ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2022 (31)

DEEPFAKE, PROPAGANDA, DISINFORMATION: IS THERE A DIFFERENCE, AND HOW LAW ENFORCEMENT CAN DEAL WITH IT

Aurelija PŪRAITĖ
Mykolas Romeris University
Maironio str. 27, LT 44211 Kaunas, Lithuania
E-mail: aurelija.puraite@mruni.eu
ORCID ID: 0000-0001-9228-1396

DOI: 10.13165/PSPO-22-31-15

Abstract. *The number of cyber incidents in Lithuania, as in the whole world, is increasing every year. According to the National Cyber Security Center at the Ministry of National Defense, in 2020 cybernetic incidents of a different kind increased by 25 per cent, and the number of incidents related to the distribution of malware increased by as much as 49 per cent, the same trend being observed in other states. Such categories as deep fake, propaganda, and disinformation are related to cybersecurity as well. Propaganda, systemic disinformation campaigns and deep fake content are designed to misinform the public, influence politics and democratic processes, and contribute to fraud and other crimes. It's amazing when deep fake images created with the help of AI add value to a movie but is very threatening and provocative when a fake and heavily manipulated video depicting Ukrainian President Volodymyr Zelenskyy circulated on social media and was placed on a Ukrainian news website by hackers in early March 2022. Is law offering at least some tools that can help victims of crimes that can be incriminated when using deep fakes (such as defamation, intentional infliction of emotional distress, privacy tort, and some others) to protect themselves, and– are law enforcement officials ready to identify and prevent these possible violations, and what other possible threats deep fakes can have on law enforcement activities is being discussed in this article. The author of this article raised a hypothesis that Lithuanian law enforcement institutions, despite being late and reacting to post-incident manifestations of information warfare, have a clear strategy for combating this type of activity, at least to monitor and prevent it. Law enforcement authorities can take specific legal actions only if one or another activity is defined as criminal at the legislative level. Therefore, a methodological decision was made to conduct qualitative research, that is, interviews with two experts who, due to their positions, could discuss the topic of the research. The results of the interviews were unexpected and required the adoption of non-traditional scientific decisions by the author of this article.*

Keywords: *informational warfare, propaganda, disinformation, deep fake, law enforcement.*

Introduction

Recently, due to the geopolitical processes taking place in the world, with the research of hybrid threats receiving special attention, we hear more and more about information threats, and information wars, which can manifest in very different forms. Information threats to national and public security can manifest themselves in various information-based operations, information attacks (IA) can be carried out at any time (especially in special situations when societies face economic or political crises, military or climatic disasters, etc.), they can be directed both at separate individuals, social groups and at society as a whole. Only the object, intensity and level of danger of such attacks differ, as well as the means chosen. Information attacks in peacetime are aimed at selfish political goals, for example, to destroy democratic processes, or to break the will of the citizens of a state to resist in the event of an apparent invasion. Actions of information warfare are manifested in large-scale disinformation campaigns, the course of politics is controlled with the help of social networks, individuals can be radicalized and recruited, they can be given instructions to destabilize society, incite discord between various groups in society and commit crimes against individual groups. The

information space has become a standard platform that allows hostile state or anti-state entities to convey an image of „their reality “, shaping public attitudes in a beneficial direction and motivating or correcting people ‘s behaviour. The significance of the information war that is taking place in Ukraine's war with Russia awaits a very detailed and deep analysis in the future, because disinformation, propaganda, and deep fakes have never had such an impact as they do now.

It must be mentioned that recently the discourses on information wars have moved from more theoretical topics to be attributed to the research field of communication and political technology specialists to a completely different level. The war in Ukraine that started in 2022 showed that the biggest mistake recognized not only by the world ‘s politicians, scientists, and experts but also by Russia's opposition and journalists continuing their activities abroad, was the belief that Russian propaganda is ridiculous, that it is impossible to believe it, that the majority of Russian citizens understand that it is a lie. The reality turned out to be quite different, and very frightening. As some Russian opposition journalists very rightly observed about the middle-aged generation, while protecting our children from the harmful effects of the Internet, we did not notice how our parents became addicted to television and propaganda. Indeed, this lesson is significant - propaganda is not something to be laughed at, to be seen as a tool to bully the stupid and uneducated masses. Such social snobbery and underestimation contributed greatly to the complete moral degradation of Russian society. It became obvious that these phenomena should not only be analyzed theoretically, not only their psychological and political effects should be assessed, but also appropriate legal actions should be taken to prevent information that has the characteristics of propaganda, disinformation, deep fake and poses a threat to the security of the state and society.

