Cybersecurity and Law

2026 Nr 1(15)

DOI: 10.35467/cal/215344

Information security threats in the digital space generated by the Russian Federation

Informacyjne zagrożenia bezpieczeństwa w przestrzeni cyfrowej generowane przez Federację Rosyjską

Michał MOGILNICKI
Akademia Sztuki Wojennej
ORCID: 0009-0003-2545-6266
E-mail: michalmogilnicki00@gmail.com

Streszczenie

Celem artykułu było ukazanie jakie informacyjne zagrożenia bezpieczeństwa są obecnie generowane przez Federację Rosyjską w przestrzeni cyfrowej. Skupiono się na przedstawieniu, w jaki sposób wyewoluowały rosyjskie formy prowadzenia rażenia informacyjnego, ze szczególnym uwzględnieniem dezinformacji, zmierzające do destabilizacji bezpieczeństwa od czasów carskich do współczesnych. Ponadto opisane zostały cechy charakterystyczne współczesnych, rosyjskich działań informacyjnych, stanowiących zagrożenie dla bezpieczeństwa, które są prowadzone w przestrzeni cyfrowej. Zwłaszcza działania dezinformacyjne, gdyż one są najczęściej spotykanym zagrożeniem bezpieczeństwa we współczesnej przestrzeni cyfrowej. A także, przykłady praktyczne prowadzenia rażenia informacyjnego w przestrzeni cyfrowej przez i w interesie Federacji Rosyjskiej, których charakter daje przesłanki, że prowadzone są w celu destabilizacji bezpieczeństwa.

Słowa kluczowe
zagrożenia informacyjne, dezinformacja, przestrzeń cyfrowa, Federacja Rosyjska, bezpieczeństwo

Abstract

The aim of this article was to demonstrate the information security threats currently being generated by the Russian Federation in the digital space. The article focuses on presenting how Russian forms of information attacks have evolved, with particular emphasis on disinformation, aimed at destabilizing security, from tsarist times to the present day. Furthermore, the article describes the characteristics of contemporary Russian information activities posing a security threat, conducted in the digital space. Disinformation activities in particular, as they are the most common security threat in the contemporary digital space, are described. Practical examples of information attacks in the digital space by and in the interests of the Russian Federation, the nature of which

suggests they are conducted with the aim of destabilizing security, are also presented. Conclusions are provided.

Keywords

information threats, disinformation, digital space, Russian Federation, security

Wprowadzenie

Podjęcie rozważań naukowych w obszarze generowania i wykorzystywania informacyjnych zagrożeń bezpieczeństwa przez Federację Rosyjską poprzez działania w przestrzeni cyfrowej, wydaje się być ważne i potrzebne. Obecnie już niemal na każdej konferencji naukowej, sympozjum, seminarium naukowym lub na każdym kongresie poświęconym bezpieczeństwu, wygłaszane są referaty dotyczące szeroko pojętej dezinformacji oraz zagrożeń informacyjnych w przestrzeni cyfrowej i ich wpływowi na bezpieczeństwo danego podmiotu, z którego najczęstszym jest państwo. Bardzo często w kontekście Federacji Rosyjskiej, jako podmiotu obecnie stanowiącego największe zagrożenie dla bezpieczeństwa Polski i innych podmiotów stosunków międzynarodowych.

Cel badań to ukazanie: Jakie były stosowane przez Federację Rosyjską formy rażenia informacyjnego, celem generowania zagrożeń bezpieczeństwa, opierające się na szczególnie na działaniach dezinformacyjnych w przestrzeni cyfrowej w ostatnich latach. Problem badawczy stanowiła próba odpowiedzi na pytanie: W jaki sposób w ostatnich latach Federacja Rosyjska generowała zagrożenia informacyjne w przestrzeni cyfrowej, celem destabilizacji bezpieczeństwa? Hipotezę badawczą stanowiło stwierdzenie, że: Rosyjskie działania dezinformacyjne, będące głównym rodzajem informacyjnych zagrożeń bezpieczeństwa tej natury, stanowią współcześnie główne narzędzie destabilizacji bezpieczeństwa, jakie są ku temu wykorzystywane w przestrzeni cyfrowej.

Metody badawcze jakie zostały zastosowane do opracowania tej publikacji, należy rozdzielić na metody empiryczne oraz metody teoretyczne. Metoda empiryczna, jaką posłużono się w badaniach, to badanie treści literatury przedmiotu. Ukierunkowane ono było głównie na wyjaśnienie aspektów teoretycznych przedmiotu badań, a także zobrazowania przykładów konkretnych form, metod oraz technik generowania zagrożeń informacyjnych w przestrzeni cyfrowej przez Federację Rosyjską, celem destabilizacji bezpieczeństwa. Natomiast metody teoretyczne jakimi się posłużono, to: analiza, dedukcja oraz wnioskowanie. Analiza dotyczyła głównie wyjaśnienia przyczyn skuteczności oraz nieskuteczności stosowanych w przestrzeni cyfrowej przez Federację Rosyjską form, metod, technik oraz narzędzi rażenia informacyjnego. Dedukcja była szczególnie przydatna do określania, jakie cele miały badane kierunki stosowanej przez Federację Rosyjską dezinformacji w przestrzeni cyfrowej, w procesie prób destabilizacji bezpieczeństwa, która to stanowi główne zagrożenie informacyjne w cyberprzestrzeni. Wnioskowanie posłużyło przede wszystkim, do opracowania propozycji zmian oraz ukuciu wskazówek dla budowy odporności społecznej na dezinformacje oraz inne zagrożenia informacyjne ze strony Federacji Rosyjskiej.

