ROCZNIKI NAUK SPOŁECZNYCH
Tom 15(51), numer 2 – 2023
DOI: https://doi.org/10.18290/rns2023.0017

KRZYSZTOF KACZMAREK

DEZINFORMACJA JAKO CZYNNIK RYZYKA W SYTUACJACH KRYZYSOWYCH

DISINFORMATION AS A RISK FACTOR IN CRISIS SITUATIONS

A b s t r a c t. False and rapidly disseminated information can model public sentiment, influence the results of democratic elections, create tensions in the international arena, and even cause armed conflicts. In the event of a crisis, disinformation may be a tool used to destabilize the internal situation of the state. In such a situation, unauthorized access to classified information may also have serious consequences.

Contemporary digital devices and the systems that manage them do not require the average user to have fluent knowledge of IT systems and technical skills. However, the development of modern technologies determines the need for constant updating of knowledge in this field. It applies in particular to people who deal with the broadly understood state security.

Keywords: crisis situation; disinformation; information security; information verification; deep fake.

WPROWADZENIE

Globalne rozprzestrzenianie się fałszywych informacji i wszechobecna dezinformacja stanowią poważne zagrożenie dla funkcjonowania społeczeństwa demokratycznego, w tym dla jego spójności, zdrowia publicznego i stabilności politycznej. Zdrowa demokracja wymaga świadomych, podejmowanych na podstawie prawdziwych informacji, decyzji. Natomiast fałszywe informacje mają negatywny wpływ na przekonania społeczne dotyczące zdrowia, nauki, międzykulturowości czy kwestii społecznych. Poza polaryzacją i radykalizacją społeczeństw, fałszywe i zmanipulowane treści (takie jak np. „spożywanie chloru leczy COVID-19") mogą być nie tylko niebezpieczne dla zdrowia, ale stanowić śmiertelne zagrożenie (Rey, 2021).

Dr KRZYSZTOF KACZMAREK – Politechnika Koszalińska, Wydział Humanistyczny, Katedra Studiów Europejskich; adres do korespondencji: ul. Kwiatkowskiego 6e, 75-343 Koszalin; e-mail: puola1972@gmail.com; ORCID: https://orcid.org/0000-0001-8519-1667.

Istotą dezinformacji jest celowe tworzenie i dystrybucja fałszywych lub zmanipulowanych treści oraz wywoływanie określonych zachowań społecznych. Może ona zatem oddziaływać destrukcyjnie na funkcjonowanie państwa (Chałubińska-Jentkiewicz, 2021a, s. 14). Akcje dezinformacyjne mogą świadczyć o przygotowaniach do przeprowadzenia operacji wojskowej, a nawet klasycznej wojny. Mogą także stanowić element działań nieregularnych łączących konwencjonalne działania zbrojne z operacjami przeprowadzanymi przez cywilów (Pietras, 2021, s. 25). Akcje te są zazwyczaj długotrwałe i ukierunkowane na wywołanie i wzmacnianie podziałów społecznych oraz podważanie zaufania do instytucji państwa (Pietras, 2021, s. 25). Dezinformacja może nie tylko kreować sytuacje kryzysowe, ale również być wykorzystywana do eskalacji niepokojów społecznych w czasie istniejących kryzysów. Tym samym dezinformacja możne stanowić część wrogich działań ukierunkowanych na skłanianie odbiorcy do pożądanych zachowań. Dlatego jednym z najistotniejszych działań mających na celu walkę z tego typu działaniami jest edukacja, której głównym efektem powinna być umiejętność samodzielnego, bez wpływu czynników trzecich, weryfikowania informacji (Gergelewicz, 2022, s. 74). Jest to o tyle istotne, że fałszywe wiadomości są podchwytywane i powtarzane nawet przez media głównego nurtu, np. agencja informacyjna Reuters była w przeszłości znaczącym dystrybutorem fałszywych wiadomości generowanych przez rosyjskie źródła (Rock Dove Solution, 2021).

Analizując możliwe akcje dezinformacyjne w czasie rzeczywistych sytuacji kryzysowych mogących wystąpić na terytorium Polski, należy przyjąć definicję takiej sytuacji. Dla celów niniejszego opracowania zostało przyjęte,

> iż sytuację kryzysową należy rozpatrywać jako splot gwałtownych zdarzeń, powodujących wzrastający wpływ sił destabilizujących równowagę w społeczeństwie, braki w zaopatrzeniu i trudności w normalnym funkcjonowaniu ludności, co wywołuje napięcia i niepewność oraz prowadzi do niekontrolowanego rozwoju wydarzeń z użyciem przemocy włącznie (Bąk, 2017, s. 9).

