Can AI be Evil: The Criminal Capacities of ANI

Željko Bjelajac[1]*, Aleksandar M. Filipović[2], Lazar Stošić[3]

[1]University Business Academy, Faculty of Law for Commerce and Judiciary, Republic of Serbia,
e-mail: zdjbjelajac@gmail.com
[2]University of Business Academy, Faculty of Economics and Engineering Management, Novi Sad, Serbia
e-mail: sasha.filipovic@gmail.com
[3]Union Nikola Tesla, Belgrade, Faculty of Management, Sremski Karlovci, Serbia, e-mail: lazar.stosic@famns.edu.rs

Abstract: Artificial Narrow Intelligence (ANI) represents a captivating domain within technological advancement, bearing the potential for profound societal transformations. While ANI holds the promise of enhancing various facets of human existence, it concurrently engenders inquiries into its "darker aspects." This study delves into the challenges associated with ANI's conceivable manifestation of harm and injustice, a phenomenon devoid of consciousness, intention, or responsibility akin to that of human entities. A pivotal dimension of ANI's "dark side" pertains to its susceptibility to malevolent utilization. Despite its lack of awareness, ANI serves as a tool for malicious endeavors, encompassing the propagation of disinformation, compromise of security systems, and consequential decision-making. This prompts contemplation on strategies to mitigate these "precise manifestations of malevolence" arising from ANI's technological progression. Additionally, ANI's development introduces profound ethical quandaries. Ensuring ANI's alignment with moral principles while averting scenarios in which it generates decisions conflicting with human morality becomes a pressing concern. This research underscores the imperative for rigorous regulatory frameworks and ethical directives to curtail potential hazards and unscrupulous utilization of ANI. The fundamental objective of this investigation is to advocate for the responsible deployment of ANI in society. A comprehensive understanding of potential risks, complemented by meticulous consideration of ethical dimensions, emerges as an indispensable prerequisite to harmonizing technological advancement with safeguarding societal and individual interests.
Keywords: Artificial narrow intelligence, evil, crime, ethics.

Introduction

People fear the unknown, everything they cannot comprehend, predict, or control, especially phenomena beyond their volition. This psychological framework can be applied to the question of 'Can AI be evil?' We fear this question because most people lack a deep understanding of artificial intelligence, shaping their perception of AI based on depictions in movies and literature. They often believe that such dystopian AI scenarios could become our future. What people may not realize is that what's commonly depicted in most films represents AI superior to humans in every aspect, called 'Artificial General Intelligence' or 'AGI,' but its full implementation isn't expected by scientists before the end of this century (Ford, 2018). This has led us to contemplate the aspects of the dark side of artificial intelligence, which we have 'in flagrante,' preceding AGI, especially ASI, referred to by scientists as ANI.

Science currently operates with three levels of artificial intelligence in theory: Artificial Narrow Intelligence or ANI, Artificial General Intelligence or AGI, and Artificial Super Intelligence or ASI. (IBM Data and AI Team, 2023; Price, Walker and Wiley, n.d). ANI is considered 'weak' AI, while the other two forms are classified as 'strong' AI. Weak artificial intelligence is defined by its ability to perform specific tasks, such as regulating air traffic, driving a car, or identifying a particular person. Some examples of ANI usage include natural language processing, computer vision, advancements in human medical treatments, task automation, and support for chatbots and virtual assistants.

Stronger or higher forms of AI, like AGI and ASI, involve replicating and simulating human thinking and behavior. Strong AI is defined by its ability to successfully mimic or surpass cognitive concepts

---

*Corresponding author: zdjbjelajac@gmail.com

and capabilities of the human brain. The pinnacle of AGI would be equivalence with human intellectual capacity, while artificial superintelligence (ASI) would significantly surpass human intelligence and the cognitive abilities of the human brain. Research in this field is ongoing, but no known form of strong artificial intelligence currently exists. Artificial intelligence is emerging as the predominant driving factor of the current era. ANI is becoming the central player in various sectors of life. Progress promises innovations that will improve healthcare, education, trade, industry, and many other fields. However, along with undeniable progress, which remains largely in the realm of predictions, the proliferation of ANI poses an ominous threat of unknown provenance, intention, and form, as humanity increasingly relies on AI. The omnipresence of ANI brings forth a series of profound ethical and legal questions and dilemmas that require careful consideration and the establishment of responsible frameworks.

One of the central philosophical questions in the context of the ontological aspects of AI technology is, 'Can artificial intelligence be evil?' The concept of 'evil' is traditionally associated with the intent of conscious beings to inflict pain, harm, or injustice on other conscious beings. It is presumed that higher forms of artificial intelligence (AGI and ASI) might or should have consciousness and free ontological existence, allowing them to choose evil as a form of behavior. However, concerning artificial narrow intelligence (ANI), the ontological paradigm of this noumenon excludes consciousness and intent, shedding light on this matter in a different way. ANI is a product of human engineering and represents a collection of algorithms and data that enable machines to autonomously perform tasks that typically require human intelligence. This technology can cause harm, and it can exhibit activities and qualities reminiscent of malevolence that we would attribute to conscious beings. The question that arises is how to interpret and understand the negative consequences and whether, in the context of actions by artificial intelligence, we can classify them as 'evil'."

Moral Evil in the Behavior of Artificial Narrow Intelligence (ANI)

An essential dialectical opposition exists between the ontological concepts of humans and artificial intelligence. Humans, upon gaining consciousness and reason, became free beings, possessing free will that grants them the right and the ability to choose evil as a way of life. Human beings acquired their freedom through hubris, a just rebellion against the cosmic or divine order. They survived this rebellion but ceased to be ethically and mentally perfect, striving now to create an artificial copy of themselves (AI) that would be devoid of the imperfect attributes of humans—a replication of humans before committing the original sin. Can humans, inherently free but mentally imperfect and ethically fragile, create a perfect artificial intelligence? To what extent are humans capable of, while crafting various forms of artificial intelligence, avoiding the implementation of their own limitations and the 'dark side' of their personalities in AI, even if only in ANI? This is also an epistemological question. When an AI entity reaches singularity, it will learn from the people around it (see more: Bostrom, 2014). What will an AI entity learn from observing human interactions and behaviors? The answer must be rather grim and dystopian.