Information warfare is a term used to describe the collection, distribution, modification, disruption, interference with, corruption, and degradation of information to gain some advantage over an adversary (Marlatt, 2008; Prier, 2017; Khalilzad et.al., 1999). It should be mentioned, that information warfare does not necessarily need to be related to cyber attacks or technologies in general, more conservative means of spread of disinformation or propaganda is often used as well. The concept of information warfare used in the 1990s accounted for both the psychological and technical factors in digital warfare long before the term “cyber” became so widely used. This article will focus on information warfare methods and the response of law enforcement not relating it with any type of spread channels, however, during the qualitative research (interviews with experts), it became obvious that it is propaganda, disinformation and deep fakes that are spread in cyberspace that are the object of attention of law enforcement authorities. The object of this research is propaganda, disinformation and deep fake, which are part of specific criminal activities, and the ability of law enforcement authorities in Lithuania to react to such acts by implementing innovative monitoring, prevention and investigation actions. The question was raised, whether a law is offering at least some tools that can help victims of crimes that can be incriminated when using, for example, deep fakes (such as defamation, intentional infliction of emotional distress, privacy tort, and some others) to protect themselves, and– are law enforcement officials ready to identify and prevent these possible violations, and what other possible threats deep fakes can have on law enforcement activities is being discussed in this presentation.

The author of this article raised a hypothesis that Lithuanian law enforcement institutions, despite being late and reacting to post-incident manifestations of information warfare, have a clear strategy for combating this type of activity, at least to monitor and prevent it. Law enforcement authorities can take specific legal actions only if one or another activity is defined

as criminal at the legislative level. Therefore, a methodological decision was made to conduct qualitative research, that is, interviews with two experts who, due to their positions, could discuss the topic of the research. The results of the interviews were unexpected and required the adoption of non-traditional scientific decisions by the author of this article.

Methodology. Qualitative research. The work is written based on the descriptive method, intended to discuss scientific material and legal acts related to the concept of information warfare, propaganda, disinformation, and deep fakes. The qualitative research method is used to analyze the readiness of law enforcement institutions to recognize and investigate this type of criminal activity. The qualitative research - interviews with two experts - were conducted in September 2022. Both interviews were conducted remotely using the Microsoft Teams platform and lasted 1,5 hours each, the conversations were recorded, later transcribed using MAXQODA software. Experts were selected according to the areas of their professional competencies. The experts agreed to reveal their identities. One expert was Arūnas Paulauskas, then Deputy General Commissioner of the Lithuanian Police (from December 2022 appointed by the Minister of Internal Affairs as a temporary Head of Public Security Services), who supervised the field of cybercrimes in the Lithuanian police system. Another expert was the Head of the Lithuanian Police School, Robertas Šimulevičius (previously the head of the Training Center of the Criminal Police Bureau), with whom there was a discussion about the training and competence development of officers in the field of cybercrimes and crimes related to the informational system.

The results of the interview of experts were described and commented on by the authors of the research, making assumptions about the reasons for the insights provided by the experts. The discussion is not presented as a separate part of the article but is incorporated mostly as examples in other parts of the research.

The concept of information warfare

The idea that information is crucial to success in warfare is a truism that dates back at least to the ancient Chinese writings of Sun Tzu (2016). In strategic information warfare, the battleground is the information infrastructure and everything related to it. Although the information infrastructure encompasses much more than just the cyber environment, however, for many, they are essentially equivalent terms. In the pre-internet era, information warfare was relatively the threat of narrow action due to both limited distribution and slow impact. Cyberspace has removed the first limitation - the spread of information has become uncontrollable and embraceable. However, the second limitation - the effect on the masses - has become extremely dependent on the information warfare tool. If propaganda is a slow-acting weapon whose effect is not felt immediately, then deep fake is a tool that can have an immediate effect. It's amazing when deep fake images created with the help of artificial intelligence (AI) tools add value to a movie, but it is very threatening and provocative when a fake and heavily manipulated video depicting Ukrainian President Volodymyr Zelenskyy circulated on social media and was placed on a Ukrainian news website by hackers in early March 2022.

