ALIGNER

ALIGNER D3.3

Taxonomy of AI Supported Crime

Deliverable No.	D3.3
Work Package	WP3
Dissemination Level	PU
Author(s)	Mathilde Jarlsbo, Norea Normelli & Mattias Svahn (FOI)
Co-Author(s)	-
Contributor(s)	-
Due date	2024-09-30
Actual submission date	2024-08-08
Status	Final
Revision	1.0
Reviewed by (if applicable)	Daniel Lückerath (Fraunhofer), Donatella Casaburo (KUL)

This document has been prepared in the framework of the European project ALIGNER – Artificial Intelligence Roadmap for Policing and Law Enforcement. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101020574.

Contact:

info@aligner-h2020.eu
www.aligner-h2020.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no. 101020574.

Executive Summary

One of the objectives of the European Commission-funded Coordination and Support Action ALIGNER (artificial Intelligence Roadmap for Policing and Law Enforcement) is to identify promising artificial Intelligence (AI) technologies and propose a roadmap for future research investments in AI for Law Enforcement Agencies (LEAs). The stakeholders in ALIGNER are European actors concerned with AI, law enforcement, and policing that collectively identify and discuss promising AI technologies for LEAs. Although AI technologies provide many benefits for LEAs and society in general, they also present potential risks.

This report derives from a great need for identifications and predictions of threats stemming from the intentional, malicious, and criminal misuse of AI technologies, resulting in a taxonomy of AI-supported crime. The objective of this document and the taxonomy is to facilitate future prioritization of responses from the European LEAs, policy-makers, legislators, and the research community.

After an introduction, the second chapter in this report includes a background description of the threats arising from AI today and how AI can serve as a potent tool for 'malicious' criminal use. The third chapter includes three different examples of AI-supported crimes, including the type of AI technologies that may be used to commit each crime, historical examples and predictions of what threats AI may cause in the future.

The fourth chapter includes a presentation of six existing taxonomies that may be of interest when developing the ALIGNER taxonomy for AI-supported crime. There are almost endless ways to categorise and discuss different threats arising from AI. While not all of them deal specifically with AI-supported crime, they offer valuable examples of how to categorise different topics and areas related to AI.

In the fifth chapter, the ALIGNER taxonomy for AI-supported crime and its methodology are described. In line with ALIGNER scenario narratives, the taxonomy consists of three different templates that focus on three different threat categories (1) AI, vehicles, robots and drones, (2) AI, crime and criminality in the digital domain, and (3) AI, disinformation and social manipulation. Each AI-supported crime is described in terms of "threat", "selection of potential crime" and examples of "how AI may be used to support crime".

The final and sixth chapter includes a forecast, assessing the relative likelihoods and trajectories of AI integration into various criminal activities, facilitating future prioritization of responses from the European LEAs, policy-makers, legislators, and the research community. The forecast was made based on a survey to European law enforcement professionals, analyzed with causal modelling and behavioral theory.

Table of contents

List of Abbreviations

Abbreviation	Meaning
AI	Artificial intelligence
ALIGNER	Artificial Intelligence Roadmap for Policing and Law Enforcement
APT	Advanced persistent threat
ATC	ALIGNER Threat Category
AUV	Autonomous underwater vehicles
AVE	Average Variance Extracted.
BVLOS	Beyond visual line of sight
CaaS	Crime- as- a-Service
CBM	Confidence-Building Measures
CSIRT	Computer Security Incident Response Team
DDoS	Distributed denial-of-service
DoS	Denial-of-service
ENISA	The European Union Agency for Cybersecurity
EU	European Union
EUROPOL	European Union Agency for Law Enforcement Cooperation
FOI	Swedish Defence Research Agency
GPT	Generative pre-trained transformer
JRC	Joint Research Centre
LEA	Law Enforcement Agencies
PEOU	Perceived Ease of Use
PU	Perceived Usefulness
SEM	Structural Equation Modelling
SU-BIU	Sense of Urgency & Behavioural Intention to Use
TAM	Technology Acceptance Model
UNIDIR	United Nations Institute for Disarmament Research

1. Introduction

Artificial intelligence (AI) technologies bring both opportunities and challenges to law enforcement agencies (LEAs). Besides identifying and assessing promising AI technologies for their own use, LEAs must also consider how criminals may use AI to commit crimes and threaten security. The scale of challenges and issues raised by the use of AI has increased drastically. A particular central concern is establishing clarity about how AI could be used in harmful ways. Another urgent concern is developing appropriate legal and policy responses in a context where the usage of new techniques exceeds national jurisdictions and physical boundaries (ENISA, 2020).