Dla dokonania analizy możliwych oddziaływań akcji dezinformacyjnych na wywołanie sytuacji kryzysowej i/lub zarządzanie nią, autor przeanalizował literaturę przedmiotu (metoda analizy literatury), ze szczególnym uwzględnieniem pozycji dotyczących dezinformacji. Poddane analizie zostały również doniesienia prasowe (wydania internetowe) dotyczące skutków rozprzestrzeniania się teorii spiskowych i fałszywych informacji oraz dane udostępnione przez zewnętrzne podmioty badawcze. Natomiast przy analizowaniu możliwych zachowań społecznych w przypadku działań dezinformacyjnych została wykorzystana metoda behawioralna.

DEZINFORMACJA W CZASIE SYTUACJI KRYZYSOWEJ

Podstawą skutecznej dezinformacji jest zbudowanie wiarygodności jej źródła. Przykładem są działania Seftona Delmera w czasie II wojny światowej. Stworzył on postać Der Chefa, rzekomego pruskiego oficera i zagorzałego nazisty. Od maja 1941 roku wypowiadał się on w audycjach radiowych nadawanych na teren Niemiec w taki sposób, aby nie budzić wątpliwości co do swojego oddania dla III Rzeszy. Jednocześnie wprowadzał w umysł odbiorcy szereg impulsów, które skutkowały wzbudzaniem wątpliwości co do słuszności działań ówczesnych władz Niemiec (Makuch, 2021, s. 163).

Choć niepożądana, dezinformacja stała się wszechobecna w cyfrowym świecie. Propaganda i fałszywe informacje mają długą historię. Jednak dopiero rewolucja cyfrowa umożliwiła bezprecedensowe rozprzestrzenianie się dezinformacji. Zjawisko to nasiliło się w sytuacjach kryzysowych, takich jak pandemia COVID-19 i agresja Rosji na Ukrainę. Chociaż wiele obaw skupia się na tym, jak dezinformacja wpływa na dyskurs internetowy i dobrobyt społeczny, to, w jaki sposób przejawia się ona w fizycznych szkodach w świecie rzeczywistym, jest stosunkowo słabo rozumiane, zwłaszcza podczas sytuacji kryzysowych (Xu, 2021).

Dyskusje dotyczące dezinformacji często analizują zachowania aktorów lub botów – w końcu automatyzacja cyfrowa umożliwiła rozprzestrzenianie się dezinformacji na skalę i szybkość niespotykaną nigdy wcześniej. Chociaż boty i złośliwi aktorzy rozprzestrzeniają i rozsiewają dezinformację, to duża część problemu dotyczy samego ekosystemu informacyjnego, który jest siecią ludzi kształtowaną przez sposób, w jaki dzielą się oni informacjami i reagują na nie. Fałszywe informacje w odosobnieniu są stosunkowo nieszkodliwe. Stają się szkodliwe dopiero wówczas, gdy ludzie przyswajają informacje, interpretują je z własnymi uprzedzeniami i czują wewnętrzny przymus działania. Istnieje szereg cech, które sprawiają, że obecne środowisko informacji cyfrowej jest podatnym gruntem dla dezinformacji (Xu, 2021).

Przede wszystkim fałszywe informacje rozprzestrzeniają się szybciej niż prawdziwe. W szeroko zakrojonych badaniach fałszywych wiadomości Massachusetts Institute of Technology odkrył, że rozprzestrzeniają się one średnio sześć razy szybciej niż prawdziwe. Okazało się, że nie jest to efekt działania botów; boty dzieliły się prawdą i fałszem w mniej więcej takim samym tempie. W rzeczywistości to ludzie częściej dzielili się fałszywymi informacjami. Badanie wykazało dwie cechy fałszywych informacji, które mają przewagę nad prawdziwymi: nowość i – najczęściej negatywne – emocje. Fałszywe in-

formacje są prawdopodobnie nowe (ze względu na fakt, że są w rzeczywistości fałszywe) i naładowane emocjami (ponieważ często mają na celu wywołanie reakcji) (Vosoughi, Roy i Aral, 2018, s. 1146-1151). Bez krytycznego zaangażowania i edukacji cyfrowej odbiorcy fałszywa informacja przykuwa uwagę, a emocje powodują, że przekazuje ją on dalej.

