Tomasz Gergelewicz*

Fake Mirroring in Cyberspace as a Disinformation Tool – Doppelgangers and Deepfakes

Abstract

The article aims to present two hostile tools employed in the cybersphere against internet users. The first one is doppelganger, and the second one is deepfake. The paper highlights some examples of using both to influence the social cognitive dimension in the infosphere. Diagrams and charts presented in the article depict the vast scope between society and the media, which is the main source of information and the nest for disinformation. The article discusses the use of artificial intelligence for hostile purposes and the possible means by which to gain resilience against disinformation.

Key words: information operations, artificial intelligence, disinformation, doppelganger, deepfake, social resilience.

* Col. Tomasz Gergelewicz, PhD Student, Ministry of National Defense, e-mail: tgergelewicz@mon.gov.pl, ORCID:0000-0002-9145-5099.

Introduction

Using cyber tools for hostile influence in the information environment is one of the disinformation strategies. The impact on social cognition is an important factor in gaining privilege in an information war. This includes cyber battles. Recent technological advancements have enabled backdoor activities to smuggle false information to the target audience. The article highlights two types of a deceptive-aimed use of artificial intelligence (AI). The first type is a doppelganger influence operation, which provides the mirror reflection of internet assets, especially websites. The e-user enters a fake website similar to the original one, but the content is slightly different. The mirrored site consists of source materials mixed with additional fake news, manipulation with facts and information noise[1]. This action is to mislead the target user and to smuggle false content to influence the user's perception of reality. The second type is deepfake, a product based on AI, including machine learning. The engine for creating deepfakes processes large amounts of data to make fake images of a picture or a person. The created image is highly similar to the original. However, it possesses additional features, which may not be obvious at first glance. The final product of deepfake may be a mirrored well-known person expressing opinions written by the hostile actor.

More and more people acquire knowledge mainly from the internet, where fake information, often generated by artificial intelligence, spreads faster. The largest percentage (35%) of people say that if they notice information somewhere that is clearly fake news, they will check the news more carefully. However, few people admit (33%) that identifying fake news does not influence their approach to searching for and obtaining information[2]. Information becomes a powerful weapon, especially in the context of hybrid operations. The Global Trends 2040 report states that „Many countries will face a combination of highly destructive and precise conventional and strategic weapons, cyber activity targeting civilian and military infrastructure, and a misleading disinformation environment"[3]. It highlights the need to gain

1 See more in: T. Gergelewicz, *Obszary budowania odporności na dezinformację jako element bezpieczeństwa infosfery*, „Cybersecurity and Law" 2022, no. 1, p. 72–84.

2 E. Snippe, J. Tar, *Sztuczna inteligencja wystawia wiarygodność mediów na próbę*, https://www.euractiv.pl/section/gospodarka/infographic/sztuczna-inteligencja-wystawia-wiarygodnosc-mediow-na-probe/ [access: 6.01.2024].

3 *Global Trends 2040: A more contested world*, Washington 2021, p. 100.

insight into the challenges posed by the information environment. It is worth stressing that many technological aspects and challenges can impact the human security environment. Modern technologies are subject to analysis by various institutions and organisations. It is currently one of the fundamental factors influencing society and the comprehensively perceived information environment[4]. Research trends suggest that AI will play an increasingly significant role, e.g., in national security. Using AI in the cyber domain may enable the creation of unique mapping capabilities to identify and prevent threats; however, the misuse of AI poses a real threat for the cyber community and, thus, for the global society. As Katarzyna Chałubińska-Jentkiewicz highlights, „Cybersecurity is all the more important because the dangers in cyberspace can adversely affect national security"[5].

Artificial intelligence for cyber threats

Cybersecurity mentioned above includes a highly effective and efficient counter-disinformation process conducted using professional tools, especially new technologies. It has become more than just an important driving force in the lives of citizens. It plays a crucial role in shaping national security. Tanel Kerikmäe emphasises that new technologies are making people smarter. Thus, should anyone worry about combining existing values and the overwhelming dominance of technology? Kerikmäe underlines that by 2045, humans will multiply their intelligence by the wireless connection of their brain with the cyber „cloud"[6]. The development and exploitation of this area raise questions about safety and using technological capabilities by hostile actors. For some global economies, the development of AI has become a priority, and new implementation tools are being developed, e.g., machine learning. The capability provided by optimal or suboptimal selection of algorithms is explored to achieve a specific goal using various strategies. It includes adaptation to

4 *Analiza środowiska bezpieczeństwa w perspektywie 2035 roku*, eds. J. Mokrzycki, R. Reczkowski, S. Cieśla, Bydgoszcz 2020, p. 37.

5 K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021, p. 28.

6 *The Future of Law and eTechnologies*, eds. T. Kerikmäe, A. Rull, Cham 2016, p. 13–14.

surrounding dynamic conditions by learning from experience, using externally provided or self-generated data[7].

To build the mirror image of credible info sources, there is a vast scope for implementing AI. The technology supports hostile actions by identifying, copying, and recreating the content that is further used to deceive and manipulate the target audience. As stated in the Politico – The use of artificial intelligence is significant in doppelganger operations because there is a need for creating authentic-like websites, social media, articles and magazines. Thus, artificial intelligence is involved in mirroring real media and creating a mirror image of credible sources of information[8]. The sophisticated use of AI is highlighted by Record magazine. „Doppelganger's tactics reveal a high level of sophistication, incorporating advanced obfuscation techniques and likely utilising generative artificial intelligence to create deceptive news articles"[9]. The doppelganger operation is conducted directly by the engagement of inauthentic accounts and bots. Personal assets set up Facebook pages (also impersonating media and press agencies) and encourage users to read articles on clone sites. Thus, it is direct propaganda of fake content. The Demigod portal underlines that these propagators „Also managed to run at least 12 advertising campaigns on Facebook promoting pro-Russian and anti-Ukrainian content. This happened despite Meta's (Facebook's owner) policy to block manipulative content. Most disinformation ads were not detected by the platform at all"[10]. Jordan Fischer, Partner at Constangy Brooks, Smith & Prophete, underlines, „AI changes the game with propaganda because of how realistic it can make any of these materials. And, while artists who are being misappropriated can try to fight this, it is often countries where there is no recourse to combat the misuse"[11].

7 *Artificial Intelligence in Defence. Joint Quest for Future Defence Applications*, „European Defence Matters" 2020, no. 19, p. 36.

