Hedvig Szabó

Redefining Security in the Digital Age: Navigating the Evolving Landscape of AI-Induced Risks

Abstract

The emergence of Artificial Intelligence (AI) has fundamentally altered the security landscape, presenting novel challenges and opportunities. I examine the complicated relationship between AI and security, emphasising the transformative impact of AI on traditional security paradigms. It examines how malicious actors exploit AI for criminal activities, thereby escalating the complexity and severity of cybercrimes. The study highlights the evolution of cybercrime types due to AI solutions, underscoring the role of psychological manipulation and deepfake technologies in creating new avenues for deception and disinformation The emergence of the "Crime as a Service" (CaaS) model on dark web marketplaces is a testament to AI's versatility, enabling criminals to commission offenses without technical acumen. The CaaS model offers services on a subscription or pay-per-use basis, encompassing a range of activities from cybercrimes like phishing and DDoS attacks to other organised crimes. In conclusion, the paper underscores the dual nature of AI in the modern era, acting as a tool for innovation and efficiency in legal sectors, while simultaneously amplifying the capabilities of criminal enterprises, thereby challenging existing legal and security frameworks.

Keywords: Artificial Intelligence, security, Crime as a Service

DOI: https://doi.org/10.36250/01260_05

Introduction

Artificial Intelligence (AI) is a part of our everyday lives, as we encounter AI-enabled solutions in all our activities, whether at work or at play.

There is no area of society that can no longer be examined from the perspective of how AI has shaped and transformed a particular social subsystem and how it impacts on the way we live. It goes without saying that the rise of AI has not been without its impact in the field of security, to highlight just a few examples:

- we can observe the social debate that has developed around autonomous vehicles in the field of road safety
- the impact of the questions of the applicability of surveillance systems for security purposes on the exercise of fundamental rights
- how cyberattacks affect the business continuity of public and commercial actors
- whether the use of generative AI can influence the outcome of elections or be used for disinformation activities

However, the paper does not address the relationship between AI and security in general, but focuses on one segment of it, the potential for crime in the AI age to be driven by the use of AI. With regard to crime, it should be noted that the analogue world before the information society was also characterised by the fact that law enforcement detected crimes committed by criminals after the fact, i.e. law enforcement went after the criminals. Crime in general is characterised by its flexibility in responding to social change, constantly innovating and looking for ways to achieve its goals more easily and reduce the risk of being caught. This is true regardless of the technology, but technology brings additional opportunities. All subversive–emerging technologies have attracted crime at the same time as they have emerged and have immediately exploited their potential, in much the same way that the emergence of the railways has attracted the emergence of rail looters.

The aim of this paper is, on the one hand, to take stock of the impact of AI on crime, the emergence of new types of risks that can be assessed in the context of AI from a criminal law point of view and, on the other hand, to draw attention to the growing phenomenon of what is known as "crime as a service", that is to say, AI allows crimes to be committed without skills and competences, because crime can be used as a service.

Changes in crime as technology evolves

Emerging technologies in recent times – mobile phones, the internet (Miller 2009) – have provided new opportunities for criminals. With the advent of the Internet, crime has recognised these and the question is being seriously raised, as we can read in the description of David Wall's seminal work *Crime and the Internet:* "Is the Internet really powerful enough to allow a sixteen year old to become the biggest threat to world peace since Adolf Hitler?" (Wall 2001).

An intense change in crime is currently taking place, triggered by the emergence of AI in technology and then by the response of criminals. AI – but now also Information and Communications Technology (ICT) – has brought a newness that was unprecedented, which is why a 16-year-old hacker may be threatening world peace.

In November 2022, Interpol organised a forum (Interpol 2022) on the use of emerging technologies in law enforcement. Basically, how law enforcement colleagues can deal with the challenges posed by the digital world, such as new types of Web 3.0 (Waheed et al. 2023) based crime. The consensus among professionals is that there is a risk that crime will outpace law enforcement.

In 2020, Europol produced a summary on "Malicious Uses and Abuses of Artificial Intelligence", indicating that the link between AI and crime is growing. On the one hand, criminals are using AI to facilitate their own situation by "finding" new victims, making more profit in a shorter time, creating more innovative criminal models. They also have new possibilities to disguise their own activities, reducing the risk of being caught. These new opportunities bring constant changes in the world of crime that pose significant challenges for law enforcement and security in general.

Crime as a Service (CaaS)

Lately AI has become a product in its own right, available for a fee or even free of charge. On the online marketplaces, both individuals and business users have many opportunities to use different types of AI applications. Business users offer this as a service to consumers, similarly to other digitalisation solutions. This allows the user to use it and in a way that he or she needs, individually.