Ponadto, jest po prostu za dużo informacji. Tradycyjnie fałszywe informacje mogą być wyeliminowane poprzez weryfikację przez zaufane źródła, niezależne sprawdzanie faktów i/lub indywidualny zdrowy rozsądek. Jednak w obecnym środowisku informacyjnym sama ilość informacji jest przytłaczająca, a szum informacyjny sprawia, że niemal każda informacja może wydawać się potencjalnie prawdziwa. Zalanie środowiska informacyjnego jest powszechną taktyką dezinformacyjną stosowaną przez aktorów w celu destabilizacji dyskursu publicznego. Co więcej, media społecznościowe nie mają standardów dziennikarskich ani reporterskich. W Internecie każdy może podzielić się swoimi poglądami i, teoretycznie, opinia każdego jest równie ważna. Aby utorować sobie drogę przez chaos, użytkownicy częściej wracają do własnych uprzedzeń i szukają informacji, które zgadzają się z ich światopoglądem i go potwierdzają (Xu, 2021).

W związku z tym dezinformacja sama się napędza. Plotki wzbudzają strach i uprzedzenia. Ludzie są bardziej skłonni do zaakceptowania plotek, jeśli się boją, są niepewni swojej przyszłości, czują się bezbronni lub mają niską sprawczość. W szumie informacyjnym uprzedzenia dają im względne poczucie stabilizacji. Informacje, które potwierdzają ich poglądy, są zatem łatwiej akceptowane niż informacje, które mogą im zaprzeczać, co z kolei rodzi więcej uprzedzeń i strachu, a tym samym większe prawdopodobieństwo zaakceptowania i przekazania stronniczych lub fałszywych informacji w przyszłości. Fakt, że ludzie mają tendencję do gromadzenia się w podobnie myślących grupach, jeszcze bardziej umacnia te bańki informacyjne (Xu, 2021).

Strach i uprzedzenia osiągają szczyt podczas kryzysów. Plotki i teorie spiskowe mogą powodować dyskryminację i przemoc wobec określonych grup społecznych. Kryzysy prowadzą również do zwiększonego wykorzystania opartych na danych narzędzi cyfrowych w celu powstrzymania rozprzestrzeniania się i alokacji zasobów. W czasie kryzysu i w obliczu zwiększonej dezinformacji i uprzedzeń, a także zwiększonego gromadzenia i wykorzystywania danych, również istotne znaczenie ma ochrona danych osobowych (Xu, 2021).

Jednakże środowisko kryzysowe może w rzeczywistości utrudnić ochronę tych danych. Na przykład w przeciążonym środowisku informacyjnym, w którym nieprawdziwe informacje mają naturalną przewagę, ludziom trudno jest odróżnić

bezpieczne, zgodne z prawem wysiłki w zakresie przetwarzania danych od niezgodnego z prawem gromadzenia danych lub oszustw. Jest to szczególnie niepokojące w czasach kryzysu, ponieważ ludzie chętniej poświęcają swoje dane osobowe, prawa i wolności w celu zagwarantowania bezpieczeństwa i ochrony. Ponadto, dane mogą być wykorzystywane do mikrotargetowania (Xu, 2021).

DYWERSJA INFORMACYJNA

Od wielu lat Polska jest obiektem ataków dezinformacyjnych ze strony Federacji Rosyjskiej (Serwis Rzeczypospolitej Polskiej). Jednak agresja Rosji na Ukrainę uruchomiła niespotykaną wcześniej falę dezinformacji. Fake newsy w polskojęzycznej cyberprzestrzeni dotyczyły między innymi problemów z dostępnością obywateli do prywatnych środków finansowych, przerw w dostawach paliw czy odnoszących się do skażenia radioaktywnego (Portal Bankowości Spółdzielczej, 2022). Rzeczywistymi skutkami tej fali dezinformacji były czasowy brak paliw na niektórych stacjach czy niedostępność gotówki w bankomatach. O tym, jak niebezpieczna może być dezinformacja związana z wojną w Ukrainie, informowała policja już w pierwszych dniach rosyjskiej agresji (Policja.pl, 2022).

Jak podaje Instytut Badania Internetu i Mediów Społecznościowych w opublikowanym 23 lutego 2022 raporcie, w okresie 21-22 lutego 2022 roku, a więc bezpośrednio poprzedzającym atak Rosji na Ukrainę, dynamicznie wzrosła liczba fake newsów mających na celu wywołanie negatywnych emocji w stosunku do władz i obywateli Ukrainy. W badaniach wykazano również, że w tej kampanii dezinformacyjnej udział brały te same konta w mediach społecznościowych, które uczestniczyły wcześniej w dystrybuowaniu treści sceptycznych wobec szczepień i istnienia pandemii COVID-19 (Instytut Badań Internetu i Mediów Społecznościowych, 2022).