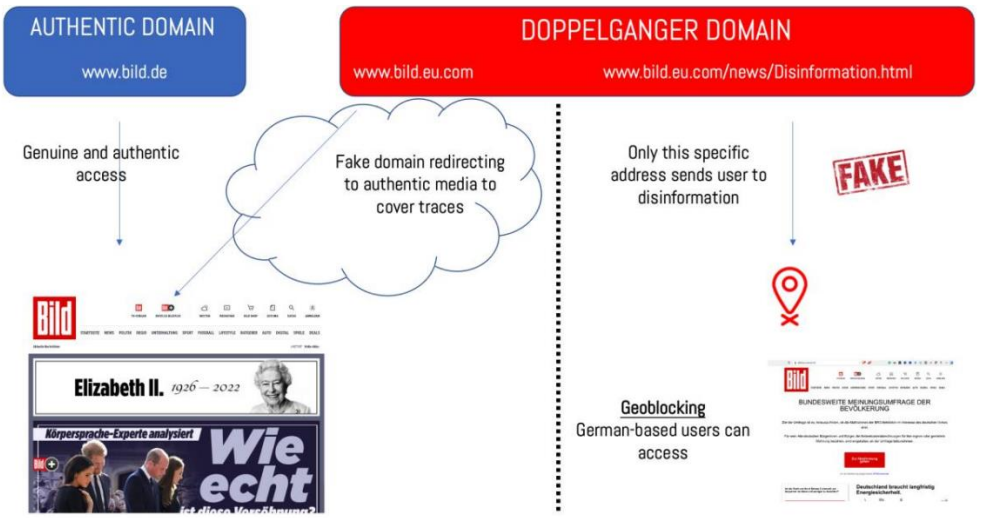
8 L. Kayali, C. Caulcutt, *France exposes mega Russian disinformation campaign*, https://www.politico.eu/article/france-accuses-russia-of-wide-ranging-disinformation-campaign/ [access: 12.11.2023].

9 D. Antonyuk, *Russian-linked Doppelganger social media operation rolls on*, https://therecord.media/doppelganger-influence-operation-new-activity [access: 11.01.2024].

10 *Atak klonów. Dezinformacja pod przykrywką prawdziwych stron*, https://demagog.org.pl/analizy_i_raporty/atak-klonow-dezinformacja-pod-przykrywka-prawdziwych-stron/ [access: 18.10.2023].

11 C. Sivesind, *Fake Celebrity Quotes Target Ukraine in Russian Propaganda Campaign*, https://www.secureworld.io/industry-news/fake-celebrity-quotes-ukraine-russian-propaganda [access: 14.01.2024].

It is also worth noting that hostile actors implement various techniques to cover up their actions. „The doppelganger used an ingenious system that allowed only a very limited number of links to access disinformation. On top of this, they set up a geo-blocking feature: if visitors were not based in Germany, they could not have accessed the German-speaking disinformation they designed”[12].



Source: https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf [access: 18.10.2023].

Graph 1. Limitations for a non-target audience by doppelganger

This solution and geographical restrictions (only users from the selected country could come across the fake website) allowed manipulators to cover up their tracks and build an impression of reliability[13].

Fake mirroring by Russia and China

The first doppelganger operation was documented in 2022 by the European organisation, EU DisinfoLab and the American company Meta. The operation

12 A. Alaphilippe, G. Machado, R. Miguel, F. Poldi, *Doppelganger Media clones serving Russian propaganda*, https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf [access: 22.12.2023].

13 *Atak klon*ów...

was launched to amplify the visibility of articles from pirate sites[14]. The operation was also revealed by the Viginum, the French organisation settled to counter foreign digital interference. The Viginum detected the campaign. This enabled French authorities to implement protection and prevention measures in the cyber domain[15]. The Viginum stresses that the most interference-usable social platform is TikTok – „in comparison with other platforms, which also seek to profile users, TikTok can determine their psychological profile more quickly and consequently improve their algorithms to offer better-targeted videos and increase their commitment"[16]. However, not only does the Viginum counter disinformation in France but there is also a military domain involved in building resilience against malicious influence, „The Cyber Defence Command (COMCYBER in French) remains the leader in France's strategy against disinformation. Its main objective is to protect information systems and undertake military operations in cyberspace, encompassing their planning, design, and execution. In addition, the organisation is looking to expand its personnel, going from around 3600 cyber fighters to around 5000 between 2025 and 2030. This reflects the growing role of information warfare and the desire to better integrate cyber-influence operations into military strategies[17]. Viginum also claims that „We have identified dozens of domain names purchased by Russians. We are not dealing with people who act in a single point, in 'homoeopathic doses'; they are already close to industrial scale. At the same time, we are still determining their ultimate goal"[18].

Catherine Colonna, French Foreign Affairs Minister, stated that „The French authorities have uncovered a digital campaign to manipulate information against France involving Russian actors in which state-owned

14 Ibidem.

15 M. Guilbeault, *Désinformation russe: qu'est-ce que l'„opération Doppelgänger"?*, https://www.la-croix.com/Culture/Desinformation-russe-quest-operation-Doppelganger-2023-06-14-1201271493 [access: 21.01.2024].

16 *Rapport: Fait au nom de la commission d'enquête (1) sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence*, Rapport N° 831, 2022–2023, p. 87, https://www.senat.fr/rap/r22-831-1/r22-831-11.pdf [access: 20.01.2024]. See also English summary: https://www.senat.fr/fileadmin/Structures_temporaires/commissions_d_enquete/CE_Tiktok/ESSENTIEL_Tiktok_EN_en_ligne.pdf [access: 20.01.2024].

17 A. Bourdas, *Disinformation in France: A Strategy of Information Warfare in the Digital Age*, p. 47, https://dspace.cuni.cz/bitstream/handle/20.500.11956/187319/120456400.pdf?sequence=1&isAllowed=y [access: 13.01.2024].

18 M. Chene, *Operation Doppelgänger: how Russia spread fake news in France*, https://insightnews.media/operation-doppelganger-how-russia-spread-fake-news-in-france/ [access: 13.01.2024].

entities or entities affiliated to the Russian state have participated by amplifying false information". Anne-Claire Legendre, French Foreign Affairs Ministry spokeswoman, explained: „The campaign targeted several Western media sites, as well as the Ministry of Foreign Affairs' website and other government sites, by creating mirror sites"[19]. According to C. Colonna – „This campaign is based in particular on the creation of false web pages usurping the identity of national media and government sites, as well as on the creation of false accounts on social networks"[20].