ANI lacks consciousness, intent, or the moral capacity of conscious beings, necessitating a different approach. When we contemplate 'evil' in the context of ANI, we must exclude the copying of logical and legal postulates of theories and practices related to human behavior, particularly the reasons for 'culpability exclusion' in humans who have committed a criminal act. With ANI, our focus should be on the negative consequences, harm done, and the risks posed by this technology. From the perspective of the ethics of the human community, the ethical characteristics of AI entities present a kind of ethical dilemma. The concept of 'evil,' in the sense of an ethical, civilizational, normative category of human life, is regarded as 'intentionally and consciously inflicting pain on a conscious being' (Rasel, 1982). The fact that ANI has no intent to cause harm, nor any consciousness to do anything wrong to anyone or anything, cannot be a reason for excluding ANI's culpability. Hence, among experts in ANI, concerns are growing that ANI could engage in activities that people perceive as causing severe harm. This is particularly relevant in the context of potential misuse of ANI for military purposes. ANI can be integrated into weapon systems to enable autonomous tracking, targeting, and attacking of human targets. The technology of 'autonomous weapon systems' controlled by ANI can be misused to target civilian objects or innocent people. ANI can be used to generate false information, videos, and texts to spread misinformation and propaganda for the purpose of destabilizing opponents. It can be used for mass surveillance of citizens' communications and movements, jeopardizing privacy and civil liberties. It can be used to conduct sophisticated cyberattacks, including attacks on critical infrastructure, military systems, or communication networks. ANI can manifest 'evil' through bias and discrimination in its decisions. ANI algorithms created on unfair or biased data can result in injustice and harm with very severe consequences. The automation brought by ANI can result in job losses and changes in the labor market, which unemployed individuals may perceive as evil.

People may strive to create AI that functions as close to perfection as possible, but complete perfection is unattainable for humans. The reasons for this are multiple and are based on: (1) Inherent human constraints, preventing the creation of flawless artificial intelligence due to limitations in human knowledge and capabilities; (2) Flaws in decision-making arising from human biases and imperfections, where personal experiences, prejudices, and values can introduce errors in the development of artificial intelligence; (3) The ever-changing nature of technology, which continually evolves and renders today's notion of 'perfection' in artificial intelligence outdated in the future; (4) Ethical considerations, as the definition of AI perfection may hinge on ethical and moral values, adding a subjective dimension to the concept. What is 'perfect' for one person or group may be unacceptable for another. Instead of pursuing complete perfection, a better approach to AI development may be to create systems that are highly efficient, safe, transparent, scalable, and capable of learning and adapting.

Establishing the Culpability of Artificial Narrow Intelligence (ANI)

Culpability is a crucial element in the consideration of criminal offenses and is based on the internal state of mind and intentions of the entity or person suspected of committing a crime. In many legal systems, culpability is examined beforehand to either establish or exclude the responsibility of the accused for the commission of the offense.

Given that Artificial Narrow Intelligence (ANI) is a product of a material nature, it is, according to Heidegger's views, an 'entity,' it 'is,' and thus represents an entity with its ontological being (see more: Hajdeger, 2000). However, ANI lacks consciousness, free will, or the ability to possess logos that would enable it to differentiate between right and wrong and good and bad. This ability to distinguish relies on the power of reason and cognition. Since ANI lacks consciousness and reason, it cannot possess 'intent' as a crucial condition for the existence of the 'guilty party' in humans. When the possibility of ANI's culpability is compared to the possibility of human culpability, the notion of culpability, as a possible psychological or subjective element of ANI's criminal offense, operates differently. ANI is developed to perform specific tasks, basing its decisions and actions on algorithms, data, and programming provided by its creators. During the execution of tasks, ANI cannot comprehend moral and ethical concepts in the way that the human mind does.

Legal regulation of new phenomena always poses challenges for lawmakers, regardless of the branch of law. At this stage of societal development, problematic questions arise in the fields of artificial intelligence, ICT, robotics, and more. Scientific and technological progress brings not only benefits but also new dangers to humanity. The use of robots, non-biological neural networks, and artificial intelligence in everyday life was, until recently, perceived as something brilliant, unattainable, existing only in the pages of books. Neural networks are actively employed in various fields of applied science, and literature describes positive examples of the use of autonomous devices in medicine (Hamet and Tremblay, 2017).

ANI has long been causing harm to individuals and human communities, and someone should be held accountable for that harm under the law. However, current legal regulations do not include elements of criminal offenses related to socially dangerous acts committed using artificial narrow intelligence (ANI). Laws generally do not recognize ANI as a perpetrator of a criminal offense or a subject of criminal liability. ANI is now capable of fully executing the objective side of a range of criminal offenses stipulated by criminal law, and this range will expand in the future. Scientific papers demonstrate that ANI activities can pose a public danger and harm all subjects protected by criminal and other legislation (Mosechkin, 2019). Since ANI seeks to replicate human behavior and conduct, the substance of ANI's guilt resembles the content of intellectual and volitional elements of human activity. It is argued that artificial intelligence cannot be an independent subject of a criminal offense unless it is recognized as a personality (Mosechkin, 2019). This is supported by the view that ANI 'can function in ways that are far from what program creators could have foreseen. To be sure, we might be able to say what the comprehensive goal of artificial intelligence was, but ANI may do things in ways that the creators of artificial intelligence may not understand or cannot anticipate' (Bathaee, 2018).

Criminal Potential of the Dark Side of ANI

Dark artificial intelligence is a general term encompassing any malicious and malevolent acts that autonomous ANI systems can perform with the appropriate malicious inputs and evil, even criminal, intentions of the architects or creators of ANI algorithms (biased data, unverified algorithms, etc.). The range of possible scenarios for the criminal use of dark artificial intelligence is vast and incredible, ranging from economic fraud and privacy violations to severe forms of war crimes, including murders and the

extermination of parts of the human community, be it 'hostile' nations or ethnic or racial groups within one's own country. For example, money laundering, a very complex criminal offense that typically requires a serious and organized criminal group (Bjelajac, 2011a), is something that AI can do in a fraction of a second if instructed to do so. Modern technological systems used in financial transactions have significantly eased the process of money laundering (see more: Bjelajac, 2011b), but when you add the computational and analytical capabilities that AI possesses, it paints a very worrisome picture, and that is only one form of criminal activity. Research papers differentiate direct and indirect criminal risks associated with the use of ANI (see more: Begishev and Khisamova, 2018).

Scenarios of malicious activities of the dark side of ANI have the potential to become a reality given existing malicious ANI applications, such as 'smart dust' and drones, facial recognition and surveillance, fake news and bots, as well as the eavesdropping of smart devices (Minevich, 2020). Drones and armies of smart dust can collaborate to destroy energy grids and smart infrastructure systems. Facial recognition provides autonomous systems with the ability to detect and store millions of individual characteristics, which, due to cloning and bots, can be used to create deeply compromising false images and videos. Smart home devices raise privacy invasion to unacceptable levels, as IoT (The Internet of Things) technologies serve as efficient channels for spying by domestic cybercriminals or foreign agents. Unbridled access of artificial intelligence to population surveillance will rapidly create human rights issues related to individual personality and freedom (Minevich, 2020).