Analizując dywersję informacyjną należy wspomnieć o technologii deepfake, która pozwala na realistyczne przedstawienie wypowiedzi i działań, które nigdy nie miały miejsca (Chałubińska-Jentkiewicz, 2021a, s. 14). Biorąc pod uwagę to, jak bardzo współczesne społeczeństwa są zależne od Internetu zarówno pod względem informacji, jak i rozrywki, oraz to, jak ludzie aktywnie zniekształcają rzeczywistość tworząc satysfakcjonujące ich treści, czasami trudno jest odróżnić rzeczywistość od fikcji. Jedną z implikacji, która wynika z deepfake, jest sytuacja, w której staje się ona „dowodem" działań danej osoby lub grupy

osób. Dzięki deepfake dywersja informacyjna może być bardziej skuteczna. Ze względu na zwiększającą się liczbę i zasięg teorii spiskowych technologia deepfake będzie prawdopodobnie miała coraz większy wpływ na życie ludzi (Garbo, 2021).

Nie można wykluczyć, że w przypadku zaistnienia sytuacji kryzysowej możliwy będzie „wyciek" spreparowanej, przedstawiającej „prawdziwy" obraz sytuacji, wypowiedzi kogoś odpowiedzialnego za bezpieczeństwo. Takie działania mogą spowodować zagrożenie dla bezpieczeństwa publicznego, a nawet dla bezpieczeństwa państwa.

W przypadku działań dywersyjnych kanały dystrybucji dezinformacji w znacznej części opierają się na zradykalizowanych grupach, których postrzeganie otoczenia nosi znamiona przynależności do sekt. Ich członków scharakteryzowała Eugenia Ewa Mandal:

> • wyłączna prawda – członkowie sekt uważają, że tylko oni mają wyłączne prawo do prawdy, świat zaś zmierza do katastrofy i jedynie oni wiedzą, jak go ratować,
> • misjonarska gorliwość,
> • członkowie sekt wierzą, że muszą ratować świat, jako jedyni znający prawdę, bez ich działalności świat byłby skazany na zagładę i potępienie,
> • nadrzędność grupy – sekta uważa się za grupę elitarną, pozostałych traktując jak chorych i zagubionych, jeżeli nie przyłączą się do sekty, nie będą zbawieni (uratowani),
> • charyzmatyczne przywództwo – sekta ma mistrza, ojca, myśliciela, który posiadł całą prawdę, jest inny od zwykłych ludzi, ma wyjątkową moc, jest czczony jak Bóg,
> • ścisła dyscyplina – dyscyplina w sekcie przyjmuje formę kontroli nad wszystkimi aspektami życia (ubiór, fryzura, język, dieta, seks), sekta wypełnia czas jej członkom tak, że nie mają czasu na nic innego niż działalność w sekcie: w sekcie pracują, sprzedają książki, werbują nowych członków, medytują itd.,
> • dławienie indywidualizmu – sekty nie akceptują osób niezależnych, buntowników, dlatego kształcenie nowicjuszy skupia się na dławieniu indywidualności, sekty odrzucają racjonalne myślenie jako „negatywne", przyjmując zasadę: „tego nie da się wyjaśnić, to trzeba przeżyć, czuć" (tzw. przeżycie kluczowe) (Mandal, 1998, s. 20).

Można zauważyć, że grupy zbudowane na bazie teorii spiskowych (dotyczących między innymi szczepień) cechują niemal wszystkie wyżej wymienione atrybuty (Termedia, 2012).

Nie jest zatem możliwe, aby do osób wierzących w teorie spiskowe trafiały jakiekolwiek logiczne argumenty. Mając swoje „wiarygodne" źródła informacji, bardzo chętnie rozpowszechniają fake newsy; tym bardziej że w swoim przekonaniu „ratują" innych. Jednak najistotniejsze jest to, kto stoi za tymi źródłami. Poczucie zagrożenia jednostki w sytuacji kryzysowej jest subiektywne, a część społeczeństwa po prostu nie wierzy w samo istnienie takiej sytuacji

zakładając, że „za wszystkim stoją potężne siły o wrogich zamiarach" (Komisja Europejska). Poglądy takie nie są groźne do momentu, kiedy osoby je reprezentujące nie próbują wpływać na funkcjonowanie instytucji i służb zarządzających sytuacją kryzysową. Przykładem były agresywne zachowania antyszczepionkowców wobec pracowników ochrony zdrowia w czasie akcji promujących szczepienia przeciwko COVID-19 (Sejm Rzeczypospolitej Polskiej, 2021) czy działania Edgara Maddisona Welcha w Waszyngtonie w 2016 roku (Blaekley, 2021). Brzemienne w skutkach mogą okazać się skoordynowane, mające na celu destabilizację państwa, akcje dezinformacyjne wykorzystujące rzeczywiste sytuacje kryzysowe.

