Crime in the time of the plague: fake news pandemic and the challenges to law-enforcement and intelligence community

Gradoń, Kacper

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Gradoń, K. (2020). Crime in the time of the plague: fake news pandemic and the challenges to law-enforcement and intelligence community. *Society Register*, *4*(2), 133-148. https://doi.org/10.14746/sr.2020.4.2.10

SOCIETY REGISTER 2020 / 4(2): 133-148
ISSN 2544–5502
DOI: 10.14746/sr.2020.4.2.10

CRIME IN THE TIME OF THE PLAGUE: FAKE NEWS PANDEMIC AND THE CHALLENGES TO LAW-ENFORCEMENT AND INTELLIGENCE COMMUNITY

KACPER GRADOŃ[1]

[1] University of Warsaw, Faculty of Law and Administration & Centre for Forensic Sciences, Krakowskie Przedmieście 26/28, 00-927 Warsaw, Poland. ORCID: 0000-0003-0750-8678, Email: k.gradon@wpia.uw.edu.pl

ABSTRACT: The Paper explores the problem of fake news and disinformation campaigns in the turmoil era of the COVID-19 coronavirus pandemic. The Author addresses the problem from the perspective of Crime Science, identifying the actual and potential impact of fake news propagation on both the social fabric and the work of the law-enforcement and security services. The Author covers various vectors of disinformation campaigns and offers the overview of challenges associated with the use of deep fakes and the abuse of Artificial Intelligence, Machine-, Deep- and Reinforcement-Learning technologies. The Paper provides the outline of preventive strategies that might be used to mitigate the consequences of fake news proliferation, including the introduction of counter-narratives and the use of AI as countermeasure available to the law-enforcement and public safety agencies. The Author also highlights other threats and forms of crime leveraging the pandemic crisis. As the Paper deals with the current and rapidly evolving phenomenon, it is based on qualitative research and uses the most up-to-date, reliable open-source information, including the Web-based material.
KEYWORDS: COVID-19, Wuhan virus, coronavirus, fake news, deep fakes, nation-state influence, information warfare, Artificial Intelligence, law enforcement

INTRODUCTION

The 2019/2020 COVID-19 pandemic has – at the time of writing (late March 2020) - affected almost all of the countries and territories of the World. It has created unprecedented chaos and unrest and has taken a significant toll on human lives (CSSE 2020), mental and physical health, and wellbeing and – to an unparalleled extent – world economy (OECD 2020). One of the impacts the COVID-19 fallout has on the society, is the rise in cyber-enabled crime, terrorism, and information warfare including – but not limited to – disinformation campaigns and fake news propagation, that are undermining social fabric, causing civil unrest, and increasing the emotional consequences: fear, anxiety and uncertainty. This translates directly to the increased challenges for the law-enforcement agencies and institutions responsible for public security and safety.

METHODS

The following paper provides the overview of the on-going developments in the problem domain. Due to the fact that it deals with phenomenon evolving at an extremely rapid pace, it is based on the qualitative analysis of the up-to-date open source data, in accordance with the International Association of Law Enforcement Intelligence Analysts and United Nations Office for Drugs and Crime (UNODC 2011) recommendations regarding the source evaluation (level A: no doubt regarding authenticity, trustworthiness, integrity, competence and history of complete reliability) and information evaluation (level 1: no doubt about accuracy) as well as source reliability (level A: completely reliable) and data validity (level 1: confirmed).

FUTURE CRIMES AND BLACK SWANS

In mid-July 2019, less than six months before the first reports on the new virus originating in the city of Wuhan in the Chinese province of Hubei appeared, the EUROPOL (European Union Agency for Law Enforcement Cooperation) published a report titled "Do Criminals Dream of Electric Sheep? How technology shapes the future of crime and law-enforcement" (EUROPOL 2019), where the Agency raised the alarming necessity of developing the foresight analysis capabilities arising from the increased threat of abuse of emerging and disruptive technologies. The Report covered the broad area of the so-called 'future crimes' and included the section on the new avenues of disinformation and fake news propagation. The Europol's Report coincided with the UK Parliament Report "Preparing for the Changing World" (UK Parliament 2019) which raised – in the chapters devoted to the new directions in cyber security and emerging computer technologies – the very similar concerns, stressing that cyber-enabled crime might significantly impact the landscape of law-enforcement and intelligence work. The UK Parliament Report stressed the problem of the undue influence of fake news on public opinion, indicating – among others – the cases where the disinformation campaigns touch the area of health-related information, indicating explicitly – quoting Broniatowski et al (2018) - the situations where the Russian bots, trolls and

'content polluters' have been agitating debate on social media platforms about the efficacy of vaccines. Both the EUROPOL and UK Parliament Reports were not referring to the potential threat of the worldwide pandemic (even in the context of the possible leverage of fake news campaigns) and focused primarily on other types of hazards and challenges. They both stressed however, that the economic costs of cyber- and cyber-enabled crimes are progressing massively, as further confirmed by numerous official national and supranational reports (EUCPN 2015; EPTT 2019; EUROPOL 2019a; UK Parliament 2019).