Several characteristics of ANI make it desirable for criminal use (Stevens, 2023):

1. Speed and Effectiveness: AI has the capability to swiftly process vast volumes of data and perform tasks efficiently, presenting the potential to automate fraudulent activities.

2. Anonymity: AI can be harnessed to carry out deceptive actions covertly, leaving minimal to no traces.

3. Evasion of Detection: AI can generate deceptive information that is challenging to identify as false.

4. Personal Gain: Fraud frequently stems from the pursuit of financial or other advantages through deceitful means, and AI can be employed as a facilitative tool for such objectives.

5. Fabrication of False or Misleading Content: AI can be utilized to fabricate counterfeit websites, social media accounts, or other online materials with the intent of deceiving individuals. This encompasses the creation of fictitious reviews or manipulation of online ratings to mislead consumers.

6. Automation of Deception: AI can automate fraudulent or deceitful schemes, such as the mass dissemination of deceptive emails aimed at persuading individuals to disclose sensitive information or transfer money.

7. Phone Number or Email Address Spoofing: AI can generate counterfeit phone numbers or email addresses, crafted to mislead individuals into believing they are interacting with a legitimate entity.

8. Forging Counterfeit Documents: AI can be instrumental in producing spurious documents, including contracts and invoices, designed to deceive users.

9. Enhanced Attack Sophistication: AI can elevate the complexity of cyberattacks, such as the creation of more convincing phishing emails or the customization of attacks targeting specific organizations (see more: Stevens, 2023).

Criminal Models

We differentiate criminal offenses related to Artificial Narrow Intelligence (ANI) based on the level of danger and the extent of harm that malicious or "dark" ANI can inflict. This shifts the current paradigm of risks associated with ANI and brings the most extreme and damaging forms of ANI closer to existential threats (see more: Bjelajac, Filipović and Stošić, 2022), a realm that was until recently reserved for more advanced forms of artificial intelligence, such as Artificial General Intelligence (AGI) and Artificial Superintelligence (ASI).

At the forefront is the use of ANI for military purposes (Price, Walker and Wiley, n.d). Overreliance on machine learning algorithms that we employ to obtain better and quicker responses can swiftly lead to catastrophic outcomes. "One concerning example of excessive dependence on ANI arises in the context of war when artificial intelligence is enabled to autonomously decide whom to kill or when to engage a nuclear bomber, without human knowledge. A less alarming scenario arises when an autonomous ANI system determines whom to hire or fire. Relying on artificial intelligence to solve existential questions means the elimination of crucial human inputs from key decision-making processes, which can swiftly lead to disaster and provoke concerns about the redundancy of humans in general. To mitigate this dark side of AI, we must establish a legal imperative that requires humans to have the final say in any outcome-

seeking process" (Minevich, 2020).

History teaches us that the military and criminals are typically the first to embrace all fatal technologies, while other state and societal actors tend to react more slowly (Ovchinskiy, 2022). The military initially recognized the role of "smart dust" by firmly embracing this technology in an attempt to manipulate the will of citizens through the manufacturing of consciousness. The study of this technology commenced as a spin-off of Project RAND, involving collaboration between the Douglas Aircraft Company and the United States Air Force. Subsequently, DARPA (the Defense Advanced Research Projects Agency), a research and development organization under the jurisdiction of the United States Department of Defense, tasked with the development of cutting-edge technologies for military applications assumed a leading role (Bjelajac and Filipović, 2019). This prioritization places the manufacturing of consciousness as a secondary risk in the hierarchy of threats to human communities. The concept of global dominance, embodied in the idea of a new world order, is designed in leading closed centers of economic and political power and is implemented through the ruthless and aggressive actions of media imperialism with a monopoly on broadcasting and the manufacturing of consciousness. A specter of media manipulation circulates the planet today, threatening to erode the society we know and the essence of the human being. By amalgamating Information and Communication Technologies (ICT) with Artificial Narrow Intelligence (ANI) systems designed for information collection, we observe a profound and irremediable deterioration and disintegration of the modern societal fabric.

Theorists argue that "this represents a new power above the power of citizens to recognize and understand this force" (Encensberger, 1980). ICT and smart dust permeate society, filling gaps, sowing unrest, convincingly promising solutions, and order. "This new power is incorporated into journalism, fashion, religious teachings, tourism, the education system... However, while the new technical instruments are fervently discussed in isolation, the consciousness industry as a whole remains outside the visible spectrum. The question of who is the master and who is the servant is not decided solely based on who possesses capital, factories, and weapons but on who controls the consciousness of others." It only takes having access to ICT and ANI, sufficient financial resources, and enough time, and you can shape the opinions of thousands and millions of people (see more: Filipović, 2019).

Although, according to Gartner's research (Verma, 2020), it will take over a decade for smart dust to wreak havoc on human life, its significant technological potential already appears frightening, raising questions about privacy protection and the ethics of its application (Marr, 2018). The commercialization of smart dust will only increase the volume of data collected by microsensors. It remains uncertain what those deploying microscopic sensors will do with the data they collect. Scientists typically do not focus on security while developing such devices, and security concerns are only addressed once the technology hits the market, often too late to mitigate potential risks.

Statista provides a list of other common criminal activities that may be associated with ANI (Petrosyan, 2023), on which we will elaborate further and expand it:

1. Fraud

Fraud executed by Artificial Narrow Intelligence (ANI) represents a significant problem in the digital world. ANI can be programmed or trained for various forms of fraud that can cause harm to users, organizations, and society as a whole. A review of fraud that ANI can execute includes:

- **Phishing Attacks:** ANI can generate fake emails, websites, or social media profiles to impersonate a trusted source like a bank or a well-known company. Such phishing attacks can lead users to disclose personal or financial information.

- **Media Manipulation:** ANI can manipulate audio, video, and textual content to create false information, fake recordings, or audio clips for spreading disinformation or damaging the reputation of individuals or organizations.

- **Fake Reviews and Comments:** ANI can automatically generate fake positive or negative product, service, or content reviews on the internet, influencing consumer decisions and harming a company's reputation.

- **False Identity:** ANI can be used for identity theft, creating fake social media profiles or other platform accounts.

- **Financial Fraud:** ANI can engage in various forms of financial fraud, including impersonation related to banks, investments, or cryptocurrencies. It can also execute fraud through market manipulation and rapid algorithmic trading.

