edu/claimbuster/, [29.04.2022].

współpracowały ze sobą, aby informować o wprowadzających w błąd wiadomościach i identyfikować je przed wyborami[120].

Duke Videofactchecking Tool to opracowane w 2017 roku rozszerzenie do przeglądarki, które zapewnia sprawdzanie na żywo faktów dotyczących informacji w telewizji. Zostało ono ocenione przez twórców za pomocą eksperymentów opartych na użytkownikach. Użytkownicy generalnie lubili mieć wyskakujące okienka generowane przez to narzędzie, choć różnili się co do tego, czy woleli otrzymywać „ocenę", czy tylko surowe informacje faktograficzne[121].

Emergent to opracowane w 2014 roku narzędzie do śledzenia plotek w czasie rzeczywistym. Jest on częścią projektu badawczego Tow Center for Digital Journalism na Uniwersytecie Columbia, który koncentruje się na tym, w jaki sposób niesprawdzone informacje i plotki są przekazywane w mediach. Jego celem jest opracowanie najlepszych praktyk w zakresie obalania dezinformacji[122].

Exifdata, Exiftool[123]. EXIF to skrót od Exchangeable Image File, formatu będącego standardem przechowywania wymienianych informacji w plikach obrazów fotografii cyfrowej przy użyciu kompresji JPEG. Prawie wszystkie nowe aparaty cyfrowe używają adnotacji EXIF, przechowując informacje o obrazie, takie jak czas otwarcia migawki, kompensacja ekspozycji, numer F, jaki system pomiaru został użyty, czy użyto lampy błyskowej, numer ISO, data i godzina wykonania zdjęcia, balans bieli, zastosowane obiektywy pomocnicze i rozdzielczość. Niektóre obrazy mogą nawet przechowywać informacje GPS, dzięki czemu można łatwo sprawdzić, gdzie zostały zrobione. Exifdata to narzędzie internetowe, które dostarcza informacji o źródle, sygnaturze czasowej, informacji o tworzeniu i modyfikacji. To narzędzie działa w celu zwalczania dezinformacji poprzez weryfikację i uwierzytelnianie obrazów[124].

Misinformation Detector. Detektor dezinformacji BitPress to opracowane w 2018 roku internetowe narzędzie typu „zdecentralizowany protokół zaufania", które zostało zaprojektowane do śledzenia wiarygodności wiadomości w przejrzysty sposób. Narzędzie mierzy zaufanie poprzez analizę treści i tego, z czym jest ona związana, tworząc sieć rozpowszechniania treści w organizacjach medialnych. Wszystkie źródła mediów otrzymują rankingi zaufania, a zatem związek między treścią a określonymi źródłami może wpływać na rankingi zaufania innych źródeł. Narzędzie obejmuje usługi sprawdzania faktów, wykorzystując połączenie technologii sprawdzania faktów ludzkich i technologii blockchain.

Narzędzie to ma na celu bezpośrednią walkę z dezinformacją poprzez zapewnienie użytkownikom oceny dokładności i wiarygodności informacji oraz poprzez oznaczanie, a następnie korygowanie, wszelkich fałszywych lub wprowadzających w błąd informacji. Narzędzie dostarcza czytelnikom informacji, które pomagają im odróżnić źródła informacji o wysokiej i niskiej jakości[125].

5.3. Zautomatyzowane narzędzia do identyfikacji kampanii informacyjnych

Rozpowszechnianie fałszywych wiadomości, dezinformacji oraz wprowadzania w błąd w sieci i mediach społecznościowych stało się pilną kwestią społeczną. Media społecznościowe są szeroko wykorzystywane nie tylko dla dobra społecznego, ale także do wprowadzania w błąd całych społeczności. Aby identyfikować i zwalczać fałszywe lub wprowadzające w błąd informacje, podjęto kilka inicjatyw dotyczących ręcznego sprawdzania faktów. Ponieważ weryfikacja poprawności treści jest priorytetem dla wielu organizacji (w tym sektora bankowego), podjęto wysiłek opracowania automatycznych systemów do sprawdzania faktów. Jednak ze względu na problemy z wiarygodnością systemów automatycznych, przyjęto rozwiązania sprawdzania faktów przez ludzi przy użyciu systemów automatycznych.