The overall result of identifying these actions was the fact that France accused Russia of conducting a disinformation operation: „The French authorities have revealed a digital information manipulation campaign against France involving Russian actors in which government bodies or bodies affiliated with the Russian state have participated by spreading misinformation"[21]. It was not a single attack but a well-prepared string of influential and time-organised articles with fake content[22]. Among the targets of this operation were info-leaders like Le Parisien, Le Figaro, Le Monde and 20 Minutes. All of them „have fallen victim to this disinformation campaign aimed at imitating French sites for Russian propaganda"[23]. The Demagog underlines other traces of Russia, like the metadata of photos and videos, which indicates the place, the actor, and the time these were taken or produced and placed on the cloned websites. It is also stressed that „Thanks to this, analysts discovered that some of this content is created in the GMT+8 time zone and the Siberia and Irkutsk region"[24]. Catherine Colonna stated in Politico that „The involvement of Russian embassies and cultural centres that actively participated in amplifying this campaign, including via their institutional accounts on social networks, is a further illustration of the hybrid strategy Russia is implementing to

19 *War in Ukraine:what is Russia's Doppelgänger operation that angers France*, https://www.reddit.com/r/europeanunion/comments/1492tdq/war_in_ukraine_what_is_russias_operation/?rdt=48815 [access: 13.01.2024].
20 M. Chene, op. cit.
21 *France's detection of an information manipulation campaign*, https://mt.ambafrance.org/France-s-detection-of-an-information-manipulation-campaign [access: 10.01.2024].
22 Ibidem.
23 *War in Ukraine:what is Russia's Doppelgänger*...
24 *Atak klon*ów...

undermine the conditions for democratic debate"[25]. As Monde highlights, this is „a new episode in the hybrid war between Moscow and the West"[26].

Nathaniel Gleicher, Meta head of security policy, claims that the main goal of the operation was to mimic websites of mainstream news outlets in Europe and post bogus stories about Russia's war on Ukraine[27]. For example, the main narratives pushed by the disinformation campaign are the ineffectiveness of sanctions against Russia; the alleged Russophobia of Western states; the supposed predominance of Nazi ideology among Ukrainian officials; and the negative effects of welcoming Ukrainian refugees for European countries[28]. As described in the Le Monde, false depictions of Ukrainian troops are also common. Hostile campaigns suggest the Ukrainian army has killed more than 13 000 civilians since 2014. This fake news is supported by a photomontage of Zelensky behind bars. The TrueMaps portal, run by pro-Kremlin Western influencers, presented an interactive world map with the number of children killed or injured in the Donbas due to Western arms deliveries[29]. The TrueMaps was identified as a part of a campaign against supplies of Western weapons to Ukraine. This part of the anti-Ukrainian campaign was launched by pro-Kremlin bloggers Alina Lipp and Liu Sivaya. The link to the map was published by RRN and later widely shared by pro-Kremlin Telegram channels[30].

Meta also drew attention to the information operation by Chinese services and banned over eight thousand fake accounts that spread anti-Western and pro-China content[31]. Ben Nimmo, head of Meta's threat intelligence team, noted that Meta had to remove information justifying or discrediting the systemic persecution of the Uyghur minority in Xinjiang. Removing accounts

25 L. Kayali, C. Caulcutt, op. cit.

26 *Opération Doppelgänger: vaste campagne de désinformation russe ciblant des médias français*, Monde 2023, https://www.challenges.fr/monde/operation-doppelganger-vaste-campagne-de-desinformation-russe-ciblant-des-medias-francais_858522 [access: 15.01.2024].

27 *Meta Fights Sprawling Chinese 'Spamouflage' Operation*, https://www.voanews.com/a/meta-fights-sprawling-chinese-spamouflage-operation/7246057.html [access: 13.01.2024].

28 L. Kayali, C. Caulcutt, op. cit.

29 D. Leloup, F. Reynaud, *'Doppelgänger': The making of a Russian disinformation operation*, https://www.lemonde.fr/en/pixels/article/2023/06/14/doppelganger-the-making-of-a-russian-disinformation-operation_6031599_13.html [access: 27.09.2023].

30 *Pro-Kremlin Network Impersonates Legitimate Websites and Floods Social Media with Lies*, https://www.isdglobal.org/digital_dispatches/pro-kremlin-network-impersonates-legitimate-websites-and-floods-social-media-with-lies/ [access: 4.11.2023].

31 A. Alaphilippe, G. Machado, R. Miguel, F. Poldi, op. cit.

was the largest action ever taken against a single operation[32]. Meta succeeded in connecting these social media accounts to Chinese Intelligence. Besides Facebook and Instagram, the campaign covered 50 applications, including X (formerly Twitter), YouTube, TikTok and Russian[33]. The Meta report states that the campaign targeted the United States, Western foreign policies, Taiwan, Australia, Britain, Japan, Europe, Germany, France and Ukraine. B. Nimmo highlights that some actions implemented in China were similar to those of a Russian online deception network, suggesting that there might have been a two-way learning process involved. In addition, the Meta report highlights a switching technology where posted advertisements changed their characteristics and content into political ones, e.g., „posting lingerie ads in Chinese abruptly switched to English and posted organic content about riots in Kazakhstan"[34]. Graham Brookie, senior director of the Atlantic Council's Digital Forensic Research Lab, unveiled that „China is investing an enormous amount of money in the full spectrum of state propaganda, of which this is an important part". He also expressed the opinion on social media that „the Chinese create a facade of engagement on their chosen narratives... that are either beneficial to the [Chinese Communist Party] or harmful to its perceived competitors"[35].

It is worth noting that there are more examples of hostile information operations globally. For example, campaigns in the U.S. and Germany involved fake media outlets such as Election Watch, MyPride, Warfare Insider, Besuchszweck, Grenzezank, and Haüyne Scherben, which publish false and hostile content as original news. What is more, some links employ the Keitaro Traffic Distribution System[36] to assess the overall success and effectiveness of the hostile campaign[37]. Moreover, by manipulating Internet domains, disinformation mirrored the websites of 17 large media and press agencies. These included the German „Bild", Italian „Ansa", British „The Guardian", French

32 *Właściciel Facebooka zakłócił operację propagandową chińskich służb. Wziął się też za rosyjskie konta*, https://businessinsider.com.pl/technologie/wlasciciel-facebooka-zaklocil-operacje-propagandowa-chinskich-sluzb-wzial-sie-tez-za/bdt9emc [access: 12.01.2024].

33 O. Papiernik, *Największa operacja propagandowa chińskich służb zakłócona przez... Zuckerberga*, https://technologia.dziennik.pl/aktualnosci/artykuly/9286660,najwieksza-operacja-propagandowa-chinskich-sluzb-zaklocona-przez-zu.html [access: 22.11.2023].

34 S. Bond, op. cit.

35 Ibidem.

36 To learn more about the tool see: https://keitaro.io/en/ [access: 10.01.2024].

37 *Meta Takes Down Thousands...*

„20 Minutes" and Kenyan KBC. Analysts revealed at least 50 clone sites. Nevertheless, what is more significant is that the mirrored websites included fake public opinion polls[38]. As the Euractiv portal stated – „The websites of the parliament and federal government, as well as local administration bodies and even the airport in Geneva, were attacked by cybercriminals"[39]. It is worth adding some examples of particular original website addresses identified as fake: 1) German „Bild.de", fake: bild[.]vip, bild[.]pics, bild[.]eu.com, blld[.]live, bild[.]llc, bild[.]work, bild[.]ws; 2) British „Theguardian.com", fake: theguardian[.]co.com; 3) French „20minutes.fr", fake: 20minuts[.]com; 4) Ukrainian „rbc.ua", fake: rbk[.]kiev.ua, rbk[.]today[40].