The Reports acknowledged above did not specifically address the global pandemic scenario, as it is an incident that – in theory - belongs to the category of High Impact – Low Probability Events (HILPs). Some types of HILP events are also referred to as the "Black Swans." According to the definition coined by Taleb (2010:xxii), a Black Swan is an event with the following three attributes: first, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility; second, it carries an extreme impact; third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable.

UK Parliament (2019) mentions the term of 'pandemic' in a specific context saying that their Report sketches out the implications of possible areas of change (some of them undesirable), and remarking that: "low probability but high impact events (...) such as the eruption of a super volcano or a pandemic, could make all such considerations irrelevant." The Blackett Review (Government Office of Science 2011), covering the High Impact Low Probability risks references the National Risk Register categories, listing pandemic human disease among other threats (such as coastal flooding, an attack on crowded places or on transport, a major industrial accident, or an outbreak of an animal disease), but still considers it to be a Black Swan type of an event.

Lee, Preston and Green (2012) cover the HILP events and say that they can be broadly divided into three types according to the general level of preparedness: "Black Swans" (events which are beyond the realm of normal expectations in history, science, finance and technology and therefore impossible or extremely difficult to predict), "Known and prepared for" (rare events which pose a significant threat (real or perceived), often as a result of historical experience or technological advance) and "Known but unprepared for" (rare events which governments and businesses may have identified as a potential threat, but where little or no action is taken to prevent or mitigate the impacts. The Authors list the "flu pandemics" under the category of "Known and prepared for" events. They say that in regards to such type of HILP event, "to a greater or lesser extent, governments and businesses invest in a wide range of preventative actions, warning systems and security measures to limit the impacts. (...) Evaluating the costs and benefits of different levels of preparedness is difficult, however, given that an event may not occur for years or decades."

It must be stressed though, that the current pandemic was not entirely the unforeseen or completely unpredictable scenario. The U.S. Department of National Intelligence (DNI) stated in January 2019 that "The United States and the world will remain vulnerable to the next flu pandemic or large-scale outbreak of a contagious

disease that could lead to massive rates of death and disability, severely affect the world economy, strain international resources, and increase calls on the United States for support" (Coats 2019). As recently as September 2019, the Global Preparedness Monitoring Board (GPMB 2019) said explicitly: "there is a very real threat of a rapidly moving, highly lethal pandemic of a respiratory pathogen killing 50 to 80 million people and wiping out nearly 5% of the world's economy. A global pandemic on that scale would be catastrophic, creating widespread havoc, instability and insecurity. The world is not prepared." Taking such clear warnings into account, the current situation (at the time of writing, that is in the end of March 2020) shows that the governments and emergency services worldwide were not prepared for the devastating scale of the developing pandemic and its catastrophic consequences.

DISINFORMATION IN THE TIME OF PANDEMIC

Some of the effects of the coronavirus pandemic that are generally overlooked at this early stage of the development of the global threat (when most of the focus is naturally put on the imminent, destructive consequences to health, life and economy) are the resulting developments in crime and terrorism. One of these threats is a rise of fake news and disinformation campaigns (distributed primarily on social media), bearing the characteristics of the nation-state sponsored, information warfare operations. 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. Fake news may also have a form of misinformation that is information being false, but not intended to cause harm - for example, individuals who don't know a piece of information is false may spread it on social media in an attempt to be helpful. Finally, malinformation is genuine information that is shared to cause harm. This includes private or revealing information that is spread to harm a person or reputation.

According to the U.S. Department of Homeland Security (2019), disinformation campaign occurs when a person, group of people, or entity (a "threat actor") coordinate to distribute false or misleading information while concealing the true objectives of the campaign. The objectives of disinformation campaigns can be broad (e.g., sowing discord in a population) or targeted (e.g., propagating a counter-narrative to domestic protests) and may employ all information types (disinformation, misinformation, malinformation, propaganda, and true information). The target of a disinformation campaign is the person or group the threat actor aims to influence in order to achieve the campaign's objective.

The increasing prevalence of fake news and disinformation campaigns is characteristic for the catastrophe situations: the U.S. Department of Homeland Security (2018) states explicitly: "Rumors, misinformation and false information on social media proliferate before, during and after disasters and emergencies." The law-enforcement agencies and intelligence services should possess an established set of analytical tools, guidelines and strategies to combat various threats arising from or leveraging the disaster scenario. Such tools require calibration to specific needs and the scale of asso-

ciated hazards, but the Police services and organizations (both on national levels and on the international scale: EUROPOL, Interpol) shall be aware of the potential vectors of the attack or disruption and have the capabilities to pro-actively mitigate the risk, either by employing their investigative and enforcement powers, or by utilizing the responsible communication campaigns. The present situation shows that the Police and public security institutions worldwide (collaborating with academic think-tanks and working groups, as well as the Non-Governmental Organizations) are aware of these threats and aim to lessen the consequences of the information and telecommunication technologies' abuse; both the EUROPOL (2020) and the Interpol (2020) have employed the thorough communication strategy involving the information campaign directed both at the professional community and the general public.