Automatyczna weryfikacja informacji, sprawdzanie faktów wydaje się właściwe dla zastosowania sztucznej inteligencji. Zastosowanie takiej technologii umożliwiłoby organizacjom weryfikującym fakty szybsze działanie i zapewnienie bardziej kompleksowego zakresu, niż mogłoby kiedykolwiek osiągnąć ręczne sprawdzanie faktów. Jednak wiele twierdzeń nie jest po prostu poprawnych lub niepoprawnych, ale może być częściowo słusznych lub poprawnych i wprowadzających w błąd bez dodatkowego kontekstu. Jedną z kluczowych ról zawodowych weryfikatorów faktów jest pomoc swoim odbiorcom w uzyskaniu pełnego zrozumienia przekazu, z jego niuansami i złożonością, zamiast stosowania klasyfikacji binarnej.

Weryfikacja faktów nie jest prostym ani rutynowym procesem. Wymaga szeregu kroków, które zaczynają

[120] https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/crosscheck.html, [30.04.2022].
[121] https://reporterslab.org/duke-students-tackle-big-challenges-in-automated-fact-checking/, [30.04.2022].
[122] http://www.emergent.info/about, [30.04.2022].
[123] https://exiftool.org/, [30.04.2022].
[124] https://exifdata.com/index.php, [02.05.2022].
[125] https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/misinformation-detector.html, [02.05.2022].

się od wyczucia mediów i dostrzeżenia twierdzeń wartych sprawdzenia, aż do stwierdzenia czy twierdzenie jest prawdziwe, częściowo prawdziwe, fałszywe, wprowadzające w błąd lub być może niemożliwe do osądzenia. Ponieważ osoby sprawdzające fakty mają do czynienia z mnogością twierdzeń, muszą zdecydować, co tak naprawdę warto sprawdzić. Taki stan rzeczy przyczynia się do rozwoju rozwiązań wykorzystujących sztuczną inteligencję.

Aby zweryfikować niektóre twierdzenia zawarte w przekazach, osoby weryfikujące fakty mogą potrzebować przeprowadzić wywiady z ekspertami, współpracować z innymi osobami weryfikującymi fakty, zrozumieć kontekst i ramy twierdzeń, wyśledzić i zweryfikować wiele źródeł i dowodów, z których wszystkie wymagają inteligencji na poziomie człowieka. Ogólna weryfikacja arbitralnych twierdzeń wymaga głębokiego zrozumienia realnego świata, który obecnie wymyka się sztucznej inteligencji. Rzeczywiście, większość metod ma na celu wspomaganie weryfikatorów faktów w ich pracy z sugestiami i zakłada, że człowiek oceni wynik weryfikacji przed przypisaniem etykiety prawda/fałsz[126].

Poniżej przedstawiono przegląd niektórych godnych uwagi systemów, które obejmują wiele etapów procesu sprawdzania faktów, oferując jednocześnie odpowiedni interfejs użytkownika.

AFCNR (ang. *Automated Fact Checking in the News Room*)

System akceptuje twierdzenie jako dane wejściowe, przeszukuje artykuły z wiadomościami, wyszukuje potencjalne dowody i przedstawia użytkownikowi ocenę stanowiska każdego dowodu wobec roszczenia oraz ogólną ocenę prawdziwości roszczenia na podstawie dowodów. System został gruntownie przetestowany przez jedenastu dziennikarzy BBC.

AFCNR to zautomatyzowana platforma do sprawdzania faktów, która po zgłoszeniu twierdzenia pobiera odpowiednie dowody tekstowe ze zbioru dokumentów, przewiduje czy każdy dowód potwierdza lub odrzuca twierdzenie i zwraca ostateczny werdykt. Przewidywania platformy jako prawidłowe szacuje się na 58% przypadków, a zwrócone trafne dowody na 59%[127].