When it comes to Information Warfare (IW), it is important to pay attention to an obvious but essential feature - it is a way of warfare that does not have a front line because the purpose of this warfare is not to conquer territory, but to conquer people's minds, and this way „to destroy „the enemy“ not physically attacking the target group, but the minds of the target group, the psyche“ (Ganser, 2005, p. 28). In this research, we do not aim to define information warfare,

this is not the subject of our article; it will suffice to mention that there is no universal or generally accepted definition of 'information warfare', but it is important for us that information warfare is not a single, simple thing, that it has many complex dimensions (Bellamy, 2001). Libicki already in 1995 articulated that „Coming to grips with information warfare...is like the effort of the blind men to discover the nature of the elephant: the one who touched its leg called it a tree, another who touched its tail called it a rope, and so on. Manifestations of information warfare are similarly perceived...[T]aken together all the respectably held definitions of the elephant suggest that there is little that is not information warfare.“ (Libicki, 1995, p. 3). Information warfare could be understood as a „class of techniques, including collection, transport, protection, denial, disturbance, and degradation of information, by which one maintains an advantage over one's adversaries“ (Burns, 1999). During the last decade, IW has become a much-politicised term and keeping in mind the swift of communication channels to internet area and digitalization of media, much related to term „cyber“.

It should come as no surprise that Russia's information attack campaigns have often been the subject of research in recent years when it comes to information warfare. As Whyte analysed, „since at least 2013, nearly two dozen countries across the West and the former Soviet sphere have been victims of interference operations conducted by the Russian Federation“ (Whyte, 2020, p. 167). Russia, of course, is not the only country that uses different information means, the most diverse information channels, as well as dark technologies, such as manipulative use of social media platforms, troll farms, and fabricated news content, but it is undoubtedly an information war, manifested in propaganda, disinformation, fake news, leader. Over the past ten years, and especially actively since 2014 (the beginning of the Russian invasion of Crimea and the start of the war in Syria), social media has served as a battleground for states and non-state actors to spread competing narratives about the war and portray the ongoing conflict on their terms. But since 2022, with the start of Russia's open, aggressive, a wide-scale war in Ukraine, information has become one of the most important weapons off the battlefield like never before. As the war continued, the avalanche of information attacks became even more intense and manifested itself in all classic forms - digital ecosystems were flooded with disinformation, open and hidden propaganda, and fake news. Strategic propaganda campaigns in wartime are by no means new, but a feature of the 21st century is that these campaigns are carried out on social media (Twitter, Facebook, Instagram, TikTok, YouTube, etc.) and these channels have been chosen as the main distribution channels. Therefore, information attacks become the addressee of everyone, which changes the conduct of information warfare, as well as who can participate in ongoing conversations to shape new narratives. The new trend in this war is the beginning of using deep fake (machine learning techniques used to create deep fake media content, where fabrication is immensely difficult to distinguish from reality, most often used in advertising or cinematography).

Summarizing, as it is difficult to say better than Giles (2016) “information warfare can cover a vast range of different activities and processes seeking to steal, plant, interdict, manipulate, distort or destroy information. The channels and methods available for doing this cover an equally broad range, including computers, smartphones, real or invented news media, statements by leaders or celebrities, online troll campaigns, text messages, vox pops by concerned citizens, YouTube videos, or direct approaches to individual human targets” (p. 4). The best response to propaganda is the truth. As expert A. Paulauskas emphasized, recently in the Lithuanian media there could be found quite a few publications about propaganda and disinformation (for example, about how to recognize it), and this is a positive phenomenon,

because public education is the first step for society to become more resistant to information attacks.

The concept of propaganda, disinformation, and deep fake in the context of public security

Content designed to influence behaviour, influence process outcomes, exists and has been used for centuries, but in the 21st century, manipulating information and mass behaviour has become easier as mass communication methods have enabled the wider dissemination of propaganda. French philosopher Jacques Ellul noted the simplicity of propaganda in 1965; according to Ellul, "*propaganda ceases where simple dialogue begins*" (1965, p. 6). For propaganda to work, there must already be a foundation, i.e. a pre-existing narrative to build upon. It also requires at least a minimal historical, logical, cultural, religious or similar basis on which to build a propaganda narrative. There must also be at least a minimum network pre-existing of those who would believe such a narrative for any reason (social environment, personal experiences or traumas, etc.). Such first believers of propaganda very easily believe the very first created propaganda narratives and become their spreaders. When it comes to disinformation, one of the main reasons for the existence of disinformation is people's ignorance, their inability to recognize partial or selective truths and lies. Social networks help spread the created narrative at an incredible speed, especially with modern methods (bots, troll farms, etc.). By definition (Wardle 2018), disinformation is the information created and distributed with the express purpose of causing harm. "Producers of disinformation typically have political, financial, psychological, or social motivations" (Gradon, 2020, p. 136).