Rozpoczęte na masową i niespotykaną dotychczas skalę w 2014 r., działania dezinformacyjne Federacji Rosyjskiej w przestrzeni cyfrowej Ukrainy, należy traktować jako wykorzystanie dezinformacji w działaniach preparacyjnych do wojny kinetycznej. Wojna ta została poprzedzona wojną informacyjną,

prowadzoną głównie w przestrzeni cyfrowej, jaką jest przede wszystkim Internet. Dezinformacja, która jest głównym zagrożeniem informacyjnym dla bezpieczeństwa, była używana do osiągania celów szczebla strategicznego oraz czerpanie innych korzyści, jak np. eksploatacja kopalń czy prestiż międzynarodowy. Działania dezinformacyjne realizowane już po rozpoczęciu inwazji 24.02.2022 r., stanowiły punkt wyjścia dla kolejnych kierunków rosyjskiego rażenia informacyjnego, które stosowano w pierwszych miesiącach konwencjonalnej wojny[1]. Wojna konwencjonalna na Ukrainie wywołana przez Federację Rosyjską w lutym 2022 r. to w rzeczywistości dwie równoległe wojny- kinetyczna prowadzona na lądzie, morzu i w powietrzu oraz informacyjna prowadzona głównie w przestrzeni cyfrowej.

Współcześnie ,,fake news" zdaje się być obecnie najczęściej stosowaną techniką, jaką Federacja Rosyjska się posługuje, generując zagrożenia informacyjne i prowadząc działania dezinformacyjne w przestrzeni cyfrowej aby destabilizować bezpieczeństwo rozlicznych podmiotów. Termin „fake news" jest używany od ponad wieku. Pierwszy raz to określenie pojawiło się w artykule, zamieszczonym na łamach tygodnika pt. Harper's w 1925 r. Tytuł artykułu brzmiał zatytułowanym ,,Fake News and the Public", co w wolnym tłumaczeniu można rozumieć jako: Fake News i społeczeństwo. W treści artykułu zawarto ubolewania nad rolą, jaką agencje informacyjne odgrywają w szybkim i bezkrytycznym rozpowszechnianiu dezinformacji w śród społeczeństwa[2]. Współczesne fake newsy można rozumieć jako publikacje zamieszczone najczęściej i przede wszystkim w przestrzeni cyfrowej lub na portalu internetowym celowo i ze świadomością zawierania przez nią fałszywych danych lub fałszywego opisu prawdziwych zdarzeń czy faktów. Bardzo często przedstawia się dane faktyczne wydarzenia, jakoby miały zupełnie innych charakter niż w rzeczywistości. Pod pojęciem fake newsa można zawrzeć tezę, że fake news jest jedynym z typów współczesnej dezinformacji. Polega na zmanipulowaniu fałszywej lub częściowo prawdziwej informacji, przekazywanej w taki sposób aby skutecznie przekonywać odbiorców o prawdziwości przekazywanych treści. Fake newsy od dezinformacji i np. propagandy zdaje się odróżniać to, że same w sobie nigdy nie są procesem rażenia informacyjnego, czyli innymi słowy oddziaływania dezinformacyjnego, a zawsze są jedynie tego elementem. Stosuje się je, aby przekonać odbiorców, jakoby dezinformacja w nich zawarta, została uznana za wiarygodne informacje[3].

Cechy charakterystyczne dezinformacji rosyjskiej jako głównego zagrożenia informacyjnego w cyberprzestrzeni

Jednym z najstarszych, udokumentowanych przykładów przeprowadzenia na terytorium Rosji działań dezinformacyjnych, mających na celu destabilizację bezpieczeństwa w państwie, zdają się być wydarzenia z 1564 roku. Car Rosji Iwan IV Groźny chciał być monarchą absolutnym i uniezależnić się od Dumy bojarskiej oraz duchowieństwa w obszarze rządzenia krajem. Wprowadził więc

[1] M. Marek, Wojna informacyjna Federacji Rosyjskiej przeciw Ukrainie Polsce i NATO, Warszawa 2025, s. 19.
[2] D. M. J. Lazer, M. A. Baum, Y. Benkler, A. J. Berinsky, K. M. Greenhill, F. Menczer, M. J. Metzger, B. Nyhan, G. Pennycook, D. Rothschild, M. Schudson, S. A. Sloman, C. R. Sunstein, E. A. Thorson, D. J. Watts, J. L. Zittrain, The science of fake news, ,,Science" 2018, vol. 359, nr. 1094, s. 3.
[3] F. Nakamura, 100 maksym o dezinformacji, Warszawa 2020, s.73.

szereg niesprzyjającym interesom bojarów praw, głównie dotyczących ich majątków. Car ogłosił swoją abdykację, na co bojarzy zareagowali entuzjazmem. W czasie gdy zjeżdżali się do Moskwy, aby jako Duma bojarska przyjąć abdykację i wybrać nowego cara spośród siebie, działania dezinformacyjne już trwały. Iwan IV oraz jego ludzie dostarczyli wiele listów mieszkańcom Moskwy, które informowały ich (czyli realnie dezinformowały) o ciężkim losie, jaki bojarski car i pozostali bojarzy zamierzają sprowadzić na nich i innych mieszkańców Rosji. Bojarów przedstawiono również jako zdrajców Rosji. W listach zawarte zostały również opisy działań jakie Iwan IV podejmował i zamierza podejmować na rzecz dobra poddanych oraz przeciw barbarzyństwu bojarów. Oczywiście takowe nigdy nie miały miejsca, ani nigdy nie zamierzano ich podejmować. Kiedy Duma się zebrała, mieszkańcy Moskwy zażądali od bojarów odrzucenia abdykacji Iwana IV oraz uniezależnienia od woli i zdania Dumy, we wszelkich kwestiach dotyczących rządzenia Rosją i Rosjanami. Odrzucenie ultimatum Moskwiczan oznaczało śmierć bojarów z ich rąk. Działania dezinformacyjne zakończyły się sukcesem. Iwanowi IV Groźnemu Duma przyznała de facto władzę absolutną i tym samym zrzekła się wszelkich udziałów w rządzeniu krajem i wpływów na decyzję Iwana IV i wszystkich kolejnych carów.