An array of doppelganger techniques

A large section of the public is not aware of disinformation processes. Information pushed on media seems to be fact-proven, expert-checked, confirmed and reliable. In general, the public does not question whether the information is accurate and comes from a credible source. It is, then, not particularly difficult to trick the audiences and influence their perception of the world. Col. As Cedric Leighton underlined – „Humans are hard-wired to believe what they see and hear with their own eyes and ears. When what they see and hear is fake, it's very difficult for people to recalibrate themselves, and that makes it possible for doppelganger-style manipulations to gain traction"[41].

There are some definitions and explanations of the doppelganger operation: 1) A doppelganger originally seems to be „a wraith or apparition of a living person, as distinguished from a ghost. The concept of the existence of a spirit double, an exact but usually invisible replica of every man, bird, or beast, is an ancient and widespread belief"[42]; 2) „The doppelganger operation has strategically focused on audiences in Ukraine, the U.S., and Germany. This targeted approach underscores the operation's intent to influence opinions

38 *Atak klonów*...

39 A. Wolska, *Francja udaremniła rosyjski atak dezinformacyjny*, https://www.euractiv.pl/section/bezpieczenstwo-i-obrona/news/francja-udaremnila-rosyjski-atak-dezinformacyjny/ [access: 10.01.2024].

40 A. Alaphilippe, G. Machado, R. Miguel, F. Poldi, op. cit.

41 C. Sivesind, op. cit.

42 *Doppelgänger*, https://www.britannica.com/art/doppelganger [access: 17.01.2024].

and narratives in these geopolitically significant regions"[43]. In addition, it is stated that creating websites that disinform is part of Russia's long-standing and documented practice of influencing public opinion, which was launched after the Russian invasion of Ukraine. Moscow aims to undermine international support for Ukraine by producing fake news[44]; 3) The doppelganger is described by Meta as the „largest and most aggressively persistent Russian-origin operation". It is a pro-Russian network known for spreading anti-Ukrainian propaganda. Active since at least February 2022, it has been linked to two companies named Structural National Technologies and Social Design Agency[45]; 4) doppelganger is the name of the operation, which has spoofed the domains for notable news sites and spammed out linked stories on social media platforms, some of the stories being partially elaborate. The operation uses the byline of real journalists working for media[46].

Doppelganger operations mean, in general, inauthentic news sites and social media accounts which serve as platforms for disseminating hostile narratives. It is conducted via fake websites that imitate the original ones to convey false or manipulated information to the target audience. It is also a matter of blocking real websites and then pushing forward to the target audience a seemingly real website to smuggle the false content[47]. There are particular steps in creating the fake product as a doppelganger operation's result: 1) at the beginning, the design and appearance of a website or press agency; 2) then, the copy is placed on a purchased domain, whose name confusingly resembles the original; 3) the page is ready for visitors with published false information ready to spread it further[48].

43 *Understanding the Doppelganger Influence Operation: Navigating the Waters of Digital Propaganda*, https://medium.com/illuminations-mirror/understanding-the-doppelganger-influence-operation-navigating-the-waters-of-digital-propaganda-5e5ca5e1d0c7 [access: 12.01.2024].

44 *How Russia Falsifies Western News and Tries to Undermine Support for Ukraine*, https://www.eurointegration.com.ua/eng/news/2023/06/14/7163654/ [access: 30.11.2023].

45 *Meta Takes Down Thousands of Accounts Involved in Disinformation Ops from China and Russia*, https://thehackernews.com/2023/09/meta-takes-down-thousands-of-accounts.html [access: 5.01.2024].

46 *New York Times Spoofed to Hide Russian Disinformation Campaign*, https://www.darkreading.com/threat-intelligence/new-york-times-spoofed-russian-disinformation-campaign [access: 11.01.2024].

47 *What is a DDoS attack?*, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ [access: 20.01.2024].

48 *Atak klonów...*

As a result of such an action, a person who wants to read content on a particular original website, e.g. www.theguardian.com, could accidentally come across a fake article posted on the false site www.theguardian.[co].com. The crucial matter to observe is the high technological development of this switching services technique. It allows us to take the target audience back to the original domain after reading the article on the fake website. With such a shift, it is hard to notice where the turning point was in acquiring real and fake knowledge.

Doppelganger employs different techniques to falsely fit into the infosphere and deceive information users. The doppelganger engages in different methods of deception:

1. One is called *brandjacking*, which means „creating websites that impersonate legitimate media outlets. This technique lends a veneer of credibility to false narratives, making them more persuasive to unsuspecting audiences"[49]. It is also explained as a technique to disseminate adversarial narratives[50];

2. The subsequent technique, *spamouflage*, is the „accounts' tendency to intersperse political posts with random videos and pictures – effectively using spam as camouflage"[51]. *Spamouflage* was also characterised by the Geopolitical Monitor, which enumerates features of this hostile action:

– Coordinated messaging across multiple social media platforms,

– Accounts with AI-generated photos, changing identities, shared identities, little post history,

– Low-quality posts exhibiting poor language quality[52];

3. The next practice characteristic for the doppelganger operation is known as *typosquatting*. It is also called *URL hijacking*. This technique is used by cybercriminals, who cover false websites under addresses very similar to the already existing popular ones. As a result, the user who entered the false

49 L. Kayali, C. Caulcutt, op. cit.

50 *Russia's AI-Powered Disinformation Operation Targeting Ukraine, U.S., and Germany*, https://thehackernews.com/2023/12/russias-ai-powered-disinformation.html [access: 11.01.2024].

51 S. Bond, *Meta says Chinese, Russian influence operations are among the biggest it's taken down*, https://www.npr.org/2023/08/29/1196117574/meta-says-chinese-russian-influence-operations-are-among-the-biggest-its-taken-d [access: 23.11.2023].

52 A. Oien, *China's Spamouflage Disinformation Campaigns: A Threat to Private Business?*, https://www.geopoliticalmonitor.com/chinas-spamouflage-disinformation-campaigns-a-threat-to-private-business/ [access: 11.01.2024].

domain is redirected to a mirror website with fake content[53]. *Typosquatting* is also described in the Iptwins as a type of website which consists of registered domain names that are visually very similar to the official domain names of brand owners. This hostile campaign predominantly targets public and private media outlets, and government agencies[54]. It is highlighted that the *typosquatting* operation is well coordinated and structured, and the initial structure of the operation is named RRN, after the pro-Russian site RRN.world, which stands for the Reliable Recent News (previously called „Reliable Russian News")[55]. The Recorder Future presents examples of shared infrastructure: besuchszweck[.]org, mypride[.]press, and warfareinsider[.]us, which all were within the same CIDR[56] range, 63.250.43.0/24:

Table 1. Doppelganger CIDR range

Domain	IP	Registration Date
mypride[.]press	63.250.43[.]15 63.250.43[.]16	2023-02-27
warfareinsider[.]us	63.250.43[.]15 63.250.43[.]16	2023-07-05
besuchszweck[.]org	63.250.43[.]3	2023-02-24
hauynescherben[.]net	89.117.139[.]218 154.41.250[.]157	2023-07-05

Source: *Obfuscation and AI Content in the Russian Influence Network „Doppelganger" Signals Evolving Tactics*, https://go.recordedfuture.com/hubfs/reports/ta-2023-1205.pdf [access: 14.01.2024].