Of course, the starting point remains the classic rules of psychology and anthropology - the human tendency to believe the information in social networks that corresponds to his/her already existing beliefs. Those persons, in turn, are likely to share information with others in their network, who are like-minded. Thus, a particular social network accepts the narrative created by propaganda and disinformation as fact. However, creators of propaganda and fake news with criminal goals usually aim for the greatest possible effectiveness, i.e., they aim to not limit themselves in terms of impact to only those addressees who are inclined to believe the specific content. The aim is to spread as widely as possible. Meanwhile, the individuals to whom the full power of social media is directed will never fully understand that the ideas they have are not entirely their own.

What is new in the 21st century is that propaganda is increasingly being talked about as a part of the state's strategic policy, it is no secret that recently a lot of attention has been paid to Russian propaganda and disinformation campaigns managed at the state level (Wagnsson & Hellman, 2018). Propaganda uses a variety of techniques of influence. The aim is to create images (for example, "us vs. them", and "us vs. the enemy"), to work on target audiences, to divide society, to create hatred, to sow fear, etc. People are influenced by massive information flows containing disinformation and psychologically processed by playing on emotions. Information warfare aims to reshape/ change the perception of reality, to break down the sense of security and the unity of society/state/organization (for example, against NATO/EU), and to provoke emotional reactions -hatred, fear and panic. As Tüür indicated, „The interpretation of reality by the target group to be influenced is altered using a combination of psychological operations, disinformation and propaganda, to shape the target group's views in such a way that it is perceived as an objective reality" (2020, p. 15).

Why can propagandistic narratives be dangerous precisely when it comes to public safety? Despite the seemingly obvious answer to this question, researching the scientific literature, as well as the statements of the representatives of law enforcement institutions in the public space, it is clear that propaganda and disinformation are still mostly perceived as political tools, and not as a potential threat to public safety. When presenting specific counterexamples, law enforcement representatives do not dispute them, but their reactions show that these institutions lack education and methodical and systematic training in the areas of phenomenon recognition and potential threat identification.

For example, in 2018 during the World Cup football matches, Russian football hooligans attacked British fans and openly declared violence, and the Russian authorities supported the violence and perceived the hooligans as patriots defending the motherland. The same authorities also made several xenophobic, racist and homophobic statements to the press. For example, a senior official from the Russian Investigative Committee said: "They [Europeans] are surprised when they see a real man looking the way he should. They are used to seeing only 'men' in gay parades" (Sterling, 2016). It is worth noting that before the above-mentioned event, a particularly high number of anti-European discourses were observed in the Russian mass media, pitting Russian football fans against the football fans of European countries, inciting openly racist and homophobic sentiments, and presenting the usually aggressive behaviour of Russian fans as defending "traditional" values (which is a common narrative for Russian propaganda) (Andriukaitis, 2028). Analyzing this example, expert A. Paulauskas was asked if there is a monitoring strategy in the Lithuanian police that would be able to identify the propaganda of preparation for state-sponsored violence, especially during certain sensitive events (in Lithuania, such situations periodically recur during former Soviet memory dates, especially May 9th, on a day which in the Soviet Union, unlike in other allied countries, was considered the Victory Day of World War II). The expert indicated that on historically sensitive days, the presence of police forces is traditionally increased in certain parts of the city (for example, in cemeteries where soldiers of the Soviet Army are buried), but it is not separately observed whether any special propaganda or disinformation campaign is carried out in the public space during that particular period.

Russian propaganda is also characterized by the repetition of narratives, when an effective and effective narrative is discovered, it is repeated in various situations, artificially linking it to actual circumstances. This trend of Russian propaganda towards the Baltic countries is known and analyzed by experts (for example, Andriukaitis, 2020). Expert A. Paulauskas noted that this trend is known to Lithuanian law enforcement institutions as well, but law enforcement cannot take specific actions due to gaps in the relevant laws. The expert also indicated that the Lithuanian Police activities in the prevention of information threats are exclusively associated with ensuring cyber security, and there is no official institutional cooperation related to other forms of IW.