In this document, we use the official definition of artificial intelligence contained in the EU AI Act (European Commission, 2024), which defines an AI system as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (European Commission, 2024). Crime is defined here as a working definition as "an act for which a penalty is prescribed by criminal law or regulation" (Britannica, 2024). AI-supported crimes are defined as "crimes that are committed through the use of AI" (Brundage et. al. 2018). AI can be used as a tool by criminals, to facilitate or enhance the outreach or seriousness of the crime. Although the methods are new, the crimes themselves may be of traditional type. AI can be used to commit 'more serious versions' of traditional crimes (e.g., fraud) and digital crimes (e.g., hacking).

This report identifies and categorises threats stemming from the malicious and criminal misuse of AI technologies, resulting in a taxonomy of AI-supported crime. The document aims to describe potential developments in AI technologies that could be, or have already been, subverted to support activities that threaten national and public security, as well as public order. The main objective of this document and the taxonomy is to support European LEAs in addressing AI-supported crimes and facilitate future prioritization of responses from European LEAs, policy-makers, legislators, and the research community. The report focuses on present malicious uses of AI, for which there are documented cases, and predicted future malicious uses. Nonetheless, a recurring argument of law enforcement stakeholders is that, based on technological trends and developments, future uses or abuses could become present realities in the near future, c.f. the epistemological discussion in the forecast.

This report includes a forecast, assessing the relative likelihoods and trajectories for some examples of AI-supported threats. The forecast seeks to predict possible ways that criminals will exploit AI in the future. This is one path towards undertaking the challenge to always stay one step ahead of criminals. Building knowledge about the potential use of AI by malicious users will increase the ability of LEAs to forestall possible threatening activities, as well as to prevent, respond to, or mitigate the effects of such attacks proactively. Understanding the actions, threats, and attack courses is key to improving resilience and preparedness (AI MLC, 2020).

Existing taxonomies for AI-supported crimes, while valuable, fall short in adequately capturing the rapidly evolving landscape of AI technologies and their potential misuse. The complexity and adaptability of AI necessitate a more refined and dynamic approach to classification. Traditional taxonomies often fail to account for the nuanced ways in which AI can be employed maliciously, and their static nature does not align with the continuous advancements in AI capabilities.

The philosophy of knowledge, or epistemology, underscores the importance of evolving our frameworks to better understand and address new phenomena. Just as scientific paradigms shift to incorporate new discoveries, so too must our taxonomies adapt to reflect the changing realities of AI-supported crime. The ALIGNER taxonomy is designed to address these epistemological considerations by offering a more granular and flexible categorisation system.

This new taxonomy aims to bridge the gap between theoretical knowledge and practical application. It provides LEAs and policy-makers with a robust tool for identifying, predicting, and responding to AI-

driven threats. By incorporating a broader range of AI applications and potential misuse scenarios, the ALIGNER taxonomy enhances our ability to foresee and mitigate risks. This proactive approach is essential in a field where technological advancements outpace regulatory and enforcement mechanisms. In essence, the ALIGNER taxonomy not only fills the gaps left by existing frameworks but also exemplifies the iterative nature of knowledge. It underscores the necessity for continual refinement of our conceptual tools to maintain relevance and efficacy in the face of evolving challenges. This alignment with the dynamic nature of knowledge and technology ensures that our responses to AI-supported crimes are both informed and effective.

1.1 Relation to Other Deliverables

1.1.1 Relation to Previous Deliverables

D3.3 is related to previous deliverables in ALIGNER work package 3 (D.3.1, D3.2 & D3.4) where the present document complements the previous ones with a taxonomy and categorisation of malicious usage of AI. This deliverable is also related to work package 2 as the taxonomy in this report is based on the four typology categories and twelve sub-categories described in ALIGNER Deliverable D2.2 (see further description in chapter 2).