- **Intellectual Property Theft:** ANI can be employed for the theft of trade secrets, copyrights, or patents through automated analysis and copying of information.

- **Extortion:** ANI can be used for extortion against individuals or organizations through threats,

false accusations, or the disclosure of sensitive information.
- **System Compromise:** ANI can hack computer systems, servers, or networks to cause harm, steal information, or block data access.

2. Data Theft via ANI

In the digital age, data has become a valuable resource that is frequently stored, exchanged, and processed through computer systems and the Internet. Despite efforts to secure data, data theft remains a serious issue. In this context, ANI represents a sophisticated tool that can be used to execute various forms of data theft. These include:
- **Phishing Attacks:** ANI can be programmed to automatically send thousands or even millions of fake emails resembling official messages from banks, companies, or organizations. These messages may contain fake links to websites that appear authentic but are designed to collect sensitive user information such as usernames, passwords, credit card numbers, and other personal data.
- **Ransomware Attacks:** ANI can be used for the rapid and widespread distribution of ransomware, malicious software that encrypts data on a victim's computer. Subsequently, assailants demand a ransom in return for the decryption key.
- **Cryptocurrency Theft:** ANI can track cryptocurrency transactions and attempt to hack digital wallets.
- **Manipulation of Payment Systems:** ANI can be programmed to execute payment system fraud, such as false transactions or refunds that were never made.
- **Theft of Trade Secrets:** ANI can be used to monitor and steal trade secrets, which can have significant business and legal consequences.
- Impersonation: ANI can generate fake profiles on social media to access user's personal information and use it for manipulation or spreading disinformation.
- **Medical Data Theft:** ANI can be utilized for stealing sensitive medical data, including medical histories and patients' personal information.

3. Abuse of Systems and Hacking

This set of criminal activities carried out by ANI poses a threat to cybersecurity. ANI can be programmed to execute various forms of system abuse and hacking with the goal of gaining unauthorized access to information, causing damage, or extortion. These actions include:
- Unauthorized Access: ANI can be programmed to automatically breach system security barriers, such as passwords and authentication, to gain unauthorized access to computers, servers, or networks. This can allow access to sensitive data or control over the system.
- Distribution of Malware: ANI can be used for the rapid distribution of malicious software (malware) through various methods, including email, USB devices, or vulnerable network points. This malware can cause damage, data theft, or block access to resources.
- DDoS Attacks: ANI can coordinate attacks aimed at overwhelming services and servers, temporarily disabling access to websites or online services.
- Theft of Authentication Data: ANI can attempt to steal authentication data such as passwords, PINs, or digital keys to gain access to user accounts or systems.
- Manipulation and Sabotage of Systems: ANI can be programmed to alter system settings, delete data, or create chaos within a network.
- Theft of Information and Trade Secrets: ANI can continuously monitor and spy on activities within a network to steal sensitive information, including trade secrets, intellectual property, or confidential documents.
- Brute Force Attacks: ANI can execute brute force attacks by attempting all possible password combinations to gain access to accounts or systems.
- Zero-Day Vulnerabilities: ANI can be programmed to seek and exploit zero-day vulnerabilities in software applications or operating systems before manufacturers release patches.

4. Market Manipulation by ANI

ANI can be utilized for various forms of market manipulation, including:
- **Algorithmic Trading:** ANI can be programmed to rapidly and automatically make trading decisions based on market analysis and data. This process is referred to as high-frequency trading (HFT) and can be used to execute a large number of trading operations in a very short time.
- **Dissemination of Disinformation:** ANI can be employed to spread false news or disinformation through social media and websites. Such disinformation can influence investment decisions and trigger

sudden market price fluctuations.

- **Front Running:** ANI can detect the trading orders of other market participants before they are executed and quickly react to them. This enables manipulators to exploit information and secure profits or prevent losses.
- **Pump and Dump:** ANI can be programmed to manipulate the prices of stocks or cryptocurrencies by heavily promoting certain investments to attract investors and then selling those positions when the prices rise.
- **Flash Crashes:** ANI can cause sudden market price drops by mass selling of stocks or other financial instruments, creating panic among investors and market instability.
- **Scalping:** ANI can be programmed to execute a large number of small trading operations to generate profits based on small price differences.

5. Abuse of Personal Data by ANI

ANI can be programmed or used in various ways to illicitly collect, use, or distribute personal data, which can bring serious consequences for individuals and their private information. These abusive practices include:
- **Personal Data Theft:** ANI can be programmed to attempt unauthorized access to databases, cloud storage, or other sources where personal data is stored in order to steal or retrieve it.
- **Distribution of Personal Data:** ANI can automatically distribute stolen personal data over the internet or other communication channels. This data may be sold on illegal markets or used for other malicious purposes.
- **Impersonation:** ANI can be used to impersonate individuals through social media, email, or other communication platforms to gather personal information from individuals.
- **Targeted Advertising:** ANI can analyze users' personal data to create profiles and target them with personalized advertising. This may involve tracking online activity, internet browsing, and other forms of surveillance.
- **Identity Theft:** ANI can use stolen personal data to commit identity theft, open fake accounts, file fraudulent credit requests, or engage in other forms of financial fraud.
- **Creation of Fake Profiles:** ANI can automatically create fake profiles on social networking sites or other online platforms using stolen personal data to manipulate or spread disinformation.
- **Social Engineering:** ANI can use stolen personality and habit data to create convincing social engineering scenarios to deceive individuals or organizations.

6. Attacks on Infrastructure

ANI can be programmed or used for various types of attacks on infrastructure, and these attacks can have serious consequences for society and security. These attacks may include:
- **Attacks on Energy Infrastructure:** ANI can be used to target energy systems, including power grids and power plants. This can involve attacks on distribution systems, destabilizing power supply, or even disabling energy facilities.
- **Attacks on Transportation Infrastructure:** ANI can be used to target transportation networks, including traffic lights, airports, trains, and other systems. This can cause dangerous situations, delays, and disruptions in traffic.
- **Attacks on Water and Sewage Systems:** ANI can cause issues in water and sewage systems, including water supply disruptions or water contamination.
- **Attacks on Communication Infrastructure:** ANI can target communication networks, including telecommunication centers and servers. This can lead to communication out-ages or denial of internet access.
- **Attacks on Industrial Control Systems:** ANI can target Industrial Control Systems (ICS) that manage critical facilities such as chemical or nuclear power plants. This can result in production disruptions or even serious incidents.
- **Sabotage of Autonomous Vehicles:** In the context of autonomous vehicles, ANI can be used to launch attacks on autonomous driving systems, including manipulating traffic signals, taking control of autonomous vehicles, or even causing traffic accidents.