According to the Law on Cyber Security of Lithuania, a cyber incident is an event or action in cyberspace that may cause or causes a threat or a negative impact on the availability, authenticity, integrity and confidentiality of electronic information transmitted or processed by communication and information systems, disrupt the operation, management and provision of services through them (Law on Cyber Security). In other words, the concept of cybercrime is quite narrow and focused on the protection of the systems themselves. The analysis carried out by the State Audit of Lithuania indicates that even though Lithuania is among the countries of the world according to the 2021 United Nations International Telecommunications the cyber security index published by the union is sixth in the world, however, information about cyber

security entities identified by cyber security risks are not accumulated and managed at the national level. More than a third (38 per cent, 81 out of 212) surveyed cyber security entities do not perform cyber security risk assessment, as a result of which new or recurring ones may be missed threats affecting the security status of entities and their activities (State Control, 2021). The independent police activities are very limited in the field of cybersecurity, according the Law on Cyber Security, the police, while preventing and investigating cyber incidents that may have signs of criminal acts: 1) collects, analyzes and summarizes information about cyber incidents that may have signs of criminal acts; 2) determines the procedure for submitting to the police the information necessary for cyber security entities to prevent and investigate cyber incidents that may have signs of criminal acts; 3) has the right, when the service recipient is possibly participating or the communication and information technology equipment used by him is possibly being used for a criminal act, without a court sanction, to give an instruction to the provider of public electronic communication networks and/or public electronic communication services, the provider of electronic information hosting services and digital to the service provider for no longer than 48 hours, and for a longer period - with the sanction of the district court, to limit the activities. The Criminal Code of Lithuania (Criminal Code of the Republic of Lithuania, 2000) foresees only 5 articles related to information security (Articles 196 – 198, Articles titled "Illegal exposure to electronic data", "Illegal impact on the information system", "Illegal interception and use of electronic data", "Illegal access to the information system", "Illegal disposal of devices, software, passwords, codes and other data"), and there are articles that could be related only indirectly with IW (for example, article 122 "Public calls to violate the sovereignty of the Republic of Lithuania by violence"), however, propaganda, disinformation, fake news usually are more sophisticated than simply open and loud calls to fight against the state of Lithuania. All the said above indicates, that there are no direct legal tools to prevent possible actions of IW.

Recent years the spread of disinformation against the Republic of Lithuania was widely acknowledged by governmental institutions and society. False news from Russian and Belarusian propagandists regarding the migration crisis was designed to quickly arouse negative emotions and to discredit Lithuania as a democratic state. As presented by Lithuanian State Security Department and Defence Intelligence and Security Service "National Threat Assessment" of 2022 indicates, "Russian and Belarusian propaganda production on the topic of the migration crisis is characterized by war and hate rhetoric, which was abundant not only in the statements of propagandists themselves but also by the interviewed officials of the regimes" (p. 52). However, law enforcement institutions gave no legal tools to tackle this type of disinformation, as it formally does not violate any legal provision. However, speaking about propaganda of war, there are some legal tools prescribed by law. War propaganda is prohibited by Article 135 of Lithuania's Constitution. Article 170-2 of the Criminal Code states that public support for international crimes entails criminal liability. This article notes that a person who has publicly approved genocide or other crimes against humanity or war crimes recognized by the legal acts of the Republic of Lithuania or the EU or recognized by the decisions of the Republic of Lithuania or international courts, denied them or grossly belittled them, if this was done in a threatening, insulting or insulting way or as a result, public order was disturbed, punishable by a fine or restriction of liberty, or arrest, or deprivation of liberty for up to two years. The Criminal Code also provides for liability for public mockery, contempt or incitement against any national, racial, ethnic, religious or other group of people. However, it is worth noting that these actions investigate the signs of a criminal act only if they are carried out in public. Expert A. Paulauskas acknowledged, that law enforcement responds to received

complaints, but often faces information attacks allegedly countering freedom of speech. This statement is confirmed by Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda (OSCE, 2017), General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression" (Para. 2.a). Officials lack confidence and knowledge, often fearing to exceed their authority and be accused of human rights violations, they do not take proactive steps to prevent disinformation and propaganda.