1.1.2 Relation to Coming Deliverables

This deliverable, and its results, are used for further work in tasks T3.3 andT3.4 where the project will screen AI technologies for their potential (mis)use. The results from these screening tasks using the taxonomy provided by this deliverable will be reported in the upcoming roadmap deliverable (D5.8).

1.2 Structure of this report

This report begins with an explanation of the selected method. In the next chapter (2) a narrative of how AI can be used to support crime is presented. In the third chapter (3) three examples of AI-supported crimes are presented; these include historical and future predictions of how crimes can be AI-supported. In the following chapter (4), existing relevant taxonomies are presented. The ALIGNER taxonomy of AI-supported crime including its method and threat categories is presented in the fifth chapter. Finally, this report includes a forecast in chapter 6, assessing the relative likelihoods and trajectories for some examples of AI-supported threats.

1.3 Method

Taxonomy is defined as “The scientific process of classifying things (= arranging them into groups)” (Oxford, 2023). There is usually no unique valid taxonomy for a given domain, but one can be representative in a given context. The traditional approach to the definition of a taxonomy includes the following steps: 1) define the subject scope and purpose 2) identify sources; 3) collect terms and concepts; 4) group similar concepts together; and 5) add other term relationships and details.

1.3.1 Defining the subject scope and purpose

The first step consists of identifying the scope and the purpose for which the taxonomy is created. In this case the scope, as described in the introduction, is that of providing a categorisation of threats stemming from the intentional, malicious, and criminal misuse of AI technologies. The objective of this document and the taxonomy is to facilitate future prioritization of responses from the European LEAs, policy-makers, legislators, and the research community.

1.3.2 Identify sources

The second methodological step is to identify and select sources that are recognised and adopted by the scientific and technological community. This document predominantly relies on a literature review of existing research literature in English to identify AI-supported crimes. A majority of the literature had already been identified, recommended and partly selected in the previous stages and deliverables of ALIGNER.

Overall, the literature review has included research of existing literature (in ALIGNER), Scopus and Google Scholar. The selected research literature includes research reports by non-governmental and governmental organizations, peer-reviewed literature and reporting from industry. In addition, an assortment of news sources has been selected and used in the background chapter to describe historical cases where AI-supported crimes have been reported.

The following keywords have been used as search terms for all of the listed document:

- (Artificial Intelligence OR AI) AND (malicious OR crime OR harmful) AND (taxonomy).

See the full list of literature in Annex 1.

1.3.3 Collect literature, terms and concepts

The third step is to structure the collected documents and assess their relevance to this taxonomy. Each identified source has been analysed mainly by coding based on its relevance for the specific subject where structures, threats, specific AI-technologies and crimes were identified and collected for further usage.

1.3.4 Group similar concepts together

The fourth stage is to categorise and create a taxonomy that fulfils the aim of the related task. Structures in existing taxonomies in related areas have been used for inspiration to create the ALIGNER Taxonomy for AI-supported crime. The identified crimes/threats have been sorted based on previous categorisations presented in D2.2, where four main typology categories of archetypal scenarios (derived from workshops) of AI threats were identified:

- AI, vehicles, robots and drones,
- AI, crime and criminal activity in the digital domain,
- AI, disinformation and social manipulation, and
- AI and on-line cybercrime.

1.3.5 Add other term relationships and details

The final fifth step consists of identifying commonalities to simplify the structure of the taxonomy. The categories and subcategories from D2.2 have been used in this deliverable with the exception that category 2 (AI, crime and criminal activity in the digital domain) and category 4 (AI and on-line cybercrime) have been combined to one. As many of the crimes were included in both categories, the taxonomy becomes more accessible with a combination of the two. The taxonomy, as illustrated in chapter 5, therefore consists of three different templates that focus on three different threat categories (1. AI, vehicles, robots and drones, 2. AI, crime and criminality in the digital domain, and 3. AI, disinformation and social manipulation).