W 1787 r. miało miejsce kolejne, duże, wewnątrzrosyjskie przedsięwzięcie dezinformacyjne. Mianowicie po zdobyciu przez Rosję w wojnie z Imperium Osmańskim i Chanatem Krymskim półwyspu krymskiego, Katarzyna II udała się tam w podróż, celem obejrzenia nowego terytorium. Na trasie przejazdu z Piotrogrodu na Krym, rozegrała się wielka operacja dezinformacyjna, której celem była przestrzeń poznawcza samej Carycy. Katarzynę II z pewnością interesowało, w jakiej kondycji i jak liczny jest jej naród. Grigorij Potiomkin doskonale zdawał sobie sprawę, że podróż przez kraj nie tylko rozczaruje Carycę ale również może ona odkryć, że raporty i sprawozdania jakie otrzymuje od Potiomkina na temat liczby ludności, gęstości zaludnienia i stopy życiowej swoich poddanych to czysta dezinformacja. Potiomkin miał kompetencje w aspekcie zarządzania Rosją pod kątem demografii lub lokalnych gospodarek, gdyż pełnił funkcję niejako współczesnego Ministra Infrastruktury. Przygotował on zatem makiety całych wiosek z papier mache, z którymi jego ludzie najpierw, bocznymi drogami, przez lasy i polami wyprzedzali kolumnę powozów z Monarchinią, a następnie rozstawiali makiety przed jej przybyciem. Po wyjeździe z ,,papierowej", oczywiście wzorcowej i dostatniej wsi, cykl się powtarzał, aż do dotarcia na Krym, który był najnowszą zdobyczą Rosji w wyniku wojny z Imperium Osmańskim i Chanatem Krymskim. Choć efektem tej operacji dezinformacyjnej nie były nadzwyczajne wydarzenia lub zmiany korzystne dla Potiomkina, zdaje się ona stanowić dobry przykład ewolucji rosyjskiego modelu operacji dezinformacyjnej na płaszczyźnie politycznej. Z racji tego, że wykreowano w umyśle Monarchini zupełnie obiegający od rzeczywistości obraz kraju, którym włada a przynajmniej próbowano. Docelowo miało to wywołać u Katarzyny II konkretne zachowania lub brak podejmowania konkretnych zachowań. Skoro Rosja jest rozwinięta, niezasadne wydaje się podejmowanie zmian, wprowadzania reform i innych aktywności. Wydaje się, że dla Potiomkina korzystne było zaniechanie podejmowania zmian i działań ku temu zmierzających, celem poprawy w obszarach demograficznym, społecznym i gospodarczym przez Carycę. Zapewne wiązałoby się to z pozbawieniem go prestiżowej funkcji i znacznych dochodów, jakie z tytułu jej pełnienia pobierał. Widok tego, co odbiorca chce zobaczyć i wpłynięcie na jego postępowanie

korzystnie dla nadawcy dezinformacji, można nazwać udaną operacją dezinformacyjną.

Przez kolejne lata teoria i praktyka dezinformacji rosyjskiej ewoluowała, aby szczyt dynamiki swojego rozwoju i możliwości destabilizacji bezpieczeństwa osiągnąć w XX w. Dzisiejsze formy wykorzystania dezinformacji przez Federację Rosyjską czerpią głównie z doświadczeń czasów radzieckich, a nie czasów Imperium Rosyjskiego. Zatem zasadnym wydaje się stwierdzić, że współczesne formy wykorzystywania dezinformacji w przestrzeni cyfrowej do destabilizacji bezpieczeństwa przez Federację Rosyjską, stanowią wypadkową doświadczeń, uniwersalnych zasad i prawidłowości, jakie zostały odkryte przez organa ZSRR i Federacji Rosyjskiej pierwszych lat jej istnienia.

Jedną z najbardziej charakterystycznych cech współczesnej, rosyjskiej działalności dezinformacyjnej, jest wykorzystywanie dezinformacji oraz prowadzenie działań dezinformacyjnych, w ramach operacji decepcyjnych. Dezinformacja z reguły polega na wprowadzeniu w błąd, czyli jej celem jest np. mylenie, zwodzenie, odwracanie uwagi, pozorowanie, manipulacja i tym podobne. Decepcja jest definiowana jako mechanizm wprowadzania w błąd instytucji państwowych przez działania wyspecjalizowanych w tym organizacji oraz służb lub różnorodnych agentów wpływu[4] Zdaje się mieć to szczególne znaczenie i stanowić bardzo poważne zagrożenie, ponieważ w ten sposób zdecydowanie skuteczniej można destabilizować bezpieczeństwo podmiotu, jakim jest np. państwo lub grupa państw. Decepcję oraz dezinformację, zarówno w ujęciu teoretycznym, jak i współczesnego modelu rosyjskiego, odróżniają nie tylko docelowe grupy odbiorców, wobec których prowadzone są działania oraz operacje, ale także do maksimum utrudniona możliwość wykrycia dezinformacji w działaniach decepcyjnych, które współcześnie coraz częściej prowadzone są w przestrzeni cyfrowej. A także weryfikacja prawdziwości treści, informacji oraz komunikatów dostarczanych na potrzeby decepcji.