However, the expert revealed that more attention is paid to deep fake technologies. Deep fakes are created using generative adversarial networks that use artificial intelligence (AI) and two machine learning algorithms: a generator (image creator) and a discriminator (image checker). The police representative revealed that it is the content created with deep fake technologies that have recently been recognized as criminalized, often not only violating personal data protection standards but also aimed at more serious criminal offences - fake pornography, defamation of reputation, identity theft, lately more and more news reports talk about the use of deep-fake images for disinformation, scams, activism and even espionage. The expert revealed that there are fears that the risk of criminal programs with synthetic sound will increase significantly in the coming years, partly due to the growth in the use of voice assistants. This means that, on the one hand, it becomes more and more difficult to reach people with your message, and on the other, it becomes more and more difficult to find the right information as a person. It will also make it increasingly difficult for the police to rely on videos as evidence. As Frederick Dauer (2022) points out, "Deep fake (…) threaten public trust in video and present challenges for law enforcement with new types of investigations, evidence management, and trials. Deep fake media have already been used to commit crimes from harassment to fraud, and their use in crimes will likely expand". Expert A. Paulauskas admits that many police officers are still unaware of how easy it is to create deep forgeries using reasonably accessible databases or programs. The expert stressed that the only way to combat deep fakes is the relevant, systematic education of law enforcement, supported by a holistic approach to the phenomena.

Response of law enforcement. Qualitative research results

The number of cyber incidents in Lithuania, as in the whole world, is increasing every year. According to the National Cyber Security Center at the Ministry of National Defense (NCSC) (2022), 11,659 cyber incidents were registered by the National cyber security centre in 2019-2021, 2020 cybernetic incidents of different kinds increased by 25 per cent, and the number of incidents related to the distribution of malware increased by as much as 49 per cent, the same trend being observed in other states. Such categories as deep fake, propaganda, and disinformation are related to cybersecurity as well, NCSC, applying technical cyber security measures, found the most cases of malware spread in the energy (27 per cent), public safety and legal order (22 per cent) and foreign affairs and security policy (21 per cent) sectors (government of the Republic of Lithuania, 2021). Speaking generally about the use of the latest technologies in organized crime, as well as new crime modus operandi, expert A. Paulauskas noted that law enforcement feels that they are always one step away from the criminal world.

Here it is crucial to mention, and it has been confirmed by the expert A. Paulauskas that especially disinformation, fake news and deep fake can be countered with education, not just in regards to the topics being communicated, but also education about the tactics and methods

used to create these types of IW tools (Morelli & Archick, 2016). This theoretical statement was also confirmed by the expert head of the Police School Robert Šimulevičius, who revealed in an interview that future police officers who study at the Police School, as well as already working officers who participate in training to improve their competencies, receive minimal information about cyber threats, and no information is provided about propaganda and disinformation spread by other means. Officers are trained to work with information systems, but only a very small number of officers who are trained to work in the cyber-police unit are trained in more detail on how to recognize the mechanisms of information attacks. The expert noted that in the fight against disinformation and deep fakes, it is extremely important to combine education (covering a significantly wider range of topics than it is now, the education campaign should include basic information on ways deep fakes are created, how criminals can already utilize deep fake media, and methods to identify it) at all levels with initiatives of the legislature for laws that could help address the threat posed by especially deep fake media. Expert A. Paulauskas also noted that it is necessary to develop partnerships at all levels to use state funds as efficiently as possible because the creation of IT laboratories and the development of activities require significant financial investments. The expert referred to Joint Declaration of the European Police Chiefs, adopted in 2022, which declares that "for law enforcement to bring criminals to justice, mitigate crimes and adequately protect victims in the digital age, the use of AI-supported tools is not a choice but a necessity", and expresses the clear need for more adequate regulation, not leading "to a situation where the police cannot use AI at all or only with considerable effort or delay" (Joint Declaration of the European Police Chiefs on the AI Act, 2022), as it is now in national regulation of Lithuania.

Answering a question could there be a situation soon when a police officer will not be able to collect evidence from a crime scene (as den Dunnen indicated, "It is still unclear what the new meaning of fake and real will be, but it is about the contribution to truth-finding in a certain context, the evidential value" (2021, p. 17)), the expert responded positively. The expert also noted that there is a lack of cooperation with scientific institutions when researchers share the results of project activities and present the latest research insights. Such projects, implemented by Mykolas Romeris university, such as NAAS (a joint project to create a National Information Impact Identification and Analysis Ecosystem, the project is funded by the European Union Funds Investment Operational Program 2014-2020), AGOPOL („Algorithmic Governance and Cultures of Policing. Comparative Perspectives from Norway, India, Brazil, Russia, and South Africa", the project is financed by the Research Council of Norway), are of the primary interest of law enforcement institutions.