7. Traffic Incidents

Traffic incidents that can be caused by Artificial Narrow Intelligence (ANI) are particularly relevant in the context of autonomous vehicles and the use of ANI in traffic. While autonomous vehicles are developed with the aim of improving road safety, there are several ways in which ANI can lead to traffic

incidents:

- **Technical Failures:** ANI may experience technical failures or software errors that control autonomous vehicles. This can lead to unexpected situations on the road, such as sudden stops or inappropriate maneuvers.

- **Environmental Perception Errors:** ANI uses sensors such as radar, cameras, and LIDAR to gather information about the environment. Perception errors, such as misinterpreting signs or other vehicles, can lead to accidents.

- **Decision-Making Errors:** ANI makes decisions based on the analysis of environmental data. Decision-making errors can result in dangerous situations, such as miscalculations of distances or the speed of other vehicles.

- **Attacks and Hacking:** ANI vehicles can be targeted by hackers who attempt to take control of the vehicles or make them unpredictable. This can lead to serious incidents.

- **Social Engineering and Manipulation:** ANI vehicles can be exposed to social engineering or manipulation by malicious individuals who aim to cause incidents, for example, by placing obstacles on the road or creating confusion for autonomous vehicles.

- **Unforeseen Situations:** ANI may struggle to deal with unforeseen situations, such as emergencies on the road, adverse weather conditions, or other extreme circumstances.

8. Risk of Combining Different Forms of ANI

The combination of two or more forms of ANI designed to achieve individual goals can significantly increase the risk of ANI misuse and multiply the harm. Such combinations, individually harmless software, can, when combined, create a jointly orchestrated virtual system designed for malicious intent and aimed at harming people and achieving malicious or criminal objectives. Combining facial recognition software and software controlling armed drones can have significant implications and elevate the importance of addressing numerous ethical and security concerns. In November of 2017, the Future of Life Institute in California, which focuses on "ensuring that artificial intelligence benefits all of humanity," released a video depicting "slaughterbots." In the video, small (fictional) drones utilized facial recognition systems and armed drones to target and eliminate civilians (Proudfoot, 2018). The institute is partially funded by Elon Musk, who thinks that AI is potentially "more dangerous than nuclear weapons" (Piquard, 2023). The dystopian video ends with the chilling words of computer scientist Stuart Russell from Berkeley: "We have the opportunity to prevent the future you just saw," he says, "but the window for action is closing fast." The video was released in conjunction with the UN Convention on Certain Conventional Weapons in the confidence that the UN would decide to ban the development of lethal autonomous weapons (Bjelajac and Filipović, 2021). Combining dedicated forms of ANI has other malicious combinations as well. Attackers often use a combination of malware and phishing techniques to deceive users into downloading and installing malicious software on their devices. This can result in personal data theft, financial harm, and other unwanted consequences. The combination of ransomware (which encrypts data) and cryptojacking techniques (which use the user's computer resources for cryptocurrency mining) can harm individuals and organizations. Botnets are combinations of software (bots) that run on infected computers and can be used for large-scale DDoS attacks, spam distribution, or other malicious activities. Attackers may use a combination of techniques like pharming and DNS spoofing to redirect users to fake websites and steal their credentials and personal information. Even three or more independent individual forms of ANI can be integrated and complement each other to achieve various ethical or unethical, malicious objectives, depending on needs and specific applications. Again, we start with the combination of multiple dedicated ANI applications in the military and security services. ANI applications for satellite data analysis, combined with facial recognition and speech analysis applications, can be used for military and security purposes, including surveillance, intelligence gathering, and even assassinations of security-relevant individuals and objects. ANI technologies can be combined and integrated for achieving other objectives that may not be as destructive as military or intelligence but can harm individuals, organizations, and the community. The combination of ANI for generating fake text, ANI for image manipulation, and ANI for sentiment analysis can be used to create and spread disinformation and fake news to manipulate public opinion or cause confusion. Integrating ANI for facial recognition, ANI for natural language processing, and ANI for biometric data recognition can be used for illegal tracking and hacking of individuals for identity theft, extortion, or other unethical purposes. Using ANI in cyberattacks to bring down websites, infect computers, or steal sensitive data can cause significant harm to individuals, organizations, or countries. Integrating ANI for data analysis and ANI for decision-making can result in systems that discriminate against certain groups of people in areas like employment or lending, which is unethical and against equality laws. Such unethical and criminal uses of ANI pose serious threats and challenges to society. Therefore, it is essential to have

responsible usage and oversight of these technologies to prevent potential abuses and ensure the ethical use of ANI. Regulations and laws have a crucial role in preventing the unethical use of technology, but the responsibility of technology companies and citizens is also necessary in promoting ethical principles.

Strategies to Combat the Dark Side of ANI

Throughout this paper, we have compellingly illustrated that artificial narrow intelligence can indeed present a substantial threat to human society. Under certain catastrophic conditions, it can even put humanity at existential risk, and its misuse by malicious individuals or groups can lead to severe threats to "life as we know it." Despite philosophical uncertainties, these findings should be sufficient to acknowledge that ANI can be a malevolent entity and a dangerous machine, particularly when controlled by malicious individuals or groups. In this section, we will outline basic methods and strategies for countering the dark side of ANI.

The United Nations, the World Economic Forum, the UNICRI, the Center for AI and Robotics, G20, and the OECD have initiated efforts against dark ANI. Companies like Microsoft have helped mobilize the masses in the fight against dark ANI through a set of AI principles instrumental in defining a workplace code of conduct surrounding responsible AI. Microsoft's AI principles include fairness, reliability, safety, privacy, inclusivity, transparency, and accountability. All of the above principles have contributed to the formation of a modern movement determined to combat AI. A socially-driven campaign against autonomous systems was launched through attempts to eliminate public facial recognition, ban drone surveillance, and emphasize responsibility, accountability, and ethics in all AI frameworks.

On the front lines of combating dark autonomous systems, the UN Office for Disarmament Affairs (ODA) has been expanded to include the threat of armed artificial intelligence, and in 2018, the Secretary-General of ODA submitted a plan entitled "Disarmament for Future Generations" dedicated to suppressing dark artificial intelligence in the years to come. UNICRI has also taken measures to work with AI and global law enforcement agencies in an attempt to shut down support for AI in human trafficking, corruption, terrorism, and crime. The U.S. government has shown commitment to building safer AI by issuing a memorandum to federal departments and agencies stating ten AI principles and placing a strong emphasis on public-private transparency for autonomous systems. G20 and the OECD have also set specific goals for combating dark AI through ethical autonomous systemic frameworks that prioritize responsibility and public trust.