Jako główne obszary, na których współcześnie wykorzystywana jest decepcja przez Federację Rosyjską to: (1) przestrzeń informacyjna w wymiarze cyfrowym- celem decepcji w tym obszarze są wszelkie systemy informacyjne np. danego państwa, sojuszu, międzynarodowej organizacji politycznej lub gospodarczej; (2) noosfera - rozumiana jako obszar ludzkiego umysłu, w którym funkcjonują idee, wyobraźnia, wartości jednostki oraz grupy społecznej lub narodu; (3) wpływ informacyjny, czyli wywoływanie pożądanych z punktu widzenia prowadzących decepcję zachowań jednostek oraz grup, na które decepcją się oddziałuje. Precyzując chodzi o to, aby za pomocą decepcji kreować i sterować tym, co docelowi odbiorcy myślą, czują oraz to przed czym odczuwają strach i czego oraz kogo się obawiają. Sednem tego jest wykreowanie takiego postrzegania rzeczywistości, w której docelowi odbiorcy dostosowują swoje zachowania do woli prowadzących decepcję.

Obecne rosyjskie podejście wyszczególnia konkretnie pięć teatrów działań dezinformacyjnych, coraz częściej prowadząc takie działania w przestrzeni cyfrowej. Zasadnym wydaje się stwierdzić, że poprzez oddziaływanie na te obszary, można doprowadzić lub wzmacniać proces destabilizacji bezpieczeństwa. Są to obszary[5]: terytorialny, technologiczny, społeczny, ewolucyjny, obszar związany z pojęciem noosphere.

[4] M. Świerczek, Jak Sowieci przetrwali dzięki oszustwu, Warszawa 2021, s. 12.

[5] T. Kacała, Rola informacji w komunikacji strategicznej, [w:] W. Scheffs (red.) Konteksty teoretyczne i praktyczne informacji w organizacji, Kalisz 2020, s. 42.

Literatura przedmiotu stanowi, że celami działań dezinformacyjnych Federacji Rosyjskiej, mającymi destabilizować bezpieczeństwo, prowadzonymi na portalach społecznościowych, które z zasady stanowią przestrzeń cyfrową, są np.[6]: dyskredytacja ustroju politycznego, modelu gospodarczego oraz wartości społecznych przeciwnika lub oponenta, popieranie wymierzania sprawiedliwości przez społeczeństwo a nie legalny wymiar sprawiedliwości przeciwnika lub oponenta, podżeganie do otwartej i brutalnej konfrontacji grup składających się na społeczeństwo przeciwnika lub oponenta na płaszczyznach: politycznej, środowiskowej, religijnej, kulturowej, etnicznej etc., prowokowanie niezadowolenia z sytuacji politycznej, społecznej, materialno-bytowej, gospodarczej i z innych w kraju przeciwnika lub oponenta, podważanie poczucia bezpieczeństwa w społeczeństwie i kluczowych grupach społecznych, których zyski i rozwój determinuje poczucie bezpieczeństwa kraju przeciwnika lub oponenta.

Współcześnie jednym z głównych wyzwań dla Federacji Rosyjskiej, jest ukrycie źródła pochodzenia działań dezinformacyjnych, jakie są prowadzone celem destabilizacji bezpieczeństwa. W tym również w przestrzeni cyfrowej. Do najczęściej używanych w tym celu metod jest stosowanie[7]: zaprzeczania, aczemunizmu, satyry, kłamstw, oskarżania, niuansów, kontrataków.

Warto podkreślić, że Federacja Rosyjska przed dokonaniem zajęcia półwyspu krymskiego, od wielu lat budowała ogromną machinę rażenia informacyjnego, mającego destabilizować bezpieczeństwo określonych podmiotów. Machinę, która oddziaływała zewnętrznie, jak i wewnętrznie. Rosyjscy dziennikarze, naukowcy, politycy czy np. dostojnicy Cerkwi, w kontekście wojny na Ukrainie wypowiadają się w różny sposób, to w rzeczywistości wszyscy mówią to samo[8]. Godnym podkreślenia jest też to, że współczesny użytkownik rosyjskiej przestrzeni cyfrowej, napotyka na te same narracje we wszystkich, cyfrowych, dostępnych całodobowo kanałach informacyjnych i portalach społecznościowych[9]. To znaczy, że np. dezinformacja telewizyjna, jest spójna z internetową, radiową, plakatową (w dużych miastach-wyświetlaną elektroniczne) itd. Chodzi o to, aby różne kanały informacyjne wzajemnie popierały dane działania dezinformacyjne, którą użytkownik przestrzeni cyfrowej, medialnej i innych uzna za informację prawdziwą. Uzbrojeniem wykorzystywanym przez największą liczbę obywateli strony zaangażowanej w wojnę, w obszarze informacyjnym konfliktu jest wszelka dezinformacja[10].