BRENDA (ang. *Browser Extension for Fake News Detection*)

Jest to rozszerzenie przeglądarki, które umożliwia użytkownikom sprawdzanie faktów bezpośrednio podczas czytania artykułów z wiadomościami. Obsługuje dwa typy danych wejściowych: pełną stronę otwartą w przeglądarce lub podświetlony fragment wewnątrz strony. W pierwszym scenariuszu system stosuje identyfikację sprawdzalności, aby zdecydować, które zdania na stronie należy sprawdzić.

BRENDA zapewnia następujące funkcjonalności:

1. ułatwia użytkownikom sprawdzenie faktów bez opuszczania witryny internetowej. Jeśli użytkownicy nie są pewni, które twierdzenia wymagają sprawdzenia faktów, BRENDA może automatycznie filtrować twierdzenia godne sprawdzenia.

2. może automatycznie wyszukiwać dowody online za pomocą wyszukiwarek internetowych i weryfikować twierdzenia.

3. wykorzystuje sprawdzony, wstępnie przeszkolony model głębokiej sieci neuronowej, który uwzględnia ukryte aspekty twierdzenia w celu zweryfikowania jego prawdziwości.

4. dostarcza fragmenty dowodów podkreślające znaczenie zarówno słów, jak i zdań istotnych dla klasyfikacji twierdzenia przy użyciu wag uwagi z modelu głębokiej sieci neuronowej[128].

ClaimPortal

Platforma internetowa do zintegrowanego monitorowania, wyszukiwania, sprawdzania i analizy twierdzeń faktycznych dotyczących twierdzeń na Twitterze osadzonych w tweetach. Jest on zintegrowany z narzędziami do sprawdzania faktów, w tym z modułem dopasowywania oświadczeń, który znajduje znane informacje weryfikujące fakty pasujące do danego tweeta, z modułem do śledzenia twierdzeń, który ocenia każde twierdzenie i odpowiadający mu tweet na podstawie ich wiarygodności. ClaimPortal zapewnia intuicyjny i wygodny interfejs wyszukiwania, który pomaga użytkownikom przeszukiwać faktyczne twierdzenia w tweetach przy użyciu warunków filtrowania według dat, kont na Twitterze, treści, hashtagów, wyników sprawdzania wiarygodności i rodzajów twierdzeń. ClaimPortal zapewnia również proste narzędzia analityczne i wizualizacyjne do wykrywania wzorców związanych z tym, w jaki sposób określone konta na Twitterze składają twierdzenia, czy w jaki sposób są dystrybuowane różne rodzaje twierdzeń[129].

[126] https://arxiv.org/pdf/2103.07769.pdf, [07.05.2022].
[127] https://arxiv.org/pdf/1904.02037.pdf, [07.05.2022].
[128] Głęboka sieć neuronowa to sieć neuronowa o pewnym poziomie złożoności, zwykle co najmniej dwuwarstwowa. Głębokie sieci przetwarzają dane w złożony sposób, wykorzystując wyrafinowane modelowanie matematyczne, https://www.sciencedirect.com/topics/computer-science/deep-neural-network, [07.05.2022].
[129] https://aclanthology.org/P19-3026.pdf, [07.05.2022].

ClaimPortal jest nowatorską infrastrukturą, ponieważ wielu weryfikatorów w dużej mierze pomija twierdzenia w tweedach. Po pobraniu tweetów w odpowiedzi na zapytanie system ocenia je pod kątem wiarygodności za pomocą ClaimBuster[130] i próbuje zweryfikować każdy tweet, korzystając z wcześniej sprawdzonych twierdzeń na PolitiFact[131]. Adres internetowy do platformy ClaimPortal to: https://idir.uta.edu/claimportal/[132].

Squash

Squash jest systemem opracowanym w laboratorium Duke Reporters. Jest częścią Lab's Tech & Check Cooperative[133]. Stanowi produkt, który słucha przemówień, debat i innych wydarzeń, transkrybuje je na tekst oraz weryfikację faktów wyświetla na ekranie wideo podczas debat, przemówień politycznych lub innych wydarzeń. Squash „słyszy" to, co mówią politycy, przekształca ich wypowiedzi na tekst, a następnie przeszukuje bazę danych wcześniej opublikowanych kontroli faktów w poszukiwaniu takich, które są z nimi powiązane. Gdy Squash znajdzie taką analizę, wyświetla jej podsumowanie na ekranie. Obecnie Squash wyświetla na ekranie 14 istotnych weryfikacji faktów[134].