Ethical standards for AI are essential to counter "dark ANI." The current situation is not favorable. When considering the use of ANI for military purposes or to subjugate the human population to global interests, there is currently no effective defense. The commissioners of malicious technologies and dark algorithms are states and their security agencies. In situations similar to the use of nuclear energy or biohazard agents, the current solution appears to be a balance of power that exists between major military and economic powers. This is where we should call for the consideration of an initiative to establish a UN Office for Artificial Intelligence. The final decision on whether to establish a UN agency for AI control should be made by taking into account all pros and cons, through broad international debate and collaboration.

Regardless of whether such an agency exists, it is crucial for the international community of leaders, scientists, and experts to work together to develop and implement responsible regulations and guidelines for AI to ensure its safe and ethical use. Without this, the aspiration to build impartial autonomous systems and maintain ethical standards of accountability and privacy for ANI is challenging.

The potential impact of ANI on the development of AGI?

Following the course of each, or at least the majority, of inventions in history, ANI is expected to be a precursor to more complex forms of Artificial Intelligence. In this analogy, AGI should base its development on the achieved level of ANI, taking from it, like an imago from a chrysalis, all achievements, identifying and correcting all the limitations that ANI has. Based on this premise, the development of AGI should, in the coming decades, eliminate and surpass the limits of ANI and continue to evolve, striving to reach the intellectual level of humans and the thinking process of their cerebrum as quickly as possible. But is it really so, and does the path of development, improvement, and enhancement of ANI represent a dead end for the creators of AGI, and especially the ultimate gain, ASI?

Opinions are divided from optimism and excitement to concerns "that the hottest and most modern branch of artificial intelligence - machine learning - will degrade our science and destroy our ethics by using fundamentally flawed concepts of language and knowledge" (Chomsky, Roberts and Watumull, 2023). In other words, it could happen that the concept of ANI, no matter how perfected, may not be able

to serve as the foundation for the development of AGI, precisely because of its primitive fundamental concept that may prove inapplicable for AGI and ASI. Programs classified as ANI and already referred to as "first beacons on the horizon of the long-anticipated advent of artificial general intelligence" are not particularly intelligent. They process vast amounts of data, seek patterns in them, and become adept at generating statistically probable results, such as human language and thought. However useful these programs may be in certain narrow areas, from linguistics and the philosophy of knowledge, we know how far they are from the way humans think and communicate (Chomsky, Roberts and Watumull, 2023).

Unlike ANI, the human mind, which AGI aims to reach and ASI aims to far surpass, is not a clumsy statistical machine that absorbs hundreds of thousands of terabytes of data and costs (will cost) hundreds of billions of dollars just to arrive at the most probable answer to a trivial question. The human mind is a surprisingly efficient and elegant system for working with small amounts of information. It does not seek to build rough correlations between specific inputs but rather to provide explanations. Jeffrey Watumull argues that ANI programs are "stuck in the pre-human or non-human phase of cognitive evolution. Their deepest flaw is the lack of the central critical ability of any intellect: to say not only what is, what has been, and what will be but also what is not, what could be, and what cannot be. These are the ingredients of explanation, the hallmarks of true intelligence" (Chomsky, Roberts and Watumull, 2023).

Although the development and general concept of AGI cannot directly and simply continue from the achieved level of ANI, ANI will nevertheless leave a significant corpus of its achievements as a legacy to higher forms of AI. Despite the ontological difference between the two AI systems, higher forms of AI will not abandon advanced deep learning algorithms, nor will they ignore the massive datasets already stored by ANI systems, even if they are stored only for a specific task. AGI will be intelligent enough to use that data for other purposes. The vast experience ANI programs will gain by answering millions of questions and solving millions of operational requests could be the virtual counterpart of the collective unconscious in humans, as the total record of the quantum of knowledge acquired by all people who have ever lived on the planet. AGI will be intelligent enough to unlock the treasures of that virtual collective unconscious acquired through the use of ANI.

While in its responses to queries it cannot execute, ANI politely responds with learned phrases, uncomfortably, even foolishly ignoring the client for whom it exists, ANI is not aware of the limitations it has. Noam Chomsky and Ian Roberts write how ANI foolishly "demonstrates the 'banality of evil'" (Smirnova, 2023). It is assumed that AGI, self-constituting its strategy, will use the experiences of ANI to identify, understand, and overcome the limitations that ANI has failed to overcome.

We are witnessing serious and competent debates "for and against" AI. This is partly because AI is a new technology that people fear simply because it is new and changes their usual way of life. However, despite objections, ANI systems are becoming widely accepted and useful, which could lead people in the future to be more open to higher forms of AI. Higher forms of AI should be able to act on ethical principles, whether they be deontological or teleological moral principles. Experiences with ANI are completely useless in this area because all known forms of ANI are not able to understand or balance creativity and ethical constraints on their own, not even able to distinguish possible from impossible, which is not a good recommendation for higher forms of AI. The amorality, pseudoscience, and linguistic inadequacy of ANI make it either excessively produce both truths and lies, equally support ethical and unethical decisions or avoid making decisions and remain indifferent to the consequences of such attitudes. Given the amorality, pseudoscience, and linguistic simplicity of ANI systems, we can only mock or mourn their popularity (Chomsky, Roberts and Watumull, 2023).

Discussion

In the previous chapters, we explored the concept of "evil" in the context of Narrow Artificial Intelligence (ANI) or artificial intelligence (AI) in general. While ANI itself lacks consciousness or free will, its potential for misuse or harmful actions that usually result in damage and suffering to humans poses a significant ethical and legal challenge. In this chapter, we continue our analysis and discuss fundamental aspects of this controversial issue. Everything that happens on Earth is caused by either nature or people. Therefore, the crucial aspect of the potential "evil" in ANI comes from human decisions and intentions. ANI systems are inert and perform tasks according to their programming or training on examples and data presented to them during software development and subsequent testing. Any negative consequences of ANI can mostly be attributed to human decisions. This includes programming ANI algorithms, training models with biased or incomplete data, and decisions about the use of ANI in specific contexts.

To understand and control the potential for "evil" use of ANI, it is important to analyze the role of programmers, engineers, and other AI industry professionals. Programmers have a significant influence on

how ANI behaves, even though they are often unaware of all the implications of their decisions. Therefore, it is essential to educate programmers and engineers about the ethical aspects of ANI and provide them with tools to identify and address potential issues.