W tym miejscu, należy udzielić odpowiedzi na następujące pytanie: Dlaczego rosyjska machina działań dezinformacyjnych i rażenia informacyjnego, szczególnie w przestrzeni cyfrowej jest skuteczna w Federacji Rosyjskiej, a niemal bezskuteczna wszędzie indziej na zachód od Federacji Rosyjskiej? Odpowiedź zdaje się być dość złożona, lecz przystępna do przyswojenia. Krótkie doniesienia wsparte cytatami z różnych źródeł, idące w parze możliwością natychmiastowej weryfikacji danej informacji lub prawdziwości komunikatu w innych mediach. To model, jeszcze nie w pełni powszechnie stosowany, lecz

[6] J. Zalewski, D. G. Dzierżyński, Wojna informacyjna w odbudowie rosyjskiej mocarstwowości, Warszawa 2019, s. 124.
[7] R. Kupiecki., F. Bryjka, T. Chłoń, Dezinformacja międzynarodowa, Warszawa 2022, s. 180.
[8] Ł. Zalesiński, Słowa jak pociski, ,,Polska zbrojna" 2023, nr 4/2023, s. 18.
[9] S. Sanovich, Russia: The origins of digital misinformation, [w:] S. C. Woolley, P. N. Howard (red.) Computational Propaganda, Oxford 2019, s. 28.
[10] M. Wrzosek, Military reconnaissance in the wars of the future forecasted development directions, Kwartalnik Bellona 2020, nr 2, s. 110.

stricte zachodni społecznego zapobiegania dezinformacji. Media, które przeniosły się niemal w całości do przestrzeni cyfrowej, stanowią istotny aspekt dla funkcjonowania jednostek i podmiotów w demokratycznym państwie, jak i społeczeństwie[11], co przekłada się na stan bezpieczeństwa danego podmiotu.

Zatem najważniejszym wnioskiem w aspekcie cech współczesnych działań dezinformacyjnych i generowania zagrożeń informacyjnych przez Federację Rosyjską, a także dezinformacji rosyjskiej, która obecnie jest prowadzona głównie w przestrzeni cyfrowej, a jej celem jest destabilizacja bezpieczeństwa, wydaje się być następujące stwierdzenie. Federacja Rosyjska zadaje się nabyć umiejętności o wysokim stopniu doskonałości w wykorzystywaniu informacji, dezinformacji, prowadzeniu działań dezinformacyjnych oraz generowaniu zagrożeń informacyjnych na długo przed tym, jak ukute zostały pojęcia wielokrotnie tutaj używane, tj. infosfera oraz środowisko informacyjne[12], a także pojawiła się powszechnie dostępna przestrzeń cyfrowa, do której dostęp mają miliardy użytkowników. Przez co wykorzystywanie dezinformacji w celu destabilizacji bezpieczeństwa stało się jeszcze poważniejszym zagrożeniem.

Dezinformacja ze strony Federacji Rosyjskiej jako cyfrowe zagrożenie dla bezpieczeństwa

Wojna konwencjonalna wywiera potężny wpływ na percepcję człowieka. Szczególnie w aspekcie poszukiwania, odbioru i rozpowszechniania informacji, wiadomości, danych czy komunikatów związanych z przetrwaniem, zapewnieniem bezpieczeństwa czy wizji upadku kraju, w którym dana jednostka lub grupa społeczna żyje. W takich warunkach odbiorcy informacji śledzą a przynajmniej poświęcają uwagę każdemu z dostępnych źródeł informacji[13]. Faktem jest, że współcześnie najbardziej dostępne i o największym zasięgu są te kanały informacyjne, funkcjonujące w przestrzeni cyfrowej i Internecie. Liczba nadawców i tym samym kreatorów przestrzeni informacyjnej po rozpoczęciu działań wojennych, również znacznie się zwiększa. Zwłaszcza jeśli kraj ponosi klęskę za klęską. Federacja Rosyjska poważnie traktuje wojnę informacyjną oraz zdaje się być świadoma, jak duży potencjał w niej się znajduje. Dowód na to zdaje się stanowić to, jak wcześnie Federacja Rosyjska rozpoczęła prowadzenie wojny informacyjnej, której głównym orężem jest dezinformacja, nim konwencjonalnie zaatakowała Ukrainę w lutym 2022 r..

Federacja Rosyjska od lat przygotowywała zaplecze techniczne i technologiczne do prowadzenia wojny w przestrzeni cyfrowej na skalę jaka obecnie jest obserwowana. W marcu 2023 r., dziennikarka pracująca dla niezależnego rosyjskiego portalu informacyjnego Fontanka.ru (ros. *Фонтанка.ру*) opisała swoje doświadczenia z przepracowania jednego dnia w tzw. ,,Batalionie Cyberżołnierzy". Zarobki służących tam żołnierzy i pracowników są dość wysokie. Jednakże najciekawsza wydaje się taktyka, która stosowana jest do ,,odpierania" cyberataków, mających na celu ujawnienie dezinformacyjnej działalności tego podmiotu. Działania obronne ograniczają się jedynie lub aż do pisania i zamieszczania prorosyjskich komentarzy na wszelkich

[11] M. Kołodziejczak, Wstęp [w:] M. Kołodziejczak, G. Pastuszko (red.) Organy zapewniające pluralizm rynku medialnego oraz ochronę praw użytkowników mediów elektronicznych, Warszawa 2022, s. 7.
[12] N. Schick, Deep fakes and the infocalypse, Londyn 2020, s. 53.
[13] D. Kułeba, Wojna o rzeczywistość, Warszawa 2023, s. 52.