As opposed to the earlier natural disasters (earthquakes, fires, volcano eruptions, tsunamis) or emergencies (such as the Fukushima Nuclear Power Station meltdown), even the ones having severe international impact, the current COVID-19 pandemic has spread quickly beyond its original Chinese source (Hubei province) and – at the time of writing – affected almost all of the countries in the World, on all continents apart from Antarctica, bringing unprecedented chaos, fear and uncertainty. It translates to the levels that disinformation campaigns can reach, as although they are never technically constrained to a specific region, they regularly tend to focus on a particular area or population group. The 2019/2020 Wuhan virus pandemic has a truly global range, enabling for the potential information warfare and other acts of state-sponsored terrorism to reach unparalleled levels.

There are numerous possibilities of who the potential instigator of disinformation campaigns could be. It could be nation-states aiming to influence the situation abroad; it could be rogue governments deliberately seeking to disrupt the life of the foreign population; it could be any group or entity intending to benefit economically or politically – be it terrorist organization, extremist group, or organized crime. Alternatively, it could be – as it frequently happens in the on-line environment – a group of non-state actors who run the so-called trolling campaigns for the sheer objective of spreading chaos and confusion.

Currently, in regards to COVID-19 pandemic, the intelligence reports point primarily to Russia and China as the main initiators of disinformation campaigns. The Russian influence in particular gained the worldwide attention with Reuters (Emmott 2020), Guardian (2020) and Deutsche Welle (2020) - among others – covering the news backed by the internal EU sources. Avast Security News Team reports that an internal document circulated among European Union officials alleges that Russia launched a „significant disinformation campaign" about the coronavirus in order to cause panic and worsen the impact of the outbreak on European countries. Created by the European External Action Service, the EU's foreign policy arm, the document claims Russia is servicing its end goal to subvert European societies by pushing disinformation online in English, Spanish, German, and French regarding the virus in order to confuse and hinder the EU's response to the pandemic. The campaign includes contradictory information and fake news such as the idea that the virus is a U.S. biological weapon (Avast 2020).

The New York Times (2020) highlights the involvement of both Russia and China in disinformation campaign related to coronavirus pandemic, saying specifically that both powers have both seized on the novel coronavirus to wage disinformation campaigns that seek to sow doubts about the United States' handling of the crisis and deflect attention from their own struggles with the pandemic. According to the Diplomat (2020) magazine, as the COVID-19 pandemic aggravates all over the world, a coronavirus-related disinformation campaign from China has been on the rise globally. The Diplomat magazine says: "this is true of China's offensives against Taiwan as well. The Investigation Bureau of Taiwan has substantiated significant increase in the dissemination of disinformation regarding the coronavirus outbreak in Taiwan. The disinformation campaigns often spread through social media platforms and are promoted by a variety of fake accounts through either posts or comments. Not surprisingly, most of the contents can be traced to Chinese online forums."

Such observations are further backed by the official Special Briefing of the U.S. Department of State (2020), where Lea Gabrielle, the U.S. Special Envoy and coordinator of the State Department's Global Engagement Center (GEC), says that since January the GEC has been tracking narratives promoted by Russian, Chinese, and Iranian-sponsored sites or different platforms related to the coronavirus. The U.S. Envoy further explains that „Russian disinformation campaign is a known Russian tactic of perpetuating disinformation by capitalizing on the chaos and the uncertainty that health scares and pandemics engender, and we are still seeing the Kremlin continue its reckless attempts to propagate disinformation, endangering global health by undermining the efforts of governments, of health agencies and organizations that are in charge of disseminating accurate information about the virus, such as the World Health Organization. We're also seeing Russia's ecosystem promoting narratives advanced by China and Iran, often ones that were first advanced by Russia." Ms. Gabrielle states: „during the crisis, we've seen Russian, Chinese, and Iranian state disinformation and propaganda ecosystems all converge around some disinformation themes intended to promote their own agendas. So on China, over the course of the crisis we've monitored a couple of narrative tracks. One is malign disinformation to falsely blame the U.S. as the origin of the coronavirus and the second has been China's effort to turn the crisis into a news story highlighting supremacy of the Chinese Communist Party (CCP) in handling the health crisis. What we've seen is the CCP mobilizing its global messaging apparatus, which includes state media as well as Chinese diplomats, to push out selected and localized versions of the same overarching false narratives." The Envoy also says „COVID-19-related topics account for about half of the content pushed by official Chinese accounts since the outbreak in early January in the Western Hemisphere. And we've seen China – they are relying on essentially a unified messaging apparatus. The PRC officials that we saw in Africa shifting their narratives, we've also seen that happening in Italy as well. So PRC officials have become really active and are showing concerted effort to systematically cater their messages to global audiences using hash tags, increasing their social media followers to convince people that they're acting responsibly, rather, and providing aid." Finally, the Global Engagement Center representative states that „we see Russia and Kremlin platforms pushing out false narratives, those false narratives being repeated by other state actors, including Beijing,

and then Russia re-tweeting them again and pushing them out as though they originally came from those state actors."