It can therefore be concluded that AI "as a service" model has become widespread. In reality, it is a business model, i.e. AI can be used as a service, it does not require mathematical or ICT knowledge to use it, it is available to anyone, it can be bought.

If we approach the use of AI from the perspective of legality, we can see that much of it is used for legitimate purposes within a legal framework. However, there are also ways in which those who use AI are, on the contrary, motivated by unlawful purposes, i.e. to commit crimes.

However, it is worth clarifying that AI is not itself lawful or unlawful. It is merely a tool that can be used for different purposes, and the intention and purpose of the user will determine whether the tool will serve the public good or whether it will assist in the commission of a crime.

It is now clear that the use of artificial intelligence is widespread, and that it is not only law-abiding citizens who benefit from it for legitimate purposes, but also criminal circles.

Well-organised criminal groups with substantial financial resources have many opportunities to use the latest technologies, including AI, and are increasingly doing so. In contrast, ad hoc criminals or groups that are not the best organised may not use their own technology, but may rely on services provided by others. Marketplaces have developed on the dark web, similarly to those on the surface web, where goods and services can be purchased (King et al. 2020). Among the illegal goods and services available on dark web marketplaces are criminal services: the buyer orders the crime to be committed and the seller agrees to perform it.

The crime as a service model is organised along the following principles:

- It "democratises" the commission of crime: offenders can purchase crimes, including cybercrimes, without technological knowledge, with the financial benefit falling on the offender rather than the service provider.
- The dark web is becoming more valuable: the anonymous marketplaces on the dark web provide an excellent opportunity to match and transact between the parties who want to commit the crime and those who can provide the service.
- Operating a subscription or pay-as-you-use model: similarly to the legal online economy, the crime as a service model in dark web can be operated by subscribing to the service or by paying before use, whichever is more appropriate depending on the type of crime. A constant phishing email campaign or ordering a specific DDoS attack is the goal.
- Specialisation and professionalism: the provision of crime as a service is characterised by increasing specialisation, with service providers specialising in one type of crime, not offering a full spectrum of activities, but performing that one type of crime with professionalism.

- Ease of access: the offender does not have to create the means of committing the offence and develop the method of execution himself, because these are available from the service provider, so the offence is open to anyone who wants to commit it.
- The complexity of offences can be increased: it is possible to order different offences from several service providers for a single target. This allows the victim's exposure and the success of the crime to be maximised.
- The model can be used not only in cybercrime: currently, cyberattacks in the dark web as a service are seen as the most feasible, but it can also be used for any crime that is organised online, such as money laundering, drugs and human trafficking.
- Continuously evolving business model: the CaaS model builds on the experience of legal business models, adopting best practices and successful strategies such as customer rating systems and service guarantee schemes.
- A challenge for law enforcement: cybercrime is a challenge in itself for law enforcement, due to the difficulty of detection. In case of this particular model, the modus operandi of the offence adds to the difficulty of detection.

On this basis, AI poses a significant risk as it increases the potential of offenders and may thus lead to an expansion of what Europol calls the criminal sharing economy.

Social engineering is the art of tricking users into revealing their data, which can then be used by hackers to gain access to ICT networks or user accounts. Cybercriminals exploit the fact that humans are the weakest link. Because people are basically well-intentioned and helpful, they are easily fooled and can therefore be targeted by virtually anyone (Trend Micro 2019). Hackers rely on basic human trust and the fact that users simply do not look for subtle signs of deception.

Phishing attacks are typically social engineering crimes. At present, most phishing attacks are indiscriminate and untargeted (Greco et al. 2023).

Generic messages are used which are tailored to big brands or current events, but it is expected that only a few users will fall victim to the attack. For this reason, the attacker tries to send as many digital messages as possible to make the attack worthwhile even if the response rate is low.

There is also a variant of phishing where only certain individuals are targeted, known as spear-phishing. AI has increased the effectiveness and success rate of phishing attacks by creating more authentic-looking (sometimes perfect) messages, for example by using information extracted from social networks or by spoofing the

style of a trusted partner. Rather than sending uniform messages to all targets, which in most cases are unlikely to hit the mark, AI-enabled phishing tailors messages to exploit specific vulnerabilities of individuals. This effectively automates spear-phishing.

In addition, artificial intelligence-enhanced learning could be used to discover "what works" in phishing. And by varying the details of the messages, based on the data extracted from them, it is possible to maximise profits (Leonov et al. 2021).

Deepfake is an information communication technology where a previously non-existent video recording of someone is created by converting existing image and sound files into a video recording that can be used to deceive by appearing real. Deepfake technology gained worldwide attention in 2018 with Jordan Peele's fake video of former U.S. President Obama insulting President Trump and warning of the dangers of deepfake media.