O tym, w jaki sposób szybko rozpowszechniające się (choć brzmiące wiarygodnie, to jednak fałszywe) informacje mogą wpływać na zachowania społeczne, świadczą chociażby masowe zakupy paliwa i wypłaty gotówki z bankomatów kilkanaście godzin po ataku Rosji na Ukrainę (Wirtualna Polska, 2022). Innym przykładem są informacje o rzekomych, bliżej nieokreślonych zagrożeniach w warszawskim metrze. Rozpowszechniająca się na początku lat 2000. pogłoska o nich skutkowała paniką części korzystających z tego środka transportu i zaangażowaniem znacznych sił policyjnych w celu sprawdzenia wszystkich niepokojących doniesień (Policja.pl., 2007).

OCHRONA INFORMACJI W CZASIE SYTUACJI KRYZYSOWEJ

W dobie cyfryzacji działań administracji publicznej ochrona danych i informacji stała się jednym z ważniejszych działań. Dotyczy to zwłaszcza informacji wrażliwych (Hoffman i Cseh, 2020, s. 200), a zapewnienie cyberbezpieczeństwa jest jednym z zadań zarówno administracji rządowej, jak i samorządu terytorialnego. Cyberbezpieczeństwo, jako przedmiot działań publicznych, jest również aspektem poruszanym w dokumentach planistycznych. Definiuje się je jako czynności, które są niezbędne do ochrony sieci i systemów komputerowych oraz użytkowników tych systemów przed cyberzagrożeniami (Karpiuk, 2021, s. 46).

W przypadku sytuacji kryzysowych dezinformacja może być wykorzystywana na dwa główne sposoby. Pierwszy to wywołanie zachowań społecznych mogących zdestabilizować sytuację na obszarze kryzysu, a drugi to uzyskanie dostępu do kanałów informacyjnych wykorzystywanych przez służby, których zadaniem jest zarządzanie zaistniałą sytuacją. Implikacją takiego dostępu może być uzyskanie przez osoby trzecie informacji niejawnych oraz ich upublicznienie i/lub zużytkowanie do ingerowania w zarządzanie sytuacją kryzysową.

Taki wpływ może odbywać się poprzez zniekształcanie lub fałszowanie informacji wymienianych pomiędzy instytucjami (i/lub osobami) zarządzającymi sytuacjami kryzysowymi.

Upublicznienie niektórych informacji może spowodować, że część sił biorących bezpośredni udział w zarządzaniu kryzysem lub zwalczaniu jego skutków musi zostać zaangażowana w takie działania, jak udrażnianie dróg ewakuacyjnych czy ochronę jakiegoś obszaru przed dostępem osób nieuprawnionych. Kolejną implikacją ujawnienia informacji niejawnych może być uzyskanie przez osoby niepowołane dostępu do materiałów niebezpiecznych, które potencjalnie mogą być wykorzystane do działań przestępczych lub terrorystycznych. Dodać trzeba, że do wyprodukowania materiałów wybuchowych mogą być użyte nawet takie substancje, jak nawozy sztuczne czy środki ochrony roślin (Zimniewicz, 2014, s. 307).

Jednakże bez względu na procedury i wykorzystywane środki techniczne najsłabszym elementem ochrony informacji jest jej użytkownik. Dotyczy to zwłaszcza osób mających autoryzowany dostęp do systemów teleinformatycznych. Okazuje się bowiem, że w skali globalnej około 95% skutecznych cyberataków jest skutkiem błędu człowieka, a nie systemu (Włodyka, 2022, s. 216).

Ostrożność w czasie korzystania z Internetu powinni zachowywać wszyscy. Jednak z punktu widzenia bezpieczeństwa informacji związanych z zarządzaniem sytuacjami kryzysowymi, szczególną powinni zachowywać ci, którzy mają dostęp do kanałów łączności służb i używają do tego celu urządzeń mobilnych oraz korzystają z bezprzewodowego dostępu do sieci.