Of course, not all of the disinformation campaigns use the same strategies or agenda. As Avast Security News Team (Avast 2020) reports, the Bleeping Computer (2020) cyber security experts findings indicate the increase in coronavirus-related spear-phishing attacks, where a state-sponsored threat actor is attempting to deploy the Crimson Remote Administration Tool (RAT) onto the systems of targets via a spear-phishing campaign using Coronavirus-themed document baits disguised as health advisories. This nation-backed cyber-espionage is suspected to be based and operating from the territory of Pakistan. The group, active since at least 2016, is known for targeting Indian defense and government entities and for stealing sensitive information designed to bolster Pakistan's diplomatic and military efforts. Bleeping Computer has reported on other nation-backed hackers seizing the moment to push their agendas, including groups based out of Pakistan, North Korea, and China. Additionally, non-political hackers are launching their own COVID-19 scams in the hopes of making money off of the global panic. Avast (2020) advises that the general public should not trust any information that they cannot verify, and shall always look for the source of the information and only trust official websites like the World Health Organization and the Centers for Disease Control and Prevention.

ARTIFICIAL INTELLIGENCE – A DOUBLE-EDGED SWORD

Although it is not yet an alarming problem (at the time of writing), we still need to take into account the upcoming developments in the disinformation-enabling technologies. During the "Artificial Intelligence & Future Crimes" workshop organized in February 2019 by the University College London (UCL) Dawes Centre for Future Crimes (the only formal research center in the World devoted specifically to the study of the problems related to the hazards associated with the emerging Information Technologies being used as tools by the criminal offenders), we were confronted with 20 scenarios of AI-enabled crime. The participating Subject Matter Experts were asked to rate them according to four factors (harm, profit, achievability, profitability) and to rank them in regards to the necessity of potential intervention (ignore, watch, act). At the very top of scenarios that we selected was the abuse of Artificial Intelligence for the purpose of creating AI-authored fake news and audio/video impersonation. At the time of the workshop, the participants were not discussing the potential exploitation of AI to create and spread disinformation during the disaster scenarios of the COVID-19 magnitude, but it was acknowledged that the opportunities for AI-enabled content manipulation are very high and the potential market for its propagation is broad.

Artificial Intelligence allows for creation of the so-called deep fakes (that are not – contrary to the common misconception – a synonym to 'fake news'). By definition (Wardle 2018), deep fake is the term currently being used to describe fabricated media produced using Artificial Intelligence. By synthesizing different elements of existing video or audio files, AI enables relatively easy methods for creating 'new' content, in

which individuals appear to speak words and perform actions, which are not based on reality. Although 'deep fakes' are still in their infancy, it is likely we will see the term 'deep fakes' used more frequently in disinformation campaigns, as these techniques become more sophisticated. It was acknowledged at the aforementioned 2019 UCL Dawes Centre workshop, where the Subject Matter Experts acknowledged that the high quality of the content produced with AI and Deep Learning technologies (including audio and video impersonation) is highly deceiving and convincing.

According to the European Parliament (2019) Report, it can be argued that 'deep fakes' present an even more difficult problem than manipulated textual content, as they are more likely to trigger strong emotions than simple text, and are less likely to be critically assessed before being 'consumed'. It is also worth noting, that – according to Nemr and Gangware (2019) - detecting altered photos and videos at scale is difficult, and rapidly advancing AI and deep learning technology is making synthetic media (manipulated or artificially-created video and audio content) easier to produce. As AI technology progresses, synthetic video and audio will appear increasingly authentic to the public and will become significantly easier to manufacture. This will lead to the migration of disinformation content from being largely "static" (memes, fake articles) to "dynamic" (video and audio). For example, the video mapping of one person's face onto another, (a "deep fake") is already widely available through public apps. Video to video synthesis technology can create realistically looking artificial video content based on a set of inputs.

Taking into account that the evolving and emerging cyber-threats (including deep fake technologies) are progressing at an unprecedented pace, the law-enforcement agencies and intelligence services must consider the possibility that the AI-enabled disinformation vectors (utilizing Machine Learning, Deep Learning and Reinforcement Learning techniques) might be used even during the current COVID-19 pandemic.

There is no universally accepted policy regarding the potential legal regulations of the AI-enabled disinformation, but there is a need for the empirically-based and widely consulted (with legal experts, law-enforcement practitioners, Subject Matter Experts and the representatives of the IT industry and Artificial Intelligence developers) de lege ferenda strategy addressing these issues. On the other hand, there is in fact the report providing the contextual analysis of the use of Artificial Intelligence to limit the spread of disinformation online: the European Parliament study authored by Marsden and Meyer (2019) titled "Regulating Disinformation with Artificial Intelligence", which questions some aspects of the use of the technology, as it might interfere with the freedom of speech and might result in AI-generated censorship, if used without strong human review and appeal processes.