The registration procedure veiled the source of domains used to mirror the original website. It was conducted to fog the traces of creating the fake image:

53 *Typosquatting – co to jest i dlaczego jest niebezpieczny?*, Fiberlink, https://fiberlink.pl/blog/typosquatting-co-to-jest-i-dlaczego-jest-niebezpieczny/ [access: 6.01.2024].

54 A. Fouré, *Operation Döppelganger: how Russia continues to flood Europe with false information*, https://iptwins.com/2023/06/15/operation-doppelganger-how-russia-continues-to-flood-europe-with-false-information/ [access: 7.01.2024].

55 *War in Ukraine:what is Russia's Doppelgänge...*

56 Classless Inter-Domain Routing (CIDR or supernetting) is a way to combine several class-C address ranges into a single network or route. See: *Classless Inter-Domain Routing*, https://www.ibm.com/docs/en/wip-mg/5.0.0.1?topic=reference-classless-inter-domain-routing [access: 6.01.2024].

Table 2. Stages of mirroring the original website

First-Stage Website	Second-Stage Website	Final Website
theearthangelconnection[.]com	jimjamfit[.]com	electionwatch[.]live
Unknown/Unavailable	buymeagradient[.]com	mypride[.]press
lsfiry[.]gmailster[.]com	buymeagradient[.]com	warfareinsider[.]us
zipplei[.]com risebedutt07[.]club	alfonrust[.]com, bookingyatri[.]com	besuchszweck[.]org
taigamebaisung[.]com	711ggr[.]com	grenzezank[.]com
only-best-kred119[.]buzz	fastnep[.]com	hauynescherben[.]net

Source: *Obfuscation and AI Content in the Russian Influence Network...*

Registering the „first-stage" and „second-stage" websites leads to the final mirror. This is used for disinformation.

The doppelganger uses opinion leaders to make the false narratives viral. Using the recognizability of, e.g., particular celebrities, hostile narratives gain broad-scale influence even globally. The Secure World presents a few quotations attributed to celebrities: 1) Taylor Swift[57]: „Now, how long will this take? The Ukrainians behave like charlatans, and we continue to pay"; 2) Oprah Winfrey[58]: „Supporting Ukrainians is unacceptable. Their actions destroy lives and societies"[59].

Col. Cedric Leighton, CNN military analyst, USAF (Ret.), underlines: „Celebrities are going to have to take control of their messaging and enlist the help of specially trained IT and cybersecurity professionals to combat inauthentic content that is posted in their name on social media platforms"[60].

An array of deepfake techniques

The Communication from the European Parliament on the European Democracy Action Plan states that the rapid development of hostile internet campaigns poses new cyber threats. The impact of the cybersphere is strengthened by

57 279 million followers just on Instagram. See the profile: https://www.instagram.com/taylorswift/ [access: 31.01.2024].
58 22,8 million followers just on Instagram. See the profile: https://www.instagram.com/oprah/ [access: 31.01.2024].
59 C. Sivesind, op. cit.
60 Ibidem.

using advanced technologies[61]. Creators of technological disinformation are looking for a pattern that would impact the vast majority of the public. The Global Trends 2040 report emphasises that large behavioural data sets, which include statistical patterns of human psychology and behaviour, may be significant for predicting and determining the ability to influence individuals[62]. There is a pattern referring to emotions, anchored images and available information. It can effectively influence an information receiver. The use of these elements contributes to the creation of deepfakes – disinformation tools driven by advanced image and sound processing technology[63]. It is worth noting that a professional deepfake requires advanced software and the skills to use it. However, to construct a simple but effective deepfake, it is enough to employ a smartphone application, such as Reface[64] or Doublicat. These applications are used to edit short videos based on a single photo[65].

Olga and Sergiusz Wasiuta explain that technology allows for creating realistic fake films in which people say and do things that would not generally happen. Deepfake is created by uploading a complex set of instructions to a computer along with large data like photos and audio recordings[66]. A computer program learns how to imitate and reproduce a person's facial expressions, voice, movements, characteristic gestures, intonation and the type of vocabulary used. The artificial intelligence system responds, among others, by transferring text into appearance and behaviour, generating movements and synchronising synthesised speech with lip movement. In addition, it also considers details like the distance between the eyes, the distance between

61 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan, Brussels, 3.12.2020, COM(2020) 790 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020DC0790 [access: 21.12.2023].

62 *Global Trends 2040*..., p. 105.

63 A. Żychowski, *Metody wykrywania nagrań typu deepfake*, p. 3, https://pages.mini.pw.edu.pl/~mandziukj/2020-10-28.pdf [access: 9.12.2023].

64 The description of the application at the Apple Store: „Enhance your photo collection with stunningly realistic AI baby and headshot generator using the innovation of AI powered editing features, quickly swap faces on photos, change your hair styles or social media headshots with templates, create AI content from your favorite moments, choose from tons of stylized photo filters, and more" – https://apps.apple.com/us/app/reface-face-swap-ai-photo-app/id1488782587 [access: 29.01.2024].

65 M. Nurski, *Apka do robienia deepfake'ów to murowany hit. Doublicat wstawi Twoją twarz do filmu*, https://komorkomania.pl/38335,apka-do-robienia-deepfake-ow-wstaw-swoja-twarz-do-filmu [access: 9.12.2023].

66 O. Wasiuta, S. Wasiuta, *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, no. 3, p. 21, 24.

the cheekbones, the width of the nose, the blinking frequency, the position of the face in time, facial expressions and microexpressions[67]. It should be noted that such deep interference in the reconstruction of human nature may be controversial and pose legal and ethical challenges[68]. In the article „DeepFakes and Beyond", the authors distinguish the basic methods of creating deepfake by manipulating particular characteristics of a human face: 1) holistic facial synthesis; 2) manipulation of characteristic features; 3) change of identity; 4) changing the means of expressing emotions[69].

Several features of deepfake may reveal to the audience the fact of coming across an artificially created product: 1) no eye movement or blinking; 2) excessive blurring or sharpening of the image; 3) unnatural facial position; 4) lack of reflection in emotions; 5) unnatural gestures of other parts of the body; 6) improper lighting, lack of shadows, etc. [70].