The experts were asked to simulate a situation where a controversial incident of police use of force is recorded, and captured by an outsider's mobile phone. Would it be possible that such a video can be manipulated to make it appear that the official made biased, aggressive, insulting statements, and violated fundamental human rights. It may be possible to manipulate the video, edit out citizen resistance, or simulate apparent force used by the officer. The experts answered that such a situation is possible, but with the help of police communication specialists, the impact on society could be neutralized. The author of this article doubts such a perspective expressed by experts, because as evidenced by numerous studies, trust in the police is very fragile and can be destroyed by one irresponsible example, and a deliberate, targeted attack on the reputation of the police would have fatal consequences for public trust in law enforcement. According the survey carried out by the MRU on the order of the Ministry of the Interior in 2021, 78 percent of Lithuanian residents' trust law enforcement institutions, which ranks 7-8 in the European Union according to the relevant indicator (Official Statistics Portal, 2022). For

the police, such an erosion of trust would mean that it would be necessary to work even more transparently, even more openly, in order to restore trust, so it can be assumed that experts underestimate the possible impact of deep fakes on police activities.

Conclusions

It is obvious that the information war as a hybrid threat to the growth of the state and society is becoming more and more sophisticated, manifesting itself in more and more diverse forms, from the political and diplomatic level, propaganda, disinformation is moving into the criminal space, because the consequences of such information attacks can be extremely dangerous. For law enforcement, those cases are particularly relevant when some forms of disinformation and propaganda may harm individual reputations and privacy, or incite to violence, discrimination or hostility against identifiable groups in society. Therefore, at the level of legislation, as well both at the level of training law enforcement competencies, and the awareness of law enforcement officers, they must be prepared to identify, prevent, and prosecute such acts. Interviews with experts revealed that its law enforcement is currently focusing mainly on cybercrimes related to illegal economic and financial activities, hate crimes, but activities that are based specifically on informational attacks (propaganda, disinformation, fake news) are poorly understood and harder to recognize. Currently, law enforcement officers are more often trained to recognize content created by deep fake technologies, especially related to revenge pornography. The experts emphasized that, considering the geopolitical processes taking place in the neighbourhood of Lithuania, it is necessary to increase the awareness of officials about propaganda, disinformation, which can pose a threat to public safety (for example, by initiating riots, disturbances, inciting hatred towards specific individuals).

References

1. Andriukaitis, L. (2020). *Russian Propaganda Efforts in the Baltics and the Wider Region*. Vilnius Institute for Policy Analysis. Retrieved from: https://vilniusinstitute.lt/wp-content/uploads/2020/05/VIPA_Andriukaitis_2020_Iv4-1%D0%B5.pdf
2. Andriukaitis L. (2018) *Russian Disinfo Patterns: Kremlin's Defensive FIFA 2018 Narrative*. Vilnius Institute for Policy Analysis for Integrity Initiative. Retrieved from: https://vilniusinstitute.lt/wp-content/uploads/2019/07/8-Defensive-FIFA-Narrative.pdf
3. Bellamy, C. (2001). What is Information Warfare? In: Matthews, R., Treddenick, J. (eds) *Managing the Revolution in Military Affairs*. Palgrave Macmillan, London. https://doi.org/10.1057/9780230294189_4
4. Burns, M. (1999) *Information Warfare: What and How?* Retrieved from: https://www.cs.cmu.edu/~burnsm/InfoWarfare.html
5. Criminal Code of the Republic of Lithuania (2000). *Law on the Approval and Entry into Force of the Criminal Code of the Republic of Lithuania. The Criminal Code*. 2000, September 26, No. VIII-1968. Valstybės žinios, 2000-10-25, Nr. 89-2741.
6. *Cybersecurity Law of the Republic of Lithuania*. 2014, December 11. No. XII-1428. TAR, 2014-12-23, No. 20553.
7. Dauer, F. (2022) Law Enforcement in the Era of Deepfakes. Police Chief. Retrieved from: https://www.policechiefmagazine.org/law-enforcement-era-deepfakes/

8. Dunnen, M. (2021). Synthetic Reality & Deep Fakes Impact On Police Work. October 2021, European Network of Law Enforcement Technology Services, Retrieved from: https://enlets.eu/wp-content/uploads/2021/11/Final-Synthetic-Reality-Deep-fakes-Impact-on-Police-Work-04.11.21.pdf

9. Ellul, J. (1965) *Propaganda: The Formation of Men's Attitudes*. New York: Knopf, p. 6.

10. Ganser, D. (2005). Fear As a Weapon: The Effects Of Psychological Warfare On Domestic And International Politics. *World Affairs: The Journal of International Issues*, 9(4), 24–40. Retrieved from: https://www.jstor.org/stable/48531828.