In my opinion, substantiated by over a decade of study of the developments of both cyber-enabled crime and terrorism, and the Artificial Intelligence technologies, the readily available IT tools, as well as the emerging technologies are a double-edged sword which can be used by both sides of the conflict: the perpetrators of crimes and terrorists on the one side, and representatives of law enforcement and intelligence services on the other. Both sides compete for domination on the "Internet Battlefield" (Gradon 2013), and the law enforcement techniques, tactics, strategies, and method-

ologies must take advantage of the available technology (including Artificial Intelligence) in order to proactively address the present and upcoming threats. Naturally, such approach has to involve handling issues of civil liberties, privacy laws, and personal rights and freedoms with utmost care. The philosophical and legal conflict of two basic rights protected by law— to privacy and to safety—must be balanced and addressed as well. Marsden and Meyer (2019) state that automated technologies are limited in their accuracy, especially for expression where cultural or contextual cues are necessary. Although I agree that this could be a serious impediment in precise detection of disinformation campaigns and fake news, I believe that the rapid developments in Artificial Intelligence and Deep & Reinforcement Learning technologies would soon overcome such limitations. Close collaboration of all stakeholders, including AI industry, legislators, policy-makers, academia, Subject Matter Experts and end-users (law-enforcement and security practitioners) would allow for the design and secure implementation of tools that would enable the enhanced detection of disinformation, while maintaining civil liberties and human rights. It is necessitated by the societal costs arising from the fake news propagation (as illustrated by the consequences of disinformation spread during the on-going coronavirus pandemic).

FACT-CHECKING AND COUNTER-NARRATIVES

It is still too early to provide the thorough analysis of the disinformation campaigns connected to the new coronavirus pandemic, as the situation develops rapidly and we learn about the new forms and avenues of fake news daily. There are numerous well-established fact-checking organizations devoted to finding, investigating and de-bunking fake news distributed in the on-line environment. Some of these organizations belong to the International Fact-Checking Network (IFCN), a unit of the Poynter Institute dedicated to bringing together fact-checkers worldwide. IFCN currently runs a website dedicated to the COVID-19 pandemic (https://www.poynter.org/covid-19-poynter-resources) including the database of over (at the time of writing) 1500 fact-checks from more than 60 countries in 15 languages (Poynter 2020). Other notable examples include Agence France Presse Fact Check website (https://sprawdzam.afp.com) available in several languages (AFP 2020) and Snopes Fact Checking website (https://www.snopes.com/collections/new-coronavirus-collection) offering its services since 1994 (Snopes 2020). It is beyond the scope of this Paper to provide the selection of case studies of fake news that are currently distributed on-line in connection with the COVID-19 pandemic, but the aforementioned fact-checking organizations offer a comprehensive and constantly updated listings of such cases, covering fake news related to the coronavirus origins and spread, prevention and treatment, national and international response, conspiracy theories and predictions, memes and misinformation, viral videos, business, industry and entertainment-related fakes associated with the current pandemic.

The fact-checking websites mentioned above and the proper information campaigns offering the clear, fact-based information and counter-narratives supported by the well-established institutions such as national health services, national and inter-

national Police agencies and reputable organizations such as the World Health Organization and the Centers for Disease Control and Prevention, are crucial to mitigate the devastating effects of the fake news propagation.

FAR-REACHING CONSEQUENCES

What are the consequences of disinformation campaigns on the general public? The immediate effect that the fake news propagation has on the society affected (especially in such extreme circumstances like the one we experience now, during the COVID-19 pandemic) is the disruption of social fabric and trust, by increasing the feelings and emotions of fear, anxiety, uncertainty and anger. Unfortunately, as Nemr and Gangware (2019) observe, the same emotions are the very characteristics that increase the likelihood a fake news message will go viral. They stress, that even when disinformation first appears on marginal sites outside of the mainstream media, mass coordinated action that takes advantage of platform business models dependent upon clicks and views helps ensure greater audience dissemination. Bot networks (set up to facilitate the amplified spread of disinformation) comprising of fake profiles intensify the message and create the impression of high activity and popularity across multiple platforms and rating algorithms.

Widespread distribution of fake news has also a significant impact on the law-enforcement and security communities and the first responders, as they need to move some of their personnel to communications and counter-narrative duties, de-bunking and demystifying the disinformation. More importantly, they have to waste their valuable resources on mitigating the effects that the fake news brings to the physical world. The panic and unrest arising from not only from the pandemic itself, but also from some of the outcomes of disinformation, misinformation and malinformation - as defined by Wardle (2018) - may cause the real consequences necessitating the use of Police force. The examples include: the increased disturbance of public order during the waves of panic-buying; physical attacks on people – as in the case reported by the BBC (2020) where the Ukrainian protesters attacked buses carrying China evacuees (according to Ukraine's security service (SBU), a fake e-mail claiming to be from the Health Ministry falsely said some evacuees had contracted the virus); a rise in cybercrime illustrated by the 350% rise in phishing attacks between the beginning of January and the end of March 2020 – the reason for that being the COVID-19 outbreak has greatly increased the usage and reliance on the Internet, giving hackers more opportunities to scam people with malware and phishing attacks (PC Magazine 2020); store looting – where in Mexico, the criminals robbed stores that were closed and posted calls on social media for people to ransack businesses (Reuters 2020). Such forms of crime and disorders are of course not new and they existed long before the COVID-19 crisis, but it is essential to stress that the law-enforcement resources are limited and must be allocated properly, according to the most crucial needs related to the strategies implemented in order to contain the pandemic.