Deepfake technology has the potential to influence people, as people tend to believe what they see–hear, and take what they see–hear as real. Researchers have also shown that fake video images can induce false testimony (Granot et al. 2018). Visual evidence is vivid, activating multiple areas of the brain, which can make it very persuasive. At first, they do not even think that what they perceive is not real at all, they have difficulty determining whether a visual or audio recording is real or fake. This has the potential to fundamentally change public confidence in audio–video technology.

This loss of trust in technology is of particular importance in law enforcement, as audio and video sources (CCTV cameras, mobile phone videos, body cameras and dashboard-mounted camera images) regularly used as evidence by law enforcement agencies can determine the success of a criminal prosecution and bring a new era of evidence evaluation, where the credibility and authenticity of evidence must be proven (Dauer 2022).

Conclusion

Although we are only at the beginning of the AI era, we have already gained practical experience of the harmful, offending effects of AI, in addition to its many benefits. No technology, such as AI, is inherently dangerous, but the opportunities that its use opens up offer criminals a much wider perspective than in the pre-AI era. Crime has adapted flexibly to technology and, with the advent of AI, has begun to use it to improve its own illegal activities. The use of AI in crime first radically reshaped crimes committed in the digital space. Alongside cybercrime, the proliferation of deepfake

could fundamentally challenge the evidence system in criminal proceedings and the authenticity of image and audio recordings. The potential for AI-enabled capabilities will reinforce the proliferation of "Crime as a Service". Of course, in the offline world, there have also been crimes that were not carried out by the criminals themselves, but were commissioned as a service from specialised "experts". But first digitalisation, and then artificial intelligence has provided an additional alternative by making some of the crimes available to anyone as a service that can be bought.

It is clear that technology is also bringing a new era in crime. Crime will exploit the full potential of technological advances and new phenomena will emerge that the security sector has not yet encountered.

References

Dauer, Frederick (2022): Law Enforcement in the Era of Deepfakes. *Police Chief Magazine,* 29 June 2022. Online: www.policechiefmagazine.org/law-enforcement-era-deepfakes/

Granot, Yael – Balcetis, Emily – Feigenson, Neal – Tyler, Tom (2018): In the Eyes of the Law: Perception Versus Reality in Appraisals of Video Evidence. *Psychology, Public Policy, and Law,* 24(1), 93–104. Online: https://doi.org/10.1037/law0000137

Greco, Francesco – Desolda, Giuseppe – Esposito, Andrea (2023): *Explaining Phishing Attacks: An XAI Approach to Enhance User Awareness and Trust.* Proceedings of the Italian Conference on CyberSecurity, (ITASEC 2023), 3–5 May 2023, Bari.

Interpol (2022): Nascent Technologies Focus of INTERPOL New Technologies Forum. *Interpol,* 21 November 2022. Online: www.interpol.int/News-and-Events/News/2022/Nascent-technologies-focus-of-INTERPOL-New-Technologies-Forum

King, Thomas C. – Aggarwal, Nikita – Taddeo, Mariarosaria – Floridi, Luciano (2020): Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. *Science and Engineering Ethics,* 26(1), 89–120. Online: https://doi.org/10.1007/s11948-018-00081-0

Leonov, Pavel Y. – Zavalishina, Alexandra K. – Kotalyanets, Oksana – Vorobyev, Alexander V. – Morozov, Nikolay V. – Ezhova, Anastasia A. (2021): *The Main Social Engineering Techniques Aimed at Hacking Information Systems.* 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 13–14 May, Yekaterinburg. Online: https://doi.org/10.1109/USBEREIT51232.2021.9455031

Miller, Vincent (2009): The Internet and Everyday Life. In Jewkes, Yvonne – Yar, Majid (eds.): *Handbook of Internet Crime.* London: Willan, 67–87. Online: https://doi.org/10.4324/9781843929338

Soice, Emily H. – Rocha, Rafael – Cordova, Kimberlee – Specter, Michael – Esvelt, Kevin M. (2023): *Can Large Language Models Democratize Access to Dual-Use Biotechnology?* Online: https://doi.org/10.48550/arXiv.2306.03809

Trend Micro (2019): Cheats, Hacks, and Cyberattacks. Threats to the Esports Industry in 2019 and Beyond. *Trend Micro,* 29 October 2019. Online: www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cheats-hacks-and-cyberattacks-threats-to-the-esports-industry-in-2019-and-beyond

Waheed, Amtul – Dhupia, Bhawna – Mesfer Aldossary, Sultan (2023): Recapitulation Web 3.0: Architecture, Features and Technologies, Opportunities and Challenges. *Intelligent Automation and Soft Computing,* 37(2), 1610–1620. Online: https://doi.org/10.32604/iasc.2023.037539

Wall, David (2001): *Crime and the Internet. Cybercrimes and Cyberfears.* London: Routledge. Online: https://doi.org/10.4324/9780203299180