Full Fact's

System został zaprojektowany jako wsparcie dla osób sprawdzających fakty. System ten śledzi strony informacyjne i media społecznościowe, identyfikuje i klasyfikuje twierdzenia w strumieniu, sprawdza, czy dane twierdzenie zostało już zweryfikowane, a następnie wzbogaca twierdzenia o dane wspierające osobę sprawdzającą fakty. System ten jest na co dzień wykorzystywany w Wielkiej Brytanii i kilku krajach Afryki[135].

Przedstawione powyżej narzędzia są dobrymi przykładami kroków podjętych w celu opracowania systemów, które umożliwiają weryfikację faktów i w efekcie skuteczne identyfikowanie twierdzeń pochodzących z różnych rodzajów źródeł (np. artykułów prasowych, transmisji i mediów społecznościowych).

Kampanie informacyjne zakłócają zdolność użytkownika do pozyskiwania użytecznych informacji z serwisów internetowych, szczególnie w sytuacjach, gdy informacje te mają kluczowe znaczenie dla podejmowania decyzji. Biorąc pod uwagę zmieniający się krajobraz współczesnego świata, problem fałszywych informacji nie jest już tylko problemem marketingowym, ale wymaga poważniejszych działań ze strony podmiotów zajmujących się bezpieczeństwem. Bardzo ważne jest, aby wszelkie próby manipulacji Internetem poprzez oszukańcze wiadomości były identyfikowane z bezwzględną skutecznością. W niniejszym rozdziale przedstawiono szereg projektów, narzędzi, metod i technik, które pozwolą użytkownikom na zastosowanie np. narzędzia w ich osobistej przeglądarce i wykorzystanie go do wykrywania i filtrowania potencjalnych fałszywych informacji.

[130] ClaimBuster to narzędzie do uczenia maszynowego. Jego algorytm wyszukuje zdania w poszukiwaniu słów kluczowych i struktur, które są powszechnie spotykane w stwierdzeniach opartych na faktach, https://idir.uta.edu/claimbuster/, [07.05.2022].

[131] PolitiFact to powstały w 2007 roku projekt, który przed wyborami uruchomiła Tampa Bay Times (wówczas St. Petersburg Times), czyli jedna z największych gazet na Florydzie. Od 2018 roku PolitiFact jest własnością Poynter Institute for Media Studies, do którego należy również gazeta. Jest organizacją non-profit, która sprawdza m.in. wypowiedzi polityków oraz ich obietnice wyborcze, https://www.politifact.com/, [09.05.2022].

[132] https://par.nsf.gov/servlets/purl/10111583, [09.05.202].

[133] Tech & Check to zbiór produktów i narzędzi, które wykorzystują automatyzację i inne technologie, aby poszerzyć zasięg weryfikacji faktów i pomóc osobom weryfikującym fakty w wykonywaniu ich pracy, https://reporterslab.org/tech-and-check/, [09.05.2022].

[134] https://reporterslab.org/squash-report-card-improvements-during-state-of-the-union-and-how-humans-will-make-our-ai-smarter/, [09.05.2022].

[135] https://fullfact.org/blog/2020/jul/afc-global/, [09.05.2022].

Zakończenie

Przeprowadzone badania nad dezinformacją i propagandą w sektorze bankowym zostały zrealizowane przez zespół Morskiego Centrum Cyberbezpieczeństwa w składzie:

dr hab. inż. Piotr Dela – kierownik zespołu, autor rozdziału 1, 2.

dr Jakub Syta – autor rozdziału 4 i współautor rozdziału 3.

dr inż. Robert Janczewski – autor rozdziału 5 i współautor rozdziału 3.