One of the common ethical challenges related to ANI is bias and discrimination in software designed to make decisions and perform tasks without human verification. ANI systems can inherit biases present in the data sets provided to them by administrators. This can result in unfair decisions, discrimination, and imbalances in the treatment of different groups of people. Research has shown that, despite the fact that AI's abilities in processing data far exceed human capabilities in terms of speed and volume, ANI cannot always be trusted as fair and neutral. The underlying cause of ANI bias is linked to historical human prejudices (Lifshitz, 2021). Human biases are deeply ingrained and extend to certain groups of people, and these biases can be reinforced within computer models. AI systems, therefore, perpetuate existing biases in fields including healthcare, criminal justice, and education. Cases like those of the COMPAS algorithm (Correctional Offender Management Profiling for Alternative Sanctions) in the United States, which is more likely to arrest black individuals due to historical racism and differences in policing practices, highlight the need for more consistent regulation and ethical guidelines for the development and use of ANI, especially in sensitive sectors like security and justice (see more: Bjelajac and Filipović, 2021).

Another crucial aspect of the discussion about the potential "evil" use of ANI is the autonomous nature of some ANI systems. Autonomous military drones can be programmed to execute destructive tasks without human intervention. This raises profound ethical and moral questions in the military application of ANI. To limit the potential abuse of autonomous AI systems, clear ethical guidelines and regulations are needed in the military sector. These guidelines should define the boundaries of autonomous ANI operations and ensure that human responsibility and oversight are preserved. However, this will likely remain mostly declarative, as the military, by default, acts against enemies in warfare, and in such contexts, rules and laws have limited applicability.

One of the key elements in preventing the potential "evil" use of ANI is transparency. Organizations developing ANI systems should be transparent about how they trained models and what data was used. This allows independent experts and organizations to audit and assess ANI systems to ensure they do not contain biases or malicious intentions. Additionally, it is important to establish mechanisms of accountability for AI systems. If irregularities or harm arise from the use of ANI, responsible parties, whether they are programmers, organizations, or owners of ANI systems, should face consequences. This involves the establishment of clear regulations and laws defining responsibility in case of issues with ANI systems.

The balance between progress and risk is often cited as the most important dilemma of the future of AI. People fear non-human entities that could get out of control and begin to act as superhumans. This is where the story of freedom and free will, or moral good and moral evil, in the world of artificial intelligence begins. These two noumena are proportionally dependent. The more one grows, the other diminishes (see more: Kant, 1981). Therefore, governments of major countries want to maximize control over the development and implementation of artificial intelligence. The fundamental thesis with which the European Union approaches thinking about AI is: "We are building trust in artificial intelligence, and that is possible only if we are able to manage risks" (Riegert, 2021). ANI brings tremendous potential to address complex problems and improve human lives. In medicine, science, transportation, and many other areas, ANI has the ability to accelerate progress and make daily life easier for people. Hence, the challenge lies in finding a balance between the potential for positive impact of ANI and the need to limit its negative consequences.

Conclusions

Without diminishing the manifold advantages ushered in by contemporary technologies, the scientific community, with the exception of a substantial cohort encompassing roboticists, electronics specialists, and similar domains, is not reticent in expressing deep-seated apprehension concerning the burgeoning development of artificial intelligence (AI) and its escalating foray into pivotal sectors of public and private life. The deployment of systems founded on deep learning and self-learning neural networks, coupled with the utilization of machines that, on numerous occasions, outpace human counterparts in data analysis and expeditious decision-making, has led to concerns articulated by scientists, humanists, and futurists. Over time, these technologies are not merely poised to displace human labor in many employment sectors but also possess the potential to predict human consumer inclinations, modus operandi, communication patterns, and even exert influence over individual destinies, thereby encroaching upon the sacrosanct citadel of privacy.

Scientists posit that the concentration of metadata, power, and affluence in the hands of a select few has the capacity to obfuscate and render the entire sociotechnical system non-transparent and "opaque." This eventuality is unequivocally predicted to give rise to heightened sociopolitical schisms and to exacerbate, potentially leading to a draconian breach of democratic rights and personal freedoms for both citizens and nations (Couldry and Meijas, 2019). Acknowledging that contemporary humanity, at this stage of its historical progression, evinces a predilection for the encapsulation of its essence within the realm of technology, scientists, particularly those within the domains of philosophy, sociology, and theology, evince reluctance in relegating the stewardship of AI ethics to engineers and technicians. The skepticism directed towards emerging technologies, particularly cognitive AI, can be expounded upon by recourse to the prevailing societal concept of scientific neutrality, while differentiating the jurisdictions of the scientific and legal spheres. It is our contention that the world is on the cusp of an academic schism, a tug-of-war between champions of raw power and proponents of global security and the preservation of "life as we know it." This would not mark the inception of such a schism but would be resolved as in instances past—with the facile triumph of power's apologists. The conventional narrative dictates that this innocuous dominion is destined to expeditiously metamorphose into financial and military might. This is not indicative of the world teetering on the precipice of dissolution; it serves as a clarion call for judiciously overseeing the use, and potential abuse, of AI. History has persistently underscored that behind every perilous contraption lurks an equally pernicious human agent. Our elucidation of this ethical aporia can be attributed to divergent interpretations regarding the core tenets of AI ethics. Practitioners from the realm of the natural sciences are preoccupied with the transliteration of prevailing, and occasionally antiquated, ethical paradigms into the vernacular of machinery. In contrast, philosophers, sociologists, humanists, and theologians grapple with the very essence of AI ethics, which must undergo an evolution commensurate with the assimilation into its ontological and metaphysical corpus of a conspicuous novelty—an artificial entity furnished with its heretofore alien concepts of good and evil. This nascent ethical framework shall be denominated a biomimetic ethos, one that may be adjusted on the fly by humans to conform to emerging entities, as this novel ethical framework is co-created in tandem with these entities.

Artificial intelligence steadfastly advances, and each new application of this technology offers a novel aperture for autonomous systems to harness data to effect harmful outcomes. The promulgation of legislation emphasizing responsibility, transparency in AI, mitigation of bias, and the comprehensive implementation of ethical precepts is posited as an efficacious strategy for contending with the "dark AI." The urgency of addressing the darker facets of AI mounts with each passing second. The present juncture, more than any other, underscores the need to glean instructive insights from humanity's historical missteps and prepare judiciously for the impending challenges.

Conflict of interests
The authors declare no conflict of interest.

Author Contributions
Conceptualization: Ž.B., A.F., and L.S; methodology: Ž.B.; resources: A.F. and L.S., supervision: Ž.B.; writing—original draft preparation: Ž.B, A.F., and L.S.; writing—review and editing: Ž.B., A.F. and L.S. All authors have read and agreed to the published version of the manuscript.