W zdecydowanej większości dostęp do Internetu poprzez sieci telefonii komórkowej podlega limitom. W związku z tym część urządzeń jest ustawiona w taki sposób, aby automatycznie łączyć się z otwartymi (lub zaufanymi) sieciami Wi-Fi, kiedy tylko te są dostępne. Należy w tym miejscu zaznaczyć, że w przypadku nawiązania takiego połączenia istnieje możliwość przejęcia przez osoby postronne wszystkich zapisanych w pamięci urządzenia danych (w tym loginów i haseł), a jego użytkownik może takiego zdarzenia nawet nie zauważyć (Omegasoft, 2020); zwłaszcza że istnieje techniczna możliwość podszywania się dostępnych sieci Wi-Fi pod zaufane (znane).

Zakładając, że urządzenie mobilne przemieszcza się w obszarze zurbanizowanym można przyjąć, iż może ono znaleźć się w zasięgu kilkudziesięciu lub nawet kilkuset sieci Wi-Fi. Przyjmując, że zdarzenia mało prawdopodobne nie są niemożliwe, należy założyć, że istnieje możliwość, iż połączy się ono z siecią, poprzez którą ktoś będzie chciał przejąć zapisane w jego pamięci informacje. Przejęcie loginów i haseł dostępowych do systemów teleinformatycznych

nie oznacza ani ich natychmiastowego wykorzystania, ani nawet takiej możliwości. Może jednak zmniejszyć poziom bezpieczeństwa tych systemów.

Wydaje się, że najlepszym sposobem na uniknięcie tego typu sytuacji jest korzystanie jedynie z bezpiecznego, zaufanego sprzętu. Jednak w czasie sytuacji kryzysowych nie zawsze istnieje taka możliwość. Poza zatem rzeczami oczywistymi, takimi jak posiadanie zainstalowanego profesjonalnego oprogramowania antywirusowego oraz niezapisywanie wprowadzanych haseł, w celu zmniejszenia ryzyka przejęcia przez osoby trzecie zapisanych informacji można wyłączać funkcję Wi-Fi w urządzeniach w czasie niekorzystania z zaufanych sieci. W tym miejscu warto zaznaczyć, że hasła zapisane na urządzeniu mobilnym mogą zostać przejęte również w przypadku utraty tego urządzenia.

Zaistnienie jednej z powyższych, hipotetycznych, sytuacji może stworzyć szczególne zagrożenie dla szeroko rozumianego bezpieczeństwa publicznego, jeżeli przejęte zostaną dane z urządzenia używanego służbowo przez osobę zajmującą się szeroko rozumianym zarządzaniem sytuacjami kryzysowymi; zwłaszcza w przypadku działań osób i instytucji mających na celu destabilizację sytuacji wewnętrznej w państwie.

WNIOSKI

Efektywność prowadzonych przez Rosję działań dezinformacyjnych może prowadzić do wniosku, że państwa autorytarne mają przewagę w wojnie informacyjnej ze względu na sposób sprawowania władzy, ponieważ w systemach demokratycznych podmioty państwowe na ogół nie są w stanie wpływać na działalność mediów (Renz, 2016). Paradoksalnie, tworząc fałszywe obrazy rzeczywistości, autokraci wykorzystują zarówno media tradycyjne, jak i tzw. media społecznościowe powstałe i funkcjonujące w Europie Zachodniej czy Stanach Zjednoczonych. Wydaje się, że chcąc temu zapobiegać wystarczyłoby, aby tacy giganci jak Facebook, Twitter, Google czy Instagram zaczęli w tym celu wykorzystywać odpowiednie narzędzia cyfrowe, którymi dysponują. Jednak wszelkie dyskusje na ten temat kończą się jedynie na deklaracjach. Tymczasem algorytmy polaryzujące społeczeństwa osłabiają Zachód i powodują, że wpływy Rosji na opinię społeczną wciąż są znaczące (Kaczmarek, 2022, s. 57).