Przeprowadzone badania ukierunkowane były na realizację głównego celu określonego jako **Zidentyfikowanie i zamodelowanie współczesnego wymiaru dezinformacji i propagandy mogących mieć wpływ na sektor bankowy.** Dodatkowo określono sześć celi szczegółowych:

1. Charakterystyka współczesnej dezinformacji.
2. Charakterystyka współczesnej propagandy.
3. Określenie celów realizowanych w kampaniach informacyjnych.
4. Opracowanie modelu zjawiska.
5. Wskazanie sposobów identyfikowania dezinformacji i propagandy.
6. Identyfikacja narzędzi wykorzystywanych w zwalczaniu dezinformacji i propagandy.

Zostały one odzwierciedlone w rozdziale 1 – cel 1 i 2; w rozdziale 2 – cel 3; w rozdziale 3 – cel 4; w rozdziale 4 – cel 5 i w rozdziale 5 – cel 6.

W wyniku przyjętej procedury badawczej i zastosowanych metod badawczych cele te zostały zrealizowane, niemniej jednak autorzy zdają sobie sprawę z tego, że opracowanie nie wyczerpuje całości złożonej problematyki dezinformacji i propagandy w sektorze bankowym. Dotyczy to zwłaszcza modeli propagandy i dezinformacji, które zostały przedstawione w formie scenariuszy. Powinny one zostać poddane dalszym badaniom na poziomie państwa. Wynika to przede wszystkim ze złożoności zjawiska, mnogości podmiotów prowadzących kampanie informacyjne i przyjętych celów oddziaływania. Sektor bankowy, choć ważny dla funkcjonowania państwa, jest tylko jednym z wielu elementów infrastruktury krytycznej państwa. Dlatego też dalsze badania nad modelami dezinformacji i propagandy powinny być prowadzone przez zespół interdyscyplinarny, uwzględniający inne krytyczne elementy stanowiące o bezpieczeństwie podmiotu, jakim jest państwo.

Należy podkreślić, że propaganda i dezinformacja są procesami zaplanowanymi w czasie, krótkookresowymi (taktyczna) lub długookresowymi (strategiczna) ukierunkowanymi na realizację przyjętych celów politycznych, ekonomicznych, społecznych i innych. Cel propagandy i dezinformacji jest uwarunkowany zdolnościami podmiotu, który realizuje kampanię informacyjną. Wymienione zdolności wyrażają się w głównej mierze posiadanym potencjałem ludzkim i finansowym niezbędnym do realizacji kampanii propagandowych i dezinformacyjnych.

Autorzy wyrażają przekonanie, że przedstawione sposoby identyfikowania i zwalczania wrogich kampanii informacyjnych znajdą swoje odzwierciedlenie w implementacji systemów prewencji przed dezinformacją i propagandą i w znacznym stopniu przyczynią się do zwiększenia bezpieczeństwa sektora bankowego.

Bibliografia

AAP-31(A) Słownik terminów i definicji dotyczących systemów łączności i informatyki NATO, STANAG 5064, Agencja Standaryzacji NATO, 2001.

Ajir M., Vailliant B., *Russian Information Warfare: Implications for Deterrence Theory,* [w:] Strategic Studies Quarterly, Fall 2018, *s. 72*, https://www.jstor.org/stable/26481910?seq=1#metadata_info_tab_contents

Aleksandrowicz T., *Podstawy walki informacyjnej,* Editions Spotkania, Warszawa 2016.

Aronson E., Pratkanis A., *Wiek propagandy*, Państwowe Wydawnictwo Naukowe, Warszawa 2004.

Bojarski W., *Podstawy analizy i inżynierii systemów*, Państwowe Wydawnictwo Naukowe, Warszawa 1984.

Chorobiński A., *Walka informacyjna jako fundamentalny składnik działalności terrorystycznej w przyszłości*; http://konkursy.byd.pl/userfiles/files/chorobinski.pdf

Ciborowski L., *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń 1999.

Clausewitz C., *O wojnie*, Wydawnictwo Test, Lublin 1995.

Conserva H. T., *Propaganda Techniqes*, AuthorHouse, Bloomington 2003.