THE CRIMES THEY ARE A-CHANGIN'

It is important to note, that disinformation and fake news distribution are not the only forms of cyber-enabled crime that take advantage of the pandemic-related crisis. Criminal offenders adapt to change and as Tilley (2015:151) notes, in the complex world of policing, change and adaptation are chronic: the law changes, communities change, the organizational arrangements for policing change, technologies change and offenders adapt and learn from one another. It is true now, when the fear, panic and unrest make wide segments of the society especially vulnerable to exploitation and attacks. The EUROPOL (2020) stresses that criminals have quickly seized the opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities. The Interpol (2020) warns that offenders see the virus outbreak as an opportunity to increase or diversify their activities.

According to the information campaigns prepared by both agencies (EUROPOL 2020 and Interpol 2020), offenders abuse the demand people have for information and supplies, by using the coronavirus crisis to carry out social engineering attacks (in the form of phishing emails), distributing malware and executing ransomware attacks. According to the UK National Fraud & Cyber Crime Reporting Centre (Action Fraud 2020), there have been 105 on-line fraud reports (related to the COVID-19 scams) to Action Fraud between 9 February 2020 and 18 March 2020, with total losses reaching nearly 970,000 British Pounds. The first report relating to Coronavirus, or COVID-19, was received on 9 February. There were 20 more reports that month. Since then, there have been 46 reports between the 1 March and 13 March, and 38 reports in just four days (14 March – 18 March).

EUROPOL (2020) also informs about the increased online activity of sexual predators who exploit children whom they expect to be more vulnerable due to isolation, less supervision and greater online exposure. Interpol stresses the increase in online fraud and sales of fake or counterfeit medical items such as surgical masks, hand sanitizers, antiviral medication and vaccines and fake COVID-19 test kits. Both agencies (EUROPOL 2020 and Interpol 2020) mention the modus operandi leveraging the coronavirus crisis in the classic "grandson" or "nephew" scam, where caller who pretends to be a relative currently being treated at hospital contacts the elderly by phone, asking to pay for the cost of the medical treatment by transferring money or by paying cash to fake public health representatives.

France24 news network (France24 2020) reports that Italian organized crime groups such as Cosa Nostra, 'Ndrangheta in Calabria and Camorra are carefully planning ahead to when the economy will start to be rebuilt, so that they could be prepared to take advantage of the business opportunities in several sectors of the industry, where they already invested, such as cleaning, disinfection, waste recycling, transportation, funeral homes, oil and food distribution. Furthermore, France24 stresses that the redirection of police resources over the crisis could also contribute to the mafia blossoming, as officers already weighed down by new roles may have to face public order problems, such as potential riots in southern Italy - fomented by organized crime groups - should the virus epicenter move from North to South. France24 informs that

the organized crime groups were allegedly believed to have orchestrated revolts in jails across the country early on in the epidemic, with prisoners fearful of catching the disease in overcrowded facilities demanding early release. Over 2,500 prisoners had been released since February 29 to ease overcrowding. (France24 2020).

The EUROPOL (2020) also draws the attention to the fact that with the increased remote work using the unprotected or under-protected access to company systems, there is a much higher possibility of cyber attacks on business and institutions, including the critical infrastructure. According to the ZDNet business technology website (ZDNet 2020), the Brno University Hospital (one of the Czech Republic's biggest COVID-19 testing laboratories) in the city of Brno, was targeted by the cyber attack during the COVID-19 outbreak. "The hospital was forced to shut down its entire IT network during the incident, and two of the hospital's other branches, the Children's Hospital and the Maternity Hospital, were also impacted" ZDNet reported. Critical national infrastructure (industries such as healthcare, energy systems and power grids, telecommunications, emergency services, finance systems, food supply, water treatment, transport, chemical and nuclear industries) are high-profile targets for coordinated attacks. As Weed (2017) notes, the key aspects of critical national infrastructure issues in cyberspace are the industrial control system (ICS) and supervisory control and data acquisition (SCADA) systems, and the primary causes of ICS and SCADA vulnerabilities fall into three general categories: insecure design, the human element, and configuration issues. As the attack on the Brno hospital indicates, there is a possibility, that cyber criminals (representing terrorist organizations, rogue governments or other state actors) might seize the opportunity that EUROPOL (2020) mentioned and leverage the COVID-19 crisis to exploit system vulnerabilities, especially by using various forms of social engineering, phishing or malware attacks on critical infrastructure employees working from home on inadequately protected computer systems.

CONCLUSIONS

Taking into account the rapidly developing situation (while this Paper has been a work in progress, that is between March 24th and March 31st 2020, the number of total confirmed cases of COVID-19 has risen worldwide from 418 thousand to over 840 thousand cases and the number of fatalities – in the same period – from less than 19 thousand to almost 42 thousand deaths, according to Center for Systems Science and Engineering at Johns Hopkins University (CSSE 2020)), it is difficult to provide a detailed analysis of trends in crime linked to the anxiety, unrest and chaos resulting from the coronavirus pandemic. The sheer pace of the events limits all research dealing with such dynamically evolving problem. The main objective of this Paper was to offer the overview of the potential threats arising from the abuse of modern Information Technologies and to raise the awareness and understanding of the ongoing and upcoming trends that the law-enforcement community and the general public would have to deal with in the near future. The Author hopes that the practitioners and stakeholders would benefit from this research by receiving the most up-to-date, preliminary threat assessment, allowing them to design strategies oriented on pre-

vention and mitigation of the negative consequences brought by the evolution and application of the known types of crime, terrorism and disorder to the new criminal landscape arising from the COVID-19 pandemic. The aim of this Paper is also to educate the general public about the vectors and strategies that disinformation, fake news propagation and cyber-enabled crime take, as being able to recognize and understand the threat is the major, most important step to render the malicious strategies used by the criminals useless.