Zgodnie z obowiązującym w Polsce prawem nieuprawniony, nawet przypadkowy, dostęp do informacji może zostać uznany za przestępstwo; nawet w przypadku, gdy są one niezabezpieczone w należyty sposób (Behan, 2020, s. 21-35). Należy jednak zwrócić uwagę na to, że w przypadku sytuacji

kryzysowej, kiedy wymagane jest niezwłoczne działanie służb, możliwość dostępu do ich kanałów łączności przez osoby z zewnątrz może mieć poważne konsekwencje, a rozpatrywanie, czy nastąpiło złamanie przepisów, odbywa się dopiero po fakcie. Można hipotetycznie założyć, że w przypadku unieruchomienia (na skutek awarii, wypadku, czynników zewnętrznych) transportu materiałów mogących służyć do produkcji materiałów wybuchowych czy brudnych bomb, służby ratunkowe zostaną przekierowane w inne miejsce. Daje to możliwość przejęcia tych materiałów przez przestępców, terrorystów lub dywersantów. W związku z tym najistotniejsze wydają się prewencja oraz przestrzeganie procedur bezpieczeństwa. Nawet jednorazowe ich zignorowanie przez jednego człowieka może mieć poważne konsekwencje dla całego systemu zarządzania kryzysowego.

BIBLIOGRAFIA

Bąk T. (2017), *Sytuacja kryzysowa*, Zeszyty Naukowe Państwowej Wyższej Szkoły Techniczno-Ekonomicznej im. ks. Bronisława Markiewicza w Jarosławiu. Współczesne problemy zarządzania, nr 10: Bezpieczeństwo publiczne, s. 7-22.

Behan A. (2020), *Współczesne systemy informatyczne a typy przestępstw z art. 267 kodeksu karnego*, Palestra, nr 2, s. 21-36.

Blaekley P. (2021), *Panic, pizza and mainstreaming the alt-right: A social media analysis of Pizzagate and the rise of the QAnon conspiracy*, Current Sociology, t. 71, nr 3, s. 509-525.

Chałubińska-Jentkiewicz K. (2021a), *Dezinformacja jako akt agresji w cyberprzestrzeni*, Cybersecurity and Law, t. 5, nr 1, s. 9-24.

Chałubińska-Jentkiewicz K. (2021b), *Disinformation – and what else*?, Cybersecurity and Law, nr 6(2), s. 9-19.

Garbo (2021), *The Dangers of Deepfakes*, https://www.garbo.io/blog/deepfakes [dostęp: 10.09.2022].

Gergelewicz T. (2022), *Obszary budowania odporności na dezinformację jako element bezpieczeństwa infosfery*, Cybersecurity and Law, t. 7, nr 1, s. 72-84.

Hoffman I. i Cseh K.B. (2020), *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for municipalities in Hungary*, Cybersecurity and Law, t. 4, nr 2, s. 199-211.

Instytut Badań Internetu i Mediów Społecznościowych (2022), *Komunikat ws. Dezinformacji ws. Sytuacji na Ukrainie w internecie*, https://ibims.pl/komunikat-ws-szerzenia-dezinformacji-ws-sytuacji-na-ukrainie-w-polskiej-przestrzeni-internetowej/?fbclid=IwAR0FkgWPHKHxZG2UdKtYN2DTeAsYTbwDZLOwaQ78_ZwZPUC1vBUng4tIl5o [dostęp: 06.09.2022].

Kaczmarek K. (2022), *Appealing to compassion as an element of Russia's hybrid warfare against the West*, Cybersecurity and Law, t. 7, nr 1, s. 51-60.

Karpiuk M. (2021), *Cybersecurity as an element in the planning activities of public administration*, Cybersecurity and Law, t. 5, nr 1, s. 45-52.

Komisja Europejska, *Jak rozpoznać teorie spiskowe*, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/identifying-conspiracy-theories_pl [dostęp: 07.09.2022].

Makuch A. (2021), *„Psychological judo" Seftona Delmera – brytyjskie techniki dezinformacji w okresie II wojny światowej*, Cybersecurity and Law, t. 5, nr 1, s. 159-170.

Mandal E.E. (1998), *Sekty i zagrożenia z nimi związane*, Chowanna, t. 1, s. 18-23.

Omegasoft (2020), *Czy otwarta sieć Wi-Fi widzi odwiedzane strony? Darmowy internet a bezpieczeństwo*, https://www.omegasoft.pl/blog/czy-otwarta-siec-wi-fi-widzi-odwiedzane-strony-darmowy-internet-a-bezpieczenstwo/ [dostęp: 06.09.2022].

Pietras M. (2021), *Wojna informacyjna jako współczesne narzędzie działań nieregularnych*, Cybersecurity and Law, t. 6, nr 2, s. 21-41.

Policja.pl (2022), *Uwaga na fake newsy na temat uchodźców!*, https://policja.pl/pol/aktualnosci/215062,Uwaga-na-fake-newsy-na-temat-uchodzcow.html [dostęp: 07.09.2022].