Dubisz S., *Uniwersalny słownik języka polskiego*, t. I, Wydawnictwo PWN, Warszawa 2003

Dziak J.J., *Chekisty: A History of the KGB,* Lexingon Books, Lexington 1987.

Fake news and disinformation online, Survey requested by the European Commission, Directorate-General for Communications Networks, Content & Technology and co-ordinated by the Directorate-General for Communication, Flash Eurobarometer 464, kwiecień 2018.

Fehler W., *Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i prawne*, Wydawnictwo Arte, Warszawa 2012.

Flakiewicz W., *Podejmowanie decyzji kierowniczych*, Państwowe Wydawnictwo Ekonomiczne, Warszawa 1973.

Foreign Propaganda, Perceptions, and Policy. The Institute of World Politics, Washington D.C.

Garber W., *Propaganda Analysis—to what ends,* The American Journal of Sociology, Chicago 1942.

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania,* Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.

Godston R., Wirtz J.J., *Strategic denial and decption: the twenty-first century challenge*, National Strategy-Information Center, Washington, D.C. 2012.

Jaskuła S., *Informacyjna przestrzeń tożsamości*, Materiały Szkoleniowe Ośrodka Rozwoju Edukacji, ORE, Warszawa 2010.

Jowert G.S., O'Donnell V., *Propaganda and persuasion*, Sage Publications, Washington D.C. 2006.

Kacała T., *Komunikacja strategiczna*, [w:] Przegląd Morski nr 3/2012.

Kuzior A., Kwiliński A., *Zarządzanie refleksyjne – prolegomena*, https://www.researchgate.net/publication/353352807_Zarzadzanie_refleksyjne_-_prolegomena_A_Kuzior_A_Kwilinski

Kwećka R., *Strategia bezpieczeństwa informacyjnego państwa*, Akademia Obrony Narodowej, Warszawa 2014.

Lewczenko S., *Private Channel* [w:] *Influence: A KGB Disinformation Tool, Counterpoint: A monthly report on Soviet Active Measures*, t. 3, kwiecień 1988 nr 11.

Linebarger P.M.A., *Psychological warfare*, Combat Forces Press, Washington D.C. 1954, Second Edition Reprinted by Combat Forces Press, Washington, D.C. 1972.

Markowski A., *Wielki słownik poprawnej polszczyzny*, Wydawnictwo PWN, Warszawa 2004.

Mazur M., *Cybernetyka i charakter,* WSZiP im. Bogdana Jańskiego w Warszawie, Warszawa 1999.

Mazur M., *Jakościowa teoria informacji*, Wydawnictwo Naukowo Techniczne, Warszawa 1970.

Nowa encyklopedia powszechna PWN, tom 4, Wydawnictwo Naukowe PWN, Warszawa 1996.

Nowakowski Z., Szafran H., Szafran R., *Bezpieczeństwo w XXI wieku. Strategia bezpieczeństwa narodowego Polski i wybranych państw*, Towarzystwo Naukowe Powszechne, Rzeszów 2009.

Nowicka J., Załoga W., Ciekanowski Z., *Komunikacja strategiczna w naukach o zarządzaniu i jakości oraz w naukach o bezpieczeństwie*, „Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach", 2018 nr 1 (14).

Pacepa I. M., Rychlak R. J., *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu*, Helion, Gliwice 2013.

PN-I-02000:2002 *Technika informatyczna – Zabezpieczenie w systemach informatycznych – Terminologia*, Polski Komitet Normalizacyjny, Warszawa 2002.

PN-I-02000:2002 Technika Informatyczna – Zabezpieczenie w systemach informatycznych – Terminologia.

Regulamin działań wojsk lądowych nr 115/2008, DWLąd, Warszawa 2008.

Shultz R.H., Godson R.: *Dezinformatsia. Active Measures in Soviet Strategy*, Pergamon Press, Nowy Jork 1984.

Sienkiewicz P., *Systemy kierowania,* Wiedza Powszechna, Warszawa 1989.

Słownik języka polskiego, t. I, Wydawnictwo Naukowe PWN, Warszawa 1993.