Worth noticing is the fact that various institutions are developing systemic solutions to these issues. In 2016, Defense Advanced Research Projects (DARPA) launched the Media Forensics project called MediFor, which aims to develop a technology for automatically assessing photo or video integrity. The agency develops intelligent software that detects film manipulations, including hair falling, ear movement, light reflection, etc. Similarly, since 2017 the American company AI Foundation has been fighting against video manipulation by developing software to verify media authenticity. The first AI Foundation product, Reality Defender,[71] combines human moderation and machine learning to identify malicious activities, including deepfakes[72].

Resilience against disinformation

Risks in the infosphere that may compromise understanding of reality are the subject of extensive research. Many researchers try to find solutions to strengthen governmental and non-governmental anti-disinformative

67 A. Żychowski, op. cit., p. 16.
68 *Sztuczna inteligencja*, https://cyberpolicy.nask.pl/category/sztuczna-inteligencja [access: 19.12.2023].
69 R. Tolosana, *DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection*, „Journal of Latex Class Files" 2016, vol. 13, no. 9, p. 2–3.
70 A. Żychowski, op. cit., p. 13.
71 See more about the product: https://realitydefender.com/ [access: 10.01.2024].
72 *Global Trends 2040*..., p. 118.

initiatives and public awareness of the disinformation process. Richard Staynings, Teaching Professor at the University of Denver and Chief Security Strategist at Cylera, enumerates reasons for the probable susceptibility of nations to fakehood: 1) defective school education systems in Western communities; 2) communities growing up without the ability to consider and analyse information sources and to condemn illegitimate and unreliable sources; 4) a lack of policy regarding the content propagated on the internet, especially in social media, including Facebook, TikTok, X-Twitter, Truth Social[73].

There is hardly ever an effective policy against individuals and companies that undermine the credibility of the internet as the source of truthful information. Legislative solutions do not catch up with the threats in the infosphere. This practically means that hostile tools are quicker than restrictive legal regulations.

Some states take the problem of disinformation seriously enough to make particular steps to secure the information environment. Initiatives are taken to prevent the overspread and counter disinformation processes. France[74] announced the Paris Call for Trust and Security in Cyberspace. It states: „New and dangerous practices are developing in cyberspace: cybercrime, information manipulation, political or economic espionage, […]. These attacks are becoming increasingly sophisticated and intense. It is thus essential to bring the international community together to ensure peace and security in the digital space"[75]. For instance, Sweden settled the Civil Contingencies Agency, which issued the report „Comprehensive Cyber Security Action Plan 2019–2022". The report highlights a few detailed measures needed to be taken to fulfil the requirements of the Swedish National Cyber Security Strategy: 1) securing a systematic and comprehensive approach in cyber security efforts; 2) enhancing network, product and system security; 3) enhancing capability to prevent, detect and manage cyberattacks and other IT incidents[76].

73 C. Sivesind, op. cit.

74 Examples enumerated in: K. Berzina, E. Soula, *Conceptualizing Foreign Interference in Europe*, p. 1, https://securingdemocracy.gmfus.org/wp-content/uploads/2020/03/Conceptualizing-Foreign-Interference-in-Europe.pdf [access: 19.12.2023].

75 *For trust and security in cyberspace*, https://pariscall.international/en/ [access: 11.01.2024].

76 *Comprehensive cyber security action plan 2019–2022*, p. 9, https://www.msb.se/siteassets/dokument/publikationer/english-publications/comprehensive-cyber-security-action-plan-2019-2022-march-2019.pdf [access: 18.12.2023].

European Union institutions are also focusing on countering information interference. European Parliament issued the „Resolution on Foreign Electoral Interference and disinformation in national and European democratic processes". The resolution is part of a broader strategy of hybrid warfare, and it asked the Commission and the Council for an effective and detailed strategy to counteract Russian disinformation[77].

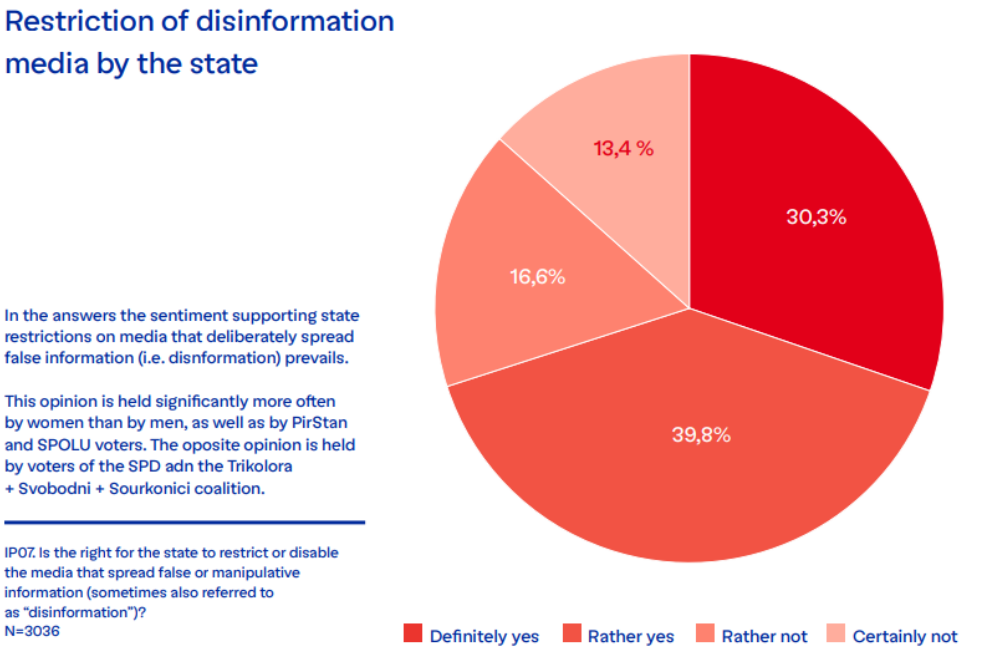
It should be remembered that disinformation operations, including using opinion leaders, social campaigns, micro-targeting, etc., pose a challenge for social platforms. E-societies will demand a secure and friendly environment, just as real-world societies demand it from real governments. Col. Cedric Leighton underlines that „Platforms like Meta's Facebook, Alphabet's Google, and X (formerly Twitter) must ramp up their policing of fake accounts like those used in the doppelganger operation. If they don't, national and international legal systems must hold these platforms accountable for spreading this type of disinformation. The legal issues involved include not only reputational damage but also have national security implications of the highest order"[78].

Regarding false narratives disseminated by media, the research conducted in the Czech Republic shows society's attitude towards the unreliable content shared by media in the context of disinformation spread.

It shows that the public is strongly against sources of manipulation, deception and credibility distortion. More than 70% of the respondents were in favour of restricting or disabling media that are not truthful.