platformach w kraju przeciwnym Federacji Rosyjskiej, jak i w krajach wspierających ten pierwszy. Dziennie pracownik lub żołnierz musi dokonać minimum 200 dezinformacyjnych lub uwiarygadniających daną dezinformację wpisów. Na jednej zmianie pracuje około 100 osób, co daje 20 000 np. komentarzy w czasie jednej zmiany. Jak podała Fontanka.ru, zmiany są dwie (trzeciej prawdopodobnie nie ma). Czyli wydajność tej jednej rosyjskiej farmy trolli to około 40 000 wpisów na dobę. Prosty rachunek wykazuje, że w tydzień liczba prorosyjskich komentarzy wyniesie co najmniej 280 000, a po miesiącu- ponad milion[14]. Natomiast jeśli chodzi o podmiot państwowy strzegący cyberprzestrzeni Federacji Rosyjskiej, to jest nim Departament ,,K" Ministerstwa Spraw Wewnętrznych Federacji Rosyjskiej (ros. *Управление «К» Министерства внутренних дел Российской Федерации*). Zatem głównym uzbrojeniem wykorzystywanym przez Kreml w wojnie z Ukrainą, zdaje się być dezinformacja[15], której celem jest destabilizacja bezpieczeństwa szczególnie w bliskim otoczeniu Federacji Rosyjskiej, wykorzystywana głównie w przestrzeni cyfrowej. To stwierdzenie wydaje się być zasadne, zważywszy na dane ilościowe zaprezentowane wcześniej, dotyczące dziennego publikowania komentarzy i wpisów internetowych przez rosyjską instytucję.

Podobna instytucja ma również się mieścić przy ulicy Sawuszkina 55 w Sankt Petersburgu. W budynku pod tym adresem prawdopodobnie przez całą dobę pracuje między 300 a 400 osób w charakterze trolli. W trakcie dwunastogodzinnej zmiany, każdy pracownik musi zamieścić na łamach najpopularniejszych portali społecznościowych, czyli wyłącznie w przestrzeni cyfrowej między sto a sto pięćdziesiąt komentarzy stanowiących dezinformację lub wspomagających daną dezinformację. Przyjmując, że pracuje na obu zmianach w sumie 350 osób i każdy z nich publikuje średnio 125 wpisów, daje to 43 750 wpisów na dobę[16]. Według innego źródła, w tej komórce na jednej zmianie pracuje od sześciuset do tysiąca osób. Każdy z pracowników dziennie publikuje od pięćdziesięciu do stu dezinformacyjnych treści cyfrowych. Oprócz pracowników stacjonarnych, wielu pracuje zdalnie[17].

Opisanie cyklu pracy rosyjskich, cyfrowych trolli, jak również innych osób zajmujących się prowadzeniem działań dezinformacyjnych w przestrzeni cyfrowej, za pomocą zamieszczania w cyfrowej przestrzeni informacyjnej materiałów dezinformacyjnych wydaje się prosty. Najpierw tworzone są materiały oddziaływania informacyjnego to znaczy np. fałszywe obrazy, grafiki komputerowe zawierające fałszywe informacje połączone z fałszywymi lub wypaczonymi obrazami, materiały multimedialne zawierające treści dezinformujące lub fałszywe historie lub opisy zdarzeń realnych, jak i tych wymyślonych. Następnie zamieszczane jest to na portalu internetowym lub generalnie cyfrowym forum dyskusyjnym o niskim zasięgu dotarcia do odbiorców, często lokalnym lub regionalnym. Potem inne trolle, prawdziwe osoby lub cyfrowe algorytmy sztucznej inteligencji udostępniają ten produkt na szpaltach cyfrowych portali informacyjnych i wszelkich innych platformach, które mają większy zasięg niż pierwotna domena cyfrowa, na których pierwszy raz zamieszczono materiał dezinformacyjny. Po osiągnięciu obecności danej dezinformacji na cyfrowych

[14] A. Mierzyńska, Efekt niszczący. Jak dezinformacja wpływa na nasze życie, Warszawa 2022, s. 283.
[15] M. Mogilnicki, Komunikacja strategiczna wobec zagrożeń informacyjnych. Teoria i praktyka, Warszawa 2024, s. 27.
[16] A. Paczuszka, Rosyjskie służby specjalne czyli jak rozbroić państwo, Łódź 2018, s. 97.
[17] S. van der Linden, Fake News, Poznań 2023, s. 271.

portalach informacyjnych czy innych cyfrowych kanałach mających największą popularność, a tym samym często największy zasięg dotarcia do zwłaszcza docelowej grupy odbiorców, podtrzymuje się sztucznie popularność danej dezinformacji wśród opinii publicznej, szczególnie tej docelowej aż dezinformacja same z siebie nie zaczną rozpowszechniać media tradycyjne. Oczywiście to wszystko dokonywane jest celem destabilizacji bezpieczeństwa podmiotu, w którego przestrzeni informacyjnej takie działania są prowadzone. A to w jaki sposób potencjalnie doprowadzą do destabilizacji bezpieczeństwa, nigdy nie jest do końca znane ani w pełni przewidywalne nawet przez prowadzących takie działania.