FUNDING: This research received no external funding.

CONFLICT OF INTEREST: The author declares no conflict of interest.

ACKNOWLEDGEMENTS: The Author would like to acknowledge the support and encouragement that he received throughout his years of research on cyber-enabled crime and terrorism from: University of Warsaw (Faculty of Law & Administration and the Centre for Forensic Sciences), University College London (Department of Security and Crime Science), University of Colorado Boulder (Center for the Study and Prevention of Violence) and the Polish-U.S. Fulbright Commission. He also wishes to thank his Family for their patience and understanding.

REFERENCES

Action Fraud. 2020. "Coronavirus-related fraud reports increase by 400% in March." UK National Fraud & Cyber Crime Reporting Centre. Retrieved March 27, 2020 (https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march).

AFP. 2020. "Dezinformacja o Koronawirusie." Agence France Presse (in Polish). Retrieved March 31, 2020 (https://sprawdzam.afp.com/dezinformacja-o-koronawirusie).

Avast Security News Team. 2020. "EU Doc claims Russia spread COVID-19 disinfo to cause panic." Retrieved March 23, 2020 (https://blog.avast.com/eu-doc-warns-of-russian-COVID-19-disinfo-campaign-avast).

BBC. 2020. "21 February 2020. Coronavirus: Ukraine protesters attack buses carrying China evacuees." Retrieved March 27, 2020 (https://www.bbc.com/news/world-europe-51581805).

Bleeping Computer. 2020. "Nation-Backed Hackers Spread Crimson RAT via Coronavirus Phishing." Retrieved: March 26, 2020 (https://www.bleepingcomputer.com/news/security/nation-backed-hackers-spread-crimson-rat-via-coronavirus-phishing/).

Broniatowski, David A. et al. 2018. "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate." *American Journal of Public Health* 108(10): 1378-1384. https://doi.org/10.2105/AJPH.2018.304567

Coats, Daniel R. 2019. "Worldwide Threat Assessment of the U.S. Intelligence Com-

munity." Washington D.C., USA: Office of the Director of National Intelligence.
CSSE. 2020. "Coronavirus COVID-19 Global Cases." Center for Systems Science and Engineering at Johns Hopkins University. Retrieved March 31, 2020 (https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6).
Deutsche Welle. 2020. "Is Russia running a coronavirus disinformation campaign?" Retrieved March 27, 2020 (https://www.dw.com/en/is-russia-running-a-coronavirus-disinformation-campaign/a-52864106).
Diplomat. 2020. "Why China's COVID-19 Disinformation Campaign Isn't Working in Taiwan." Retrieved Mach 25, 2020 (https://thediplomat.com/2020/03/why-chinas-COVID-19-disinformation-campaign-isnt-working-in-taiwan/).
Emmott, Robin. 2020. "Russia deploying coronavirus disinformation to sow panic in West, EU document says." Reuters World News. Retrieved March 28, 2020 (https://www.reuters.com/article/us-health-coronavirus-disinformation/russia-deploying-coronavirus-disinformation-to-sow-panic-in-west-eu-document-says-idUSKBN21518F).
EUCPN – European Crime Prevention Network. 2015. "Cybercrime: a theoretical overview of the growing digital threat." *EUCPN Theoretical Paper Series*. Brussels, Belgium: EUCPN Secretariat.
EPTT European Parliament Think Tank. 2019. "Cyber: how big is the threat?" Brussels, Belgium: EPTT.
European Parliament. 2019. "Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States." Brussels, Belgium: Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union.
EUROPOL. 2019. "Do Criminals Dream of Electric Sheep? How technology shapes the future of crime and law-enforcement." The Hague, The Netherlands: European Union Agency for Law Enforcement Cooperation.
EUROPOL. 2019a. "IOCTA. Internet Organized Crime Threat Assessment." The Hague, The Netherlands: European Union Agency for Law Enforcement Cooperation.
EUROPOL. 2020. "Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis." The Hague, The Netherlands: European Union Agency for Law Enforcement Cooperation.
France24. 2020. "29 March 2020. "Mafia primed to feast on Italy's virus devastation." Retrieved March 29, 2020 (https://www.france24.com/en/20200329-mafia-primed-to-feast-on-italy-s-virus-devastation).
Government Office of Science. 2011. *Blackett Review of High Impact Low Probability Risks*. London, England: Department for Business, Innovation and Skills.
GPMB. 2019. "A World at Risk. Annual report on global preparedness for health emergencies." Geneva, Switzerland: Global Preparedness Monitoring Board and World Health Organization.
Gradon, Kacper. 2013. "Crime Science and the Internet Battlefield. Securing the Analog World from Digital Crime." *IEEE Security & Privacy Magazine* 11(5): 93-95.
Guardian. 2020. "Russian media 'spreading COVID-19 disinformation'." Retrieved

March 27, 2020 (https://www.theguardian.com/world/2020/mar/18/russian-media-spreading-COVID-19-disinformation).