Słownik języka polskiego, Wydawnictwo Naukowe PWN, Warszawa 2007.

Słownik terminów z zakresu bezpieczeństwa narodowego, Akademia Obrony Narodowej, Warszawa 2008.

Sułek M., *Trzy działy prakseologii*, „Rocznik Naukowy Wydziału Zarządzania w Ciechanowie Wyższej Szkoły Menadżerskiej w Warszawie", z. 12, t. II, Ciechanów 2008, s. 2, www.mises.pl

Sun Tzu, *Sztuka wojny,* Wydawnictwo Przedświt, Warszawa 1994.

Tarczydło B., *Kampania społeczna w teorii i praktyce*, AGH, Kraków, źródło: https://www.ue.katowice.pl/fileadmin/_migrated/content_uploads/19_B.Tarczydlo_Kampania_spoleczna_w_teorii_i_praktyce.pdf

The Embassies and Foreign Affairs, „The Whitehall Gazette & St James's Review", Londyn 1926.

Volkoff V., *Psychosocjotechnika*, d*ezinformacja oręż wojny*, Antyk, Warszawa 1999.

Wielka encyklopedia PWN, tom 17, Wydawnictwo naukowe PWN, Warszawa 2003.

Wiener N., *Cybernetics: Or Control and Communication in the Animal and the Machine,* (Hermann & Cie) & Camb. Mass. (MIT Press), Paris 1948.

Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI wieku*, Przegląd Bezpieczeństwa Wewnętrznego nr 12/15.

Wrzosek M., *Dezinformacja jako komponent operacji informacyjnej*, Akademia Obrony Narodowej, Warszawa 2005.

https://www.investopedia.com/terms/b/bernard-madoff.asp

https://sjp.pwn.pl/sjp/dezinformacja;2554971.html

https://www.thesun.co.uk/tech/17574335/tesla-reveals-secret-bitcoin-stash-worth-2billion-elon-musk/

https://www.theguardian.com/technology/2021/may/12/elon-musk-tesla-bitcoin

https://www.knf.gov.pl/knf/pl/komponenty/img/Dobre%20praktyki%20w%20zakresie%20przeciwdzia%C5%82ania%20atakom%20DDoS_77247.pdf

https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf

https://www.manrs.org/

https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

https://www.scmp.com/news/china/military/article/3025403/john-bolton-accuses-china-stealing-f-35-technology-make-stealth

https://www.cybsecurity.org/pl/analiza-nowej-doktryny-informacyjnej-rosji/,

https://alebank.pl/120-tys-fejkow-dziennie-w-polskim-internecie-od-rosyjskich-trolli/?id=403919&catid=25926

https://www.claimsjournal.com/news/national/2020/01/06/294849.htm

https://www.bankinfosecurity.com/sony-pictures-cyber-attack-timeline-a-7710

https://www.ll.mit.edu/r-d/projects/reconnaissance-influence-operations

http://twittertrails.com/

http://www.emergent.info/about

https Iffy Quotient://hoaxy.osome.iu.edu

https://aclanthology.org/P19-3026.pdf

https://addons.mozilla.org/pl/firefox/addon/trustedtimes/

https://arxiv.org/pdf/1904.02037.pdf

https://arxiv.org/pdf/2103.07769.pdfhttps://captainfact.io/

https://chrome.google.com/webstore/detail/ad-observer/enliecaalhkhhihcmnbjfmmjkljlcinl

https://chrome.google.com/webstore/detail/know-news/bmlfbcipfpdohbhhlkibdiacikbpaofm

https://counteringdisinformation.org/index.php/interventions/fakerfact

https://csmr.umich.edu/projects/iffy-quotient/

https://disinformationindex.org/the-index/

https://en.wikipedia.org/wiki/Nudge_theory

https://exifdata.com/index.php

https://fullfact.org/blog/2020/jul/afc-global/

https://idir.uta.edu/claimbuster/

https://idir.uta.edu/claimbuster/

https://ifcncodeofprinciples.poynter.org/know-more/the-commitments-of-the-code-of-principles