Dostępność do przestrzeni cyfrowej innego państwa, zwłaszcza w obszarze i poprzez internet, daje możliwość upubliczniania w niej dowolnego rodzaju treści skierowanych do innych narodów, co stanowi narzędzie *par excellence* dla współczesnej dezinformacji[18], którą Federacja Rosyjska wykorzystuje szczególnie w przestrzeni cyfrowej, celem destabilizacji bezpieczeństwa wybranych podmiotów. Dlatego należy mieć na uwadze, że wzrost popularności źródeł i platform cyfrowych to zjawisko potencjalnie obusieczne. Gdyż z jednej strony zapobiega to złożonemu spreparowaniu materiałów dezinformacyjnych, jak np. fałszywe wydanie dziennika telewizyjnego z udziałem sobowtóra Prezydenta Ukrainy. A więc zapobiega powstawaniu i oddziaływaniu zagrożenia bezpieczeństwa, umieszczonego w przestrzeni cyfrowej. Ponadto zasadnym wydaje się nadmienić, że w rosyjskim żargonie dezinformacyjnym funkcjonuje specjalne określenie na spreparowane materiały audiowizualne, ukazujące daną osobę lub grupę osób. Określa się je mianem *компрометирующие материалы*, co w wolnym tłumaczeniu oznacza materiały kompromitujące, z zaznaczeniem osobowego obiektu oddziaływania[19]. Natomiast, z drugiej strony odwzorowanie graficzne stron internetowych oficjalnych lub wiarygodnych ukraińskich portali i serwisów nie stanowi dla Kremla żadnego problemu. Mało odbiorców weryfikuje adres http wyświetlających się u góry ekranu po załadowaniu strony internetowej. Te często wyglądają identycznie, a jedyne co może ujawnić dezinformację to właśnie adres http, który zazwyczaj jest ignorowany.

Podsumowanie

Dzisiejsze i przyszłe realia zdają się bardzo wyraźnie wskazywać, że w procesie zapewniania, utrzymywania i przywracania bezpieczeństwa powinny być realizowane wszelkie działania, których celem jest powstrzymanie jednego z najpoważniejszych zagrożeń dla aktualnego środowiska bezpieczeństwa państwa w obecnym, jak i przyszłym świecie. Mianowicie, tym zagrożeniem jest wszechobecna w przestrzeni cyfrowej dezinformacja rosyjska. Inne zagrożenia informacyjne generowane przez Federację Rosyjską, również nie mogą być ignorowane, lecz dezinformacja jest spotykana najczęściej. Należy wskazać, że Internet oraz social media stanowią otwarte, cyfrowe wrota dla zamieszczania za ich pośrednictwem wszelkich materiałów dezinformacyjnych, które po rozpowszechnieniu rujnują środowisko bezpieczeństwa państwa, a także destabilizują bezpieczeństwo w wielorakich jego obszarach. Social media, czyli media społecznościowe to bezpośrednia i szybka platforma komunikacyjna, na

[18] M. Mogilnicki, Rosyjskie przygotowania dezinformacyjne do wojny z Ukrainą, Cybersecurity & Cybercrime 2024, T. I, nr 4, s. 273.
[19] E. Pietrobon, The Art of Secret War, USA 2020, s.11.

której materiały dezinformacyjne informacje mogą być natychmiastowo rozpowszechniane oraz docierać do nieograniczonej liczby odbiorców[20].

Odnosząc się do problemu badawczego, należy stwierdzić, że wykorzystanie trolli zdaje się być główną formą, jaka była wykorzystywana przez Federację Rosyjską do generowania zagrożeń informacyjnych w przestrzeni cyfrowej, celem destabilizacji bezpieczeństwa za wykorzystaniem działań dezinformacyjnych realizowanych w przestrzeni cyfrowej. Oprócz tej formy, występowały również fake newsy. Cel badań również zdaje się zostać osiągnięty.

Weryfikacja hipotezy badawczej, zdaje się przebiec pozytywnie. Ukazanie w artykule licznych form, metod a także ich złożonego charakteru i wzajemnego oddziaływania, jakie są stosowane przez Federację Rosyjską, celem destabilizacji bezpieczeństwa poprzez generowanie zagrożeń informacyjnych oraz działania dezinformacyjne w przestrzeni cyfrowej, zdaje się to potwierdzać. Współcześnie cyberprzestrzeń zdaje się być nadrzędnym obszarem, dla realizowania opisanych działań przez Kreml. Zasadnym wydaje się zatem stwierdzić, że rosyjskie działania dezinformacyjne, realizowane w przestrzeni cyfrowej, stanowią współcześnie główny obszar, w którym odbywa się działalność Kremla, mająca na celu destabilizację bezpieczeństwa wybranych podmiotów poprzez wystawianie ich na oddziaływanie generowanych przez siebie zagrożeń informacyjnych. Zarówno w aspekcie poznawczym, jak i praktycznym.

Wnioski jakie wynikają z przeprowadzonych rozważań na temat rosyjskich form generowania zagrożeń informacyjnych i wykorzystywania działań dezinformacyjnych w przestrzeni cyfrowej, celem destabilizacji bezpieczeństwa, zdają się jawić następująco.

Po pierwsze, historia dezinformacji rosyjskiej jako formy i jednocześnie narzędzia wykorzystywanego do destabilizacji bezpieczeństwa danego podmiotu liczy sobie co najmniej kilka wieków. O ile do wieku XX w. realizowana była niemal wyłącznie za wykorzystaniem materiałów fizycznych, jak listy Iwana IV, poprzez makiety ,,wiosek potiomkinowskich" oraz fałszywe treści drukowane w takich tytułach jak np. ,,Prawda", ,,Izwiestja" czy ,,Krasnaja Zwiezda" przed 1992 r., to współcześnie ma ona charakter głównie cyfrowy. Współcześnie to właśnie przestrzeń cyfrowa jest głównym polem dla stosowania na nim działań dezinformacyjnych, celem destabilizacji bezpieczeństwa przez Federację Rosyjską.