Policja.pl (2007), *Nierozsądne plotki,* https://policja.pl/pol/aktualnosci/12331,Nierozsadne-plotki.html [dostęp: 6.06.2022].

Portal Bankowości Spółdzielczej (2022), *Panika i fake newsy: jak nie ulec dezinformacji?*, https://bs.net.pl/panika-i-fake-newsy-jak-nie-ulec-dezinformacji/ [dostęp: 06.09.2022].

Renz B. (2016), *Blogi: Hybridisota lännen heikkous, ei Venäjän vahvuus*, Valtioneuvoston Selvitys – ja Tutkimustoiminta, https://tietokayttoon.fi/ajankohtaista/blogi/-/blogs/hybridisota-lannen-heikkous-ei-venajan-vahvuus [dostęp: 27.08.2022].

Rey T. (2021), *The rise of disinformation and 'fake news' in times of crisis*, https://atalayar.com/en/content/rise-disinformation-and-fake-news-times-crisis [dostęp:10.09.2022].

Rock Dove Solution (2021), *How your crisis plan can help combat Fake News*, https://www.rockdovesolutions.com/blog/how-your-crisis-plan-can-help-combat-fake-news [dostęp: 10.09.2022].

Sejm Rzeczypospolitej Polskiej (2021), *Interpelacja nr 26306 do Ministra Spraw Wewnętrznych i Administracji w sprawie zapewnienia bezpieczeństwa pracownikom ochrony zdrowia w związku z atakami antyszczepionkowców*, https://www.sejm.gov.pl/sejm9.nsf/InterpelacjaTresc.xsp?key=C68CBB [dostęp: 30.07.2022].

Serwis Rzeczypospolitej Polskiej, *Polska na celowniku dezinformacji*, https://www.gov.pl/web/sluzby-specjalne/polska-na-celowniku-dezinformacji [dostęp: 06.09.2022].

Termedia (2012), *Antyszczepionkowe sekty*, https://www.termedia.pl/mz/Antyszczepionkowe-sekty,7057.html [dostęp: 07.09.2022].

Vosoughi S., Roy D. i Aral S. (2018), *The spread of true and false news online*, Science, t. 359, nr 6380, s. 1146-1151.

Wirtualna Polska (2022), *Gigantyczne kolejki na stacjach paliw. Kierowcy tankują na zapas w obawie przed podwyżkami i reglamentacją*, Gigantychttps://finanse.wp.pl/gigantyczne-kolejki-na-stacjach-paliw-kierowcy-tankuja-na-zapas-w-obawie-przed-podwyzkami-i-reglamentacja-6740877026302464azne kolejki na stacjach paliw. Kierowcy tankują na zapas w obawie przed podwyżkami i reglamentacją - WP Finanse [dostęp: 6.06.2022].

Włodyka E.M. (2022), *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewnienia cyberbezpieczeństwa*, Cybersecurity and Law, t. 7, nr 1, s. 202-219.

Xu R. (2021), *You can't handle the truth: misinformation and humanitarian action*, https://blogs.icrc.org/law-and-policy/2021/01/15/misinformation-humanitarian/ [dostęp: 06.06.2022].

Zimniewicz R. (2014), *Środki używane przez terrorystów przy zamachach bombowych*, Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje, nr 15, s. 305-311.

DEZINFORMACJA JAKO CZYNNIK RYZYKA W SYTUACJACH KRYZYSOWYCH

Streszczenie

Fałszywe, szybko rozpowszechniające się informacje mogą modelować nastroje społeczne, wpływać na wyniki demokratycznych wyborów, powodować napięcia na arenie międzynarodowej, a nawet być przyczyną konfliktów zbrojnych. W przypadku zaistnienia sytuacji kryzysowej dezinformacja może być narzędziem wykorzystywanym w celu destabilizowania sytuacji wewnętrznej państwa. W takich okolicznościach poważne konsekwencje może mieć również dostęp osób niepowołanych do informacji niejawnych.

Współczesne urządzenia cyfrowe i zarządzające nimi systemy nie wymagają od przeciętnego użytkownika biegłej znajomości systemów informatycznych i umiejętności technicznych. Jednak rozwój nowoczesnych technologii determinuje potrzebę ciągłego uaktualniania wiedzy w tym zakresie. Dotyczy to w szczególności osób, które zajmują się, szeroko rozumianym, bezpieczeństwem państwa.

Słowa kluczowe: sytuacja kryzysowa; dezinformacja; bezpieczeństwo informacji; weryfikacja informacji; deep fake.