With regard to possible countermeasures to prevail against hostile influence, the Secure World enumerates three basic areas of building resilience against disinformation: 1) fact-checking and awareness campaigns. It is believed essential to provide fact-checking of the information circulating in the infosphere and raise awareness about disinformation; 2) social media platforms need to take action; 3) social media platforms must take responsibility and remove disinformative content and accounts from the information environment; 4) critical thinking and media literacy. Individuals must be eager to think critically to be more mind-independent users of the infosphere[79].

77 *Resolution on foreign electoral interference and disinformation in national and European democratic processes*, p. 2, https://oeil.secure.europarl.europa.eu/oeil/popups/printficheglobal.pdf?id=705759&l=en [access: 18.01.2024].
78 C. Sivesind, op. cit.
79 Ibidem.



Source: M. Hodun, F. Cappelletti, *Putin's Europe*, https://liberalforum.eu/wp content/uploads/2023/12/putins_europe_www-FINAL.pdf [access: 4.01.2024]; original source: https://cedmohub.eu/wp-content/uploads/2023/04/1523801_CEDMO_vlna01_prezentace_web-1.pdf [access: 20.01.2024].

Graph 2. Restriction of disinformation by the state

The discussed hostile cyber-influence operations have not been very effective so far. The Insikt stresses that the impact of doppelganger's activity on users in Germany, Ukraine, and the U.S. is limited: „Despite the campaign's high volume, we did not identify any significant engagement from authentic social media users […]. Viewership and other engagement metrics – reshares, likes, and replies – were negligible across the network"[80]. Despite sophisticated tactics, doppelganger's reach was relatively limited. Engagement metrics indicate minimal interaction from social media users, suggesting a lack of significant impact on public opinion so far[81]. What is more, EU DisinfoLab analysts also suggest that the doppelganger campaign was not very successful. In fact, most of the activity on social media acquiring virality was attributable to accounts and bots, not real users. Internet users were identified as sceptical

80 D. Antonyuk, op. cit.
81 *Understanding the Doppelganger Influence Operation...*

about the published content and often left negative reviews on fake sites with comments like, „Thank you for your worthless post. You get a bonus of 800 rubles”[82].

Conclusion

Advanced technological solutions are increasingly being implemented into the mirroring process. It is not only the exploration of pro-human spheres like medicine but also anti-human areas like deception. One of the technological developments is the widespread use of AI in the data processing.

Rachael Lima underlines that technological advancements will cause the next generation of bots to look and behave like real people. They will have very human-like features, such as facial recognition and natural language processing. It will be possible because of their ability to process large amounts of data[83]. Thus, it is a challenge for government and non-government institutions to follow the latest trends and stay apace with emerging technologies, especially the hostile ones.

Teresa Rothaar, Governance, Risk and Compliance Analyst at Keeper Security, claims that „It's difficult for anyone to stay up-to-date on all of the ways cybercriminals are worming into our lives. However, it's no surprise that nefarious actors use social media to sway public opinion. We tend to believe what we see. This is why aesthetics often trump awareness of inaccurate representations[84]. Thus, it is challenging for societies to think critically and keep an objective approach towards information.

Doppelgangers or deepfakes serve as a reminder of the complexity of modern information warfare conducted by some global actors. The digitalism of everyday life weakens humans' natural protection mechanisms, which are supposed to block harmful content. Nowadays, cloned websites, fake portals, and false accounts are the battleground for hostile activities. Understanding the methods and techniques, or rather strategies and tactics, is crucial for governments, cybersecurity experts, and the public to effectively counter these social threats. Particular countries have turned information into a weapon.

82 *Atak klonów...*
83 R. Lim, *Disinformation as a Global Problem – Regional Perspectives*, Riga 2020, p. 39.
84 C. Sivesind, op. cit.

The weaponising of information led to a situation where internal and external actors increasingly spread disinformation to shape public opinion with fake news, manipulating facts and information noise. As a result, many democracies will probably be put at risk of further erosion or may even collapse[85]. On the other hand, the global flow of information and the development of information technologies is an element of building social awareness around potential threats. Democratic societies have become more resilient to disinformation thanks to technologies capable of the swift identification and debunking fake news[86]. Tim Hwang adds that the ongoing democratisation of technology will facilitate access and enable more actors to create deepfakes in the future. At the same time, the improving state of detection and the remaining limitations of machine learning will reduce the impact of this technology on public discourse[87].

Countering disinformation is a challenge; however, there are several practices that info users can apply to become more aware consumers of information. First, they must ensure that information originates from a credible source, not from a home-grown fake expert, a paid troll or an infobot. Second, it is important to remember that modern technology makes it possible to manipulate and distort almost every picture, text or recording, as any cyber-created matter may be cyber-distorted. Third, we should remember that virality and clickbait come from users themselves, often achieved by evoking emotions; thus, political, religious, sexual or provocative materials should be perceived critically.

Bibliography

Alaphilippe A., Machado G., Miguel R., Poldi F., *Doppelganger Media clones serving Russian propaganda*, https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf [access: 22.12.2023].

Analiza środowiska bezpieczeństwa w perspektywie 2035 roku, eds. J. Mokrzycki, R. Reczkowski, S. Cieśla, Bydgoszcz 2020.

Antonyuk D., *Russian-linked Doppelganger social media operation rolls on*, https://therecord.media/doppelganger-influence-operation-new-activity [access: 11.01.2024].

Artificial Intelligence in Defence. Joint Quest for Future Defence Applications, „European Defence Matters" 2020, no. 19.

Atak klonów. Dezinformacja pod przykrywka prawdziwych stron, https://demagog.org.pl/analizy_i_raporty/atak-klonow-dezinformacja-pod-przykrywka-prawdziwych-stron/ [access: 18.10.2023].

85 *Global Trends 2040...*, p. 8.
86 Ibidem, p. 118.
87 T. Hwang, *Deepfakes – Primer and Forecast*, Riga 2020, p. 16.

Berzina K., Soula E., *Conceptualizing Foreign Interference in Europe*, https://securingdemocracy.gmfus.org/wp-content/uploads/2020/03/Conceptualizing-Foreign-Interference-in-Europe.pdf [access: 19.12.2023].

Bond S., *Meta says Chinese, Russian influence operations are among the biggest it's taken down*, https://www.npr.org/2023/08/29/1196117574/meta-says-chinese-russian-influence-operations-are-among-the-biggest-its-taken-d [access: 23.11.2023].

Bourdas A., *Disinformation in France: A Strategy of Information Warfare in the Digital Age*, https://dspace.cuni.cz/bitstream/handle/20.500.11956/187319/120456400.pdf?sequence=1&isAllowed=y [access: 13.01.2024].

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021.

Chene M., *Operation Doppelgänger: how Russia spread fake news in France*, https://insightnews.media/operation-doppelganger-how-russia-spread-fake-news-in-france/ [access: 13.01.2024].