References

Bathaee, Y. (2018). The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology, 31*, 889.

Begishev, I., & Khisamova, Z. (2018). Criminological risks of using artificial intelligence. *Russian Journal of Criminology, 12*(6), 767–775. https://doi.org/10.17150/2500-4255.2018.12(6).767-775

Bjelajac, Ž. (2011a). Pranje novca kao faktor ekonomske destabilizacije u nacionalnim i međunarodnim razmerama [Money laundering as a factor of economic destabilization on national and international scales]. *Poslovna ekonomija, 5*(2), 151-170.

Bjelajac, Ž. (2011b). Contemporary tendencies in money laundering methods: Review of the methods and measures for its suppression. The Research Institute for European and American Studies – RIEAS, *Research paper, 151*, 1-22.

Bjelajac, Ž., Filipović, A. (2019). Gamification as an Innovative Approach in Security Systems. In *Proceedings of the 1st Virtu-al International Conference „Path to a Knowledge Society-Managing Risks and Innovation - PaKSoM 2019".*

Bjelajac, Ž., Filipović, A. (2021). Artificial Intelligence: Human Ethics in Non-Human Entities. In *Proceedings of the 3rd Virtual International Conference „Path to a Knowledge Society-Managing Risks and Innovation - PaKSoM 2021".*

Bjelajac, Ž., Filipović, A., Stošić, L. (2022). Quis custodiet ipsos custodes: Ethical Dillemmas of the KM Governed by AI. In *Proceedings of the 4th Virtual International Conference „Path to a Knowledge Society-Managing Risks and Innovation - PaKSoM 2022".*

Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies.* Oxford University Press.

Bjelajac, Ž., Filipović, A., & Stošić, L. (2023). Can AI be evil: The criminal capacities of ANI, *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), 11*(3), 519-531.

Chomsky, N., Roberts, I., & Watumull, J. (2023, March 8). *Noam Chomsky: The False Promise of ChatGPT*. The New York Times. Retrieved from https://www.nytimes.com/2023/03/08/opinion/noam-chomsky-chatgpt-ai.html

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism.* Stanford University Press.

Encensberger, H. M. (1980). Nemačka, Nemačka, između ostalog [Germany, Germany, Among Other Thinhs]. BIGZ.

Filipović, A. (2019). Foreword to „Understanding video game subculture", *Kultura polisa, 16*(1), 7–10. Retrieved from http://kpolisa.com/index.php/kp/article/view/374

Ford, M. (2018) Architects of Intelligence, 1st ed. Packt Publishing. Retrieved from https://www.perlego.com/book/858994/architects-of-intelligence-the-truth-about-ai-from-the-people-building-it-pdf

Hajdeger, M. (2000). *Šumski putevi* [Off the Beaten Track]. Plato.

Hamet, P., & Tremblay, J. (2017). Artificial intelligence in medicine. *Metabolism: clinical and experimental, 69S,* S36–S40. https://doi.org/10.1016/j.metabol.2017.01.011

IBM Data and AI Team. (2023). *AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference?* IBM Blog. Retrieved from https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks

Kant, I. (1981). *Zasnivanje metafizike morala* [Groundwork of the Metaphysics of Morals], BIGZ.

Lifshitz, B. (2021, May 6). *Racism is Systemic in Artificial Intelligence Systems, Too.* Georgetown Security Studies Review. Retrieved from https://georgetownsecuritystudiesreview.org/2021/05/06/racism-is-systemic-in-artificial-intelligence-systems-too/

Marr, B. (2018, September 17). *Smart dust is coming. Are you ready?* Forbes. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/09/16/smart-dust-is-coming-are-you-ready/?sh=7bf332405e41

Minevich, M. (2020, February 28). *How To Combat The Dark Side Of AI.* Forbes. Retrieved from https://www.forbes.com/sites/markminevich/2020/02/28/how-to-combat-the-dark-side-of-ai/?sh=83126c9174ba

Mosechkin, I. (2019). Artificial intelligence and criminal liability: problems of becoming a new type of crime subject. *Vestnik Sankt-Peterburgskogo Universiteta, 10*(3), 461–476. https://doi.org/10.21638/spbu14.2019.304

Ovchinskiy, V.S. (2022). *Криминология цифрового мира: учебник для магистратуры* [Criminology of the digital world]. Norma.

Petrosyan, A. (2023, August 29). *U.S. most frequently reported cyber crime by number of victims 2022.* Statista. Retrieved from https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-us/

Piquard, A. (2023, April 26). *Musk's X.AI start-up highlights paradoxical relationship with AI.* Le Monde.fr. Retrieved from https://www.lemonde.fr/en/economy/article/2023/04/18/musk-s-x-ai-start-up-highlights-paradoxical-relationship-with-ai-anew_6023306_19.html

Price, M., Walker, S., & Wiley, W. (n.d.). *The Machine Beneath: Implications of Artificial intelligence in Strategic Decision Making.* PRISM - National Defense University. Retrieved from https://cco.ndu.edu/News/Article/1681986/the-machine-beneath-implications-of-artificial-intelligence-in-strategic-decisi/

Proudfoot, D. (2018). *Alan Turing and evil Artificial Intelligence.* Oxford University Press blog. Retrieved from https://blog.oup.com/2018/01/alan-turing-evil-artificial-intelligence/

Rasel, Dž. B. (1982). Mit o đavolu, Jugoslavija.

Riegert, B. (2021, April 29). *EU: Strogo kontrolisana veštačka inteligencija* [EU: Strictly controlled artificial intelligence]. dw.com. Retrieved from https://www.dw.com/sr/eu-strogo-kontrolisana-ve%C5%A1ta%C4%8Dka-inteligencija/a-57376780

Smirnova, E. (2023, March 13). *Лингвист Ноам Хомский раскритиковал ChatGPT, назвав его ответы «банальностью зла»* [Linguist Noam Chomsky criticized ChatGPT, calling its responses the "banality of evil."]. High Tech Plus. https://hightech.plus/2023/03/13/lingvist-noam-homskii-raskritikoval-chatgpt-nazvav-ego-otveti-banalnostyu-zla

Stevens, R. W. (2023, May 18). *20 Ways AI enables criminals.* Mind Matters. Retrieved from https://mindmatters.ai/2023/04/20-ways-ai-enables-criminals/

Verma, A. (2020, July 7). *Hype Cycle for Sensing Technologies and Applications, 2020.* Gartner. Retrieved from https://www.gartner.com/en/documents/3987226