Po drugie, aby skutecznie przeciwdziałać rozprzestrzenianiu się zagrożeń informacyjnych i dezinformacji rosyjskiej, będącej dla Kremla formą destabilizacji bezpieczeństwa, coraz częściej wykorzystywaną w przestrzeni cyfrowej, należy zawsze przeprowadzać szczegółową analizę strony internetowej, tytułu czasopisma wydawanego cyfrowo lub np. prawdziwości odwołań, na które powołuje się dany podmiot rozpowszechniający konkretną informację. Oprócz tego dotrzeć do informacji na temat składu redakcji, autora informacji, właściciela tytułu lub domeny a także źródeł finansowania domeny lub tytułu, na którym pojawiła się dana informacja. Jeśli informacja jest nadawana, upubliczniania czy komunikowana ustnie, należy podjąć te same kroki, tylko że nie wobec podmiotu a wobec osoby będącej nadawcą informacji. Należy też zwrócić uwagę na jego ogólny stan psychofizyczny oraz sprawdzić, czy w momencie nadawania informacji, osoba nie znajdowała się pod wpływem środków zaburzających świadomość.

[20] D. Domalewska, Wykorzystanie mediów społecznościowych do zarządzania bezpieczeństwem na szczeblu lokalnym i regionalnym [w:] D. Domalewska, R. Bielawski (red.) Uwarunkowania współczesnego środowiska bezpieczeństwa, Warszawa 2020, s. 247.

Po trzecie, należy wdrażać narzędzia cyfrowe o wysokim stopniu doskonałości, służące do automatycznego wykrywania i oznaczania treści wizualnych oraz multimedialnych fałszywych informacji. A także, tworzyć i promować aplikacje mobilne oraz narzędzia cyfrowe, które pomagają użytkownikom przestrzeni cyfrowej w szybkim sprawdzaniu źródeł informacji i ich autentyczności. Podążając za prof. M. Wrzoskiem, zasadnym wydaje się w tym miejscu również stwierdzić, że Polska powinna budować system odporności na rosyjską dezinformację, dążyć do rozwijania własnych systemów informacyjnych zdolnych do przeciwstawienia się rosyjskiej dezinformacji[21].

Po czwarte, bardzo potrzebnym zdaje się być uświadamianie, jakie treści, informacje czy przekazy i produkty cyfrowe najprawdopodobniej trafią lub będą poszukiwane przez specyficzną grupę adresatów, a także jakie potencjalne skutki może wywołać dany przekaz lub produkt, w aspekcie jego potencjalnego wpływu na stan bezpieczeństwa danego podmiotu.

Bibliografia

Domalewska D., Wykorzystanie mediów społecznościowych do zarządzania bezpieczeństwem na szczeblu lokalnym i regionalnym. [w:] Domalewska D., Bielawski R. (red.), Uwarunkowania współczesnego środowiska bezpieczeństwa, Warszawa 2020.

Kacała T., Rola informacji w komunikacji strategicznej, [w:] Scheffs W. (red.), Konteksty teoretyczne i praktyczne informacji w organizacji, Kalisz 2022.

Kołodziejczak M., Wstęp. [w:] Kołodziejczak M., Pastuszko G. (red.), Organy zapewniające pluralizm rynku medialnego oraz ochronę praw użytkowników mediów elektronicznych, T.2, Warszawa 2022.

Kułeba D., Wojna o rzeczywistość, Warszawa 2023.

Kupiecki R., Bryjka F., Chłoń T., Dezinformacja międzynarodowa, Warszawa 2022.

Marek M., Wojna informacyjna Federacji Rosyjskiej przeciw Ukrainie Polsce i NATO, Warszawa 2025.

Mierzyńska A., Efekt niszczący. Jak dezinformacja wpływa na nasze życie, Warszawa 2022.

Mogilnicki M., Komunikacja strategiczna wobec zagrożeń informacyjnych. Teoria ipraktyka, Warszawa 2024.

Mogilnicki M., Rosyjskie przygotowania dezinformacyjne do wojny z Ukrainą, „Cybersecurity & Cybercrime" 2024, T. I, nr. 4.

Nakamura F., 100 maksym o dezinformacji, Warszawa 2020.

Paczuszka A., Rosyjskie służby specjalne czyli jak rozbroić państwo, Łódź 2018.

Pietrobon E., The Art of Secret War, USA 2020.

Sanovich S., Russia: The origins of digital misinformation. [w:] Woolley S. C., Howard P. N. (red.), Computational Propaganda, Oxford 2019.

Schick N., Deep fakes and the infocalypse, Londyn 2020.

Świerczek M., Jak Sowieci przetrwali dzięki oszustwu, Warszawa 2021.

van der Linden S., Fake News, Poznań 2023.

Wrzosek M., Military reconnaissance in the wars of the future forecasted development directions, „Kwartalnik Bellona" 2020, nr. 2.

Wrzosek M., Rosyjska wojskowa operacja specjalna- nowa forma konfliktu zbrojnego?, „Rocznik Bezpieczeństwa Morskiego" 2024, Tom: XVIII.

Zalesiński Ł., Słowa jak pociski, „Polska Zbrojna" 2023, nr. 4.

Zalewski J., Dzierżyński D. G., Wojna informacyjna w odbudowie rosyjskiej mocarstwowości, Warszawa 2019.

[21] M. Wrzosek, Rosyjska wojskowa operacja specjalna- nowa forma konfliktu zbrojnego?, ,,Rocznik Bezpieczeństwa Morskiego" 2024, T. XVIII, s. 589.