Interpol. 2020. "COVID-19 Pandemic. Guidelines for Law Enforcement." Lyon, France: International Criminal Police Organization.

Lee, Bernice, Felix Preston and Gemma Green. 2012. "Preparing for High-impact, Low-probability Events. Lessons from Eyjafjallajökull. A Chatham House Report." London, England: The Royal Institute of International Affairs.

Marsden, Chris and Trisha Meyer. 2019. "Regulating Disinformation with Artificial Intelligence." Brussels, Belgium: European Parliamentary Research Service – Scientific Foresight Unit.

Nemr, Christina and William Gangware. 2019. *Weapons of Mass Distraction. Foreign State-Sponsored Disinformation in the Digital Age*. Washington D.C., USA: Park Advisors.

New York Times. 2020. "As Virus Spreads, China and Russia See Openings for Disinformation." Retrieved March 28, 2020 (https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html).

OECD. 2020. "New OECD Outlook on a Global Economy." The Organisation for Economic Co-operation and Development Report. Retrieved March 31, 2020 (https://www.oecd.org/coronavirus/en/).

PC Magazine. 2020. "March 30 2020. Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine." Retrieved March 31, 2020 (https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine).

Poynter Institute. 2020. "Fighting the Infodemic: The #CoronaVirusFacts Alliance." Retrieved March 31, 2020 (https://www.poynter.org/coronavirusfactsalliance/).

Reuters World News. 2020. "March 26, 2020. Mexicans fear looting spree as shops robbed, online messages incite theft." Retrieved March 30, 2020 (https://www.reuters.com/article/us-health-coronavirus-mexico-crime/mexicans-fear-looting-spree-as-shops-robbed-online-messages-incite-theft-idUSKBN21D056).

Snopes. 2020. "The Coronavirus Collection. Fact Checking COVID-19." Retrieved March 31, 2020 (https://www.snopes.com/collections/new-coronavirus-collection/).

Taleb, Nassim N. 2010. *The Black Swan. The Impact of the Highly Improbable*. London, England: Penguin Books.

Tilley, Nick. 2015. "There is nothing as practical as a good theory: Teacher-learner relationships in applied research for policing." Pp. 141-153 in *Applied Police Research: Challenges and opportunities*, edited by E. Cockbain and J. Knutsson. Oxon, England: Routledge.

UK Parliament. 2019. "Research for Parliament – Preparing for the Changing World." London, England: POST (the Parliamentary Office of Science and Technology).

UNODC. 2011. "Criminal Intelligence. Manual for Analysts." United Nations Office for Drug and Crime. Vienna, Austria: United Nations Publications.

U.S. Department of Homeland Security. 2018. "Countering False Information on Social Media in Disasters and Emergencies. Social Media Working Group for Emergency Services and Disaster Management Report." Washington D.C., USA: DHS Science

and Technology.
U.S. Department of Homeland Security. 2019. "Combatting Targeted Disinformation Campaigns. A Whole-Of-Society Issue." Washington D.C., USA: DHS Analytic Exchange Program.
U.S. Department of State. 2020. "Special Briefing on Disinformation and Propaganda Related to COVID-19." Washington D.C., USA: USDS.
Wardle, Claire. 2018. "Information Disorder: The Essential Glossary." Harvard, MA: Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School.
Weed, Scott A. 2017. "US Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure." Maxwell Air For Base, AL, USA: Air University Press.
ZDNet. 2020. "March 13, 2020. Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak." Retrieved March 25, 2020 (https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/).

BIOGRAPHICAL NOTE

Kacper Gradon is an Associate Professor at the Faculty of Law and Director of the Centre for Forensic Sciences at the University of Warsaw (Poland). He is also the UCL Honorary Senior Research Associate at the Department of Security and Crime Science and Visiting Fulbright Professor at the University of Colorado Boulder – Center for the Study and Prevention of Violence. His research expertise includes multiple homicide, criminal analysis and counter-terrorism. His current research deals with the application of Open Source Intelligence and digital & Internet forensics and analysis to forecasting and combating cyber-enabled crime and terrorism (including fake news and disinformation campaigns). He has 20 years of experience of consultancy and cooperation with Police and Intelligence services in Poland, UK, US and Canada. Graduate of the London Metropolitan Police Specialist Operations Training of Hostage Negotiations, the National Cyber-Forensics Training Alliance and the FBI "Dark Web Investigations" and the International Association of Law Enforcement Intelligence Analysts "Open Source Intelligence" courses. Lectured and held visiting professorship positions in the UK, USA, Canada, India, Australia, New Zealand, Brazil, Botswana, Japan, the Netherlands, Spain and Germany. Participated in over 200 academic and Police conferences and events worldwide. He was the UoW Primary Investigator in the 2014-2017 European Commission FP7 project PRIME (Preventing, Interdicting and Mitigating Extremist Events) dealing with lone-actor extremism and terrorism.

ARTICLE HISTORY: Received 2020-03-30 / Accepted 2020-04-05