https://mediabiasfactcheck.com/about/

https://osome.iu.edu/tools/botslayer

https://our.news/how-it-works/?main

https://par.nsf.gov/servlets/purl/10111583

https://reporterslab.org/duke-students-tackle-big-challenges-in-automated-fact-checking/

https://reporterslab.org/squash-report-card-improvements-during-state-of-the-union-and-how-humans-will-make-our-ai-smarter/

https://reporterslab.org/tech-and-check/

https://securingdemocracy.gmfus.org/hamilton-dashboard/

https://whotargets.me/en/about/

https://www.ibm.com/pl-pl/topics/what-is-blockchain

https://www.io-archive.org/#/

https://www.ll.mit.edu/r-d/projects/reconnaissance-influence-operations

https://www.newscheck.com

https://www.politifact.com/

https://www.rand.org/research/projects/truth-decay/fighting-disinformation.html

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html#q=&typeOfTool=Bot%2Fspam+detection&typeOfTool=Codes+and+standards

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html#q=&typeOfTool=-Credibility+scoring

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/newscheck-trust-index.html

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/opensources.html

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/who-targets-me.html

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/crosscheck.html

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/misinformation-detector.html

https://www.sciencedirect.com/topics/computer-science/deep-neural-network

https://www.thefactual.com

https://www.rand.org/research/projects/truth-decay/fighting-disinformation.html

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html#q=&typeOfTool=Bot%2Fspam+detection&typeOfTool=Codes+and+standards

https://en.wikipedia.org/wiki/Nudge_theoryhttps://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html#q=&typeOfTool=Credibility+scoring

https://disinformationindex.org/the-index

https://counteringdisinformation.org/index.php/interventions/fakerfact

https://chrome.google.com/webstore/detail/know-news/bmlfbcipfpdohbhhlkibdiacikbpaofmhttps://mediabiasfactcheck.com/about/

https://ifcncodeofprinciples.poynter.org/know-more/the-commitments-of-the-code-of-principleshttps://www.newscheck.com

https://www.ibm.com/pl-pl/topics/what-is-blockchain

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/newscheck-trust-index.html

https://our.news/how-it-works/?main

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/opensources.html https://www.thefactual.com

https://addons.mozilla.org/pl/firefox/addon/trustedtimes/

https://osome.iu.edu/tools/botslayer

https://chrome.google.com/webstore/detail/ad-observer/enliecaalhkhhihcmnbjfmmjkljlcinl

https://securingdemocracy.gmfus.org/hamilton-dashboard/

https://csmr.umich.edu/projects/iffy-quotient/

https://www.io-archive.org/#/

http://twittertrails.com/

https://whotargets.me/en/about/

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/who-targets-me.html

https://captainfact.io/

https://idir.uta.edu/claimbuster/

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/crosscheck.html

https://reporterslab.org/duke-students-tackle-big-challenges-in-automated-fact-checking/

http://www.emergent.info/about

https://exiftool.org/

https://exifdata.com/index.php

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/misinformation-detector.html

https://arxiv.org/pdf/2103.07769.pdf

https://arxiv.org/pdf/1904.02037.pdf

https://www.sciencedirect.com/topics/computer-science/deep-neural-network

https://aclanthology.org/P19-3026.pdf

https://idir.uta.edu/claimbuster/

https://www.politifact.com/

https://par.nsf.gov/servlets/purl/10111583

https://reporterslab.org/tech-and-check/

https://reporterslab.org/squash-report-card-improvements-during-state-of-the-union-and-how-humans-will-make-our-ai-smarter/

https://fullfact.org/blog/2020/jul/afc-global/

https://pl.sputniknews.com/swiat/2020022111965248-sputnik-to-sredniowiecze-rzeczniczka-msz-rosji-skomentowala-protesty-na-ukrainie/

https://edition.cnn.com/2013/09/11/us/edward-snowden-fast-facts/index.html

Raport przygotowany na zlecenie Fundacji
Warszawski Instytut Bankowości

PROGRAM
ANALITYCZNO
BADAWCZY