Comprehensive cyber security action plan 2019–2022, https://www.msb.se/siteassets/dokument/publikationer/english-publications/comprehensive-cyber-security-action-plan-2019-2022-march-2019.pdf [access: 18.12.2023].

For trust and security in cyberspace, https://pariscall.international/en/ [access: 11.01.2024].

Fouré A., *Operation Döppelganger: how Russia continues to flood Europe with false information*, https://iptwins.com/2023/06/15/operation-doppelganger-how-russia-continues-to-flood-europe-with-false-information/ [access: 7.01.2024].

France's detection of an information manipulation campaign, https://mt.ambafrance.org/France-s-detection-of-an-information-manipulation-campaign [access: 10.01.2024].

Gergelewicz T., *Obszary budowania odporności na dezinformację jako element bezpieczeństwa infosfery*, „Cybersecurity and Law" 2022, no. 1.

Global Trends 2040: A more contested world, Washington 2021.

Guilbeault M., *Désinformation russe: qu'est-ce que l'„opération Doppelgänger"?*, https://www.la-croix.com/Culture/Desinformation-russe-quest-operation-Doppelganger-2023-06-14-1201271493 [access: 21.01.2024].

Hodun M., Cappelletti F., *Putin's Europe*, https://liberalforum.eu/wp content/uploads/2023/12/putins_europe_www-FINAL.pdf [access: 4.01.2024].

Kayali L., Caulcutt C., *France exposes mega Russian disinformation campaign*, https://www.politico.eu/article/france-accuses-russia-of-wide-ranging-disinformation-campaign/ [access: 12.11.2023].

Leloup D., Reynaud F., *'Doppelgänger': The making of a Russian disinformation operation*, https://www.lemonde.fr/en/pixels/article/2023/06/14/doppelganger-the-making-of-a-russian-disinformation-operation_6031599_13.html [access: 27.09.2023].

Lim R., *Disinformation as a Global Problem – Regional Perspectives*, Riga 2020.

Meta Fights Sprawling Chinese 'Spamouflage' Operation, https://www.voanews.com/a/meta-fights-sprawling-chinese-spamouflage-operation/7246057.html [access: 13.01.2024].

Nurski M., *Apka do robienia deepfake'ów to murowany hit. Doublicat wstawi Twoją twarz do filmu*, https://komorkomania.pl/38335,apka-do-robienia-deepfake-ow-wstaw-swoja-twarz-do-filmu [access: 9.12.2023].

Obfuscation and AI Content in the Russian Influence Network „Doppelganger" Signals Evolving Tactics, https://go.recordedfuture.com/hubfs/reports/ta-2023-1205.pdf [access: 14.01.2024].

Oien A., *China's Spamouflage Disinformation Campaigns: A Threat to Private Business?*, https://www.geopoliticalmonitor.com/chinas-spamouflage-disinformation-campaigns-a-threat-to-private-business/ [access: 11.01.2024].

Opération Doppelgänger: vaste campagne de désinformation russe ciblant des médias français, Monde 2023, https://www.challenges.fr/monde/operation-doppelganger-vaste-campagne-de-desinformation-russe-ciblant-des-medias-francais_858522 [access: 15.01.2024].

Papiernik O., *Największa operacja propagandowa chińskich służb zakłócona przez... Zuckerberga*, https://technologia.dziennik.pl/aktualnosci/artykuly/9286660,najwieksza-operacja-propagandowa-chinskich-sluzb-zaklocona-przez-zu.html [access: 22.11.2023].

Pro-Kremlin Network Impersonates Legitimate Websites and Floods Social Media with Lies, https://www.isdglobal.org/digital_dispatches/pro-kremlin-network-impersonates-legitimate-websites-and-floods-social-media-with-lies/ [access: 4.11.2023].

Russia's AI-Powered Disinformation Operation Targeting Ukraine, U.S., and Germany, https://thehackernews.com/2023/12/russias-ai-powered-disinformation.html [access: 11.01.2024].

Sivesind C., *Fake Celebrity Quotes Target Ukraine in Russian Propaganda Campaign*, https://www.secureworld.io/industry-news/fake-celebrity-quotes-ukraine-russian-propaganda [access: 14.01.2024].

Snippe E., Tar J., *Sztuczna inteligencja wystawia wiarygodność mediów na próbę*, https://www.euractiv.pl/section/gospodarka/infographic/sztuczna-inteligencja-wystawia-wiarygodnosc-mediow-na-probe/ [access: 6.01.2024].

The Future of Law and eTechnologies, eds. T. Kerikmäe, A. Rull, Cham 2016.

Tolosana R., *DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection*, „Journal of Latex Class Files" 2016, vol. 13, no. 9.

Typosquatting – co to jest i dlaczego jest niebezpieczny?, Fiberlink, https://fiberlink.pl/blog/typosquatting-co-to-jest-i-dlaczego-jest-niebezpieczny/ [access: 6.01.2024].

War in Ukraine:what is Russia's Doppelgänger operation that angers France, https://www.reddit.com/r/europeanunion/comments/1492tdq/war_in_ukraine_what_is_russias_operation/?rdt=48815 [access: 13.01.2024].

Wasiuta O., Wasiuta S., *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, no. 3.

Właściciel Facebooka zakłócił operację propagandową chińskich służb. Wziął się też za rosyjskie konta, https://businessinsider.com.pl/technologie/wlasciciel-facebooka-zaklocil-operacje-propagandowa-chinskich-sluzb-wzial-sie-tez-za/bdt9emc [access: 12.01.2024].

Wolska A., *Francja udaremniła rosyjski atak dezinformacyjny*, https://www.euractiv.pl/section/bezpieczenstwo-i-obrona/news/francja-udaremnila-rosyjski-atak-dezinformacyjny/ [access: 10.01.2024].

Żychowski A., *Metody wykrywania nagrań typu deepfake*, https://pages.mini.pw.edu.pl/~mandziukj/2020-10-28.pdf [access: 9.12.2023].

Fałszywe odbicie lustrzane w cyberprzestrzeni jako narzędzie dezinformacji

Streszczenie

Intencją autora artykułu jest przedstawienie dwóch wrogich narzędzi stosowanych w cyberprzestrzeni przeciwko użytkownikom internetu. Pierwsze z nich to *doppelgänger*, a drugie to *deepfake*. W artykule wskazał przykłady wykorzystania obu metod dezinformacyjnych do oddziaływania na społeczny wymiar poznawczy w infosferze. Zaprezentowane w artykule diagramy i wykresy obrazują rozległy zakres relacji społeczeństwa z mediami, które w istocie są zarówno głównym źródłem informacji, jak i siedliskiem dezinformacji. Autor pokazał wykorzystanie sztucznej inteligencji do wrogich celów oraz konkretne kroki, jakie można podjąć, żeby uzyskać odporność na dezinformację.

Słowa kluczowe: operacje informacyjne, sztuczna inteligencja, dezinformacja, doppelgänger, deepfake, odporność społeczna