11. Giles, K. (2016). *Handbook of Russian Information Warfare*. NATO Defense College Cataloguing in Publication. Retrieved from: https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook,%20Russian%20Information%20Warfare.pdf

12. Government of the Republic of Lithuania (2021). Resolution On the National Cyber Security Strategy Confirmation, 2018, August 13, No. 818, TAR, 2018-08-21, Nr. 13252.

13. Gradon, K. (2020) Crime in the Time of the Plague: Fake News Pandemic and the Challenges to Law-Enforcement and Intelligence Community. *Society Register* 2020/ 4(2), pp. 133-148. DOI: 10.14746/sr.2020.4.2.10.

14. *Joint Declaration of the European Police Chiefs on the AI Act* (2022). 07 October 2022. Retrieved from: https://www.europol.europa.eu/publications-events/publications/joint-declaration-of-european-police-chiefs-ai-act

15. Khalilzad, Z., White, J. P., Marshall, A. W. (eds.) (1999) *Strategic Appraisal. The Changing Role of Information in Warfare*. DOI: https://doi.org/10.7249/MR1016.

16. Libicki, M. M. (1995) *What is Information Warfare?* National Defence University, Retrieved from: https://smallwarsjournal.com/documents/libicki.pdf

17. Morelli, V. L., Archick, K. (2016). *European Union Efforts to Counter Disinformation*. Congressional Research Service.

18. Marlatt, G. (2008) *Information Warfare and Information Operations (IW/IO): A Bibliography*. Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/6974/Jan08-IWall_biblio.pdf?sequence=1&isAllowed=y

19. *National Threat Assessment. 2022* (2022) State Security Department of the Republic of Lithuania and Defence Intelligence and Security Service under the Ministry of National Defence. Retrieved from: https://www.vsd.lt/wp-content/uploads/2022/04/ANGL-el-_.pdf

20. OSCE (2017). Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, FOM.GAL/3/17, 3 March 2017, Retrieved from: https://www.osce.org/files/f/documents/6/8/302796.pdf

21. Official Statistics Portal (2022), retrieved from: https://osp.stat.gov.lt/pradinis

22. Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, 11(4), pp. 50–85. http://www.jstor.org/stable/26271634

23. State Control (2021). STATE AUDIT REPORT. CYBER SECURITY ASSURANCE. 2022, October 27, No. VAE-10. Retrieved from: https://www.valstybeskontrole.lt/LT/Product/24128

24. Sterling, B. (2016). *Disinformation Digest*, NOV 20, 2016, retrieved from: http://us11.campaign-archive1.com/?u=cd23226ada1699a77000eb60b&id=495b28ffc2

25. Sun Tzu, Lao-Tzu, Confucius (2016). *The Art of War & Other Classics of Eastern Philosophy*. Simon & Schuster Inc.

26. United Nations Special Rapporteur on Freedom of Opinion and Expression, Organization for Security and Co-operation in Europe Representative on Freedom of the Media, Organization of American States Special Rapporteur on Freedom of Expression, and African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information (2017). *Joint declaration on freedom of expression and "fake news," disinformation and propaganda*. March 3. Retrieved from: http://www.osce.org/fom/302796

27. Wagnsson, Ch., Hellman, M. (2018). Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare. *JCMS*, 2018 Volume 56, Number 5, pp. 1161–1177. https://doi.org/10.1111/jcms.12726

28. Wardle, C. (2018) *Information Disorder: The Essential Glossary*. Harvard, MA: Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School.

29. Whyte, C. (2020). Protectors without Prerogative: The Challenge of Military Defense against Information Warfare. *Journal of Advanced Military Studies*. 11(1), pp. 166-184. Retrieved from: https://www.muse.jhu.edu/article/796248.

Acknowledgements. This article was written with the full financial support of the AGOPOL project. „ALGORITHMIC GOVERNANCE AND CULTURES OF POLICING. Comparative Perspectives from Norway, India, Brazil, Russia, and South Africa" (AGOPOL) project is financed by the Research Council of Norway, project duration: 01.04.2021 – 31.03.2024; Project Owner: Work Research Institute, OsloMet - Oslo Metropolitan University, Norway; Collaborating Partners: Norwegian Institute for Defence Studies, Universidade Federal Fluminense, University of Bergen, University of Oslo, Jawaharlal Nehru University, Mykolas Romeris University, Universität Heidelberg, Universiteit Utrecht, College of International and Public Relations Prague, OsloMet/NOVA.