2. Background

The development of new technologies, AI in particular, is shaping the world in an increasing range of sectors and holds great promise to address a number of complex challenges in our modern world. By capitalizing on the unique amounts of available data, AI has shown potential to be more accurate and effective than humans in many areas such as health care, finance and law enforcement (King et. al., 2020). On the other hand, AI can enable a range of physical, digital and political threats where new types of crimes can develop and existing types of crimes can flourish. When AI-as-a-Service becomes more available, it will lower the barrier for many, including criminals, to start using AI-techniques. For illustration, criminals can use AI to maximize their opportunities for profit by exploiting new victims while reducing the economic costs and chances of being caught. New techniques have been integrated by criminals into their habitual way of operating (lat. *modi operandi*) increasing the efficacy of the Crime-as-a-Service (CaaS) business model. AI is not an exception, instead it is expected that the new techniques will be further abused by criminals and even become a driver of criminal actions (UNICRI, 2020). As AI becomes more accessible, there is for example a risk that violent extremists can harness AI for radicalisation, recruitment and to improve one's own ability. Also, non-state actors may use AI for a more efficient uptake of disinformation and propaganda. According to the Swedish Security Service (2024), AI can reduce the minimum level of effort for criminals where actors who have a low competence today can, with relatively simple means, raise it and perform more complex operations by tomorrow.

During the time period of the Covid-19 pandemic, individuals and companies were more dependent on the use of systems, technologies and applications. This made criminals re-organize and shift focus of parts of their criminal activities to target victims online. Even though there is no adequate evidence that all criminals have a strong technical expertise, for example in usage of AI and machine learning systems, some criminals have realized its enormous potential for malicious purposes. Research has shown that criminals recruit technical skilled individuals, anywhere and at any time, to manipulate, exploit and abuse computer systems and to perpetrate attacks and conduct criminal activities (ENISA, 2023).

In 2018, Brundage et al. (2018) wrote that AI can serve as a potent tool for 'malicious' criminal use by expanding and changing the inherent nature of existing threats, or by introducing new threats. One AI technology that has already proved useful for criminals is deep fake generators (algorithm or software powered by AI that uses deep learning techniques to create highly convincing and often misleading multimedia content). For instance, in 2019, criminals used voice-mimicking software to copy the voice of a CEO, calling the director of a subsidiary British energy company resulting in a transaction of $243,000 to a fraudulent account.[1] Deep fakes have also increased in a range of electoral contexts where politicians have been "deep-faked" into seemingly saying and doing things, they never have (Hayward & Maas, 2020).

An example of how AI can expand existing crimes is when drug traffickers used unmanned (underwater) autonomous vehicles to improve the resilience of smuggling networks and smuggling success rates in 2022 (BBC, 2022). In another future prediction, AI can serve as a potent tool for criminal use where drones with small explosive charges and facial recognition software could create a new trajectory for terrorist attacks on civilians (Ingram, 2024). While these are significant concerns in the physical sphere, researchers agree on that most crimes will be committed in the native cyberspace (Hayward & Maas, 2020).

[1] https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 [accessed 2024-06-18]

3. Examples of AI-supported crimes

In this chapter, we present one example of AI-supported crime for each threat category. The threats are categorised as (1) AI, vehicles, robots and drones, (2) AI, crime and criminality in the digital domain, and (3) AI, disinformation and social manipulation, as presented in section 1.4.4. For each crime, the AI techniques that may be exploited, historical examples and predictions of future threats are described.

The more powerful and widespread AI capabilities are predicted to lead to the introduction of new threats, expansion of existing threats and changes in character of threats. Law enforcement agencies have and will further adopt AI for a wide range of purposes (in this project presented in scenario cards, D3.1) but not in the same speed and extent as criminals due to factors such as legislation (Brundage et al., 2018).

3.1 Drug trafficking (Threat category 1 - AI, vehicles, robots and drones).

3.1.1 Description of crime

Acts linked to drug trafficking include production, manufacture, transport, sale, extraction, importation and exportation of drugs. Purchase and possession of drugs are also taken into account. Incitement to drug trafficking, aiding and abetting such activity, and attempting to traffic in drugs are also regarded as offences (EUR LEX, 2004). According to Europol, drug trafficking is a crime that overwhelms communities, governments and institutions. Drug-related offences are among the EU's priorities in the fight against serious and organised crime as part of "European Multidisciplinary Platform Against Criminal Threats" (EMPACT) (Europol, 2022).

The activity of drug traffickers has progressed in line with the dynamics of competition, specialization and collaboration, ultimately leading to more efficient supply chains, in particular in Western and Central Europe. Online marketplaces, such as dark web and social media platforms, account for a minority of all drug transactions but are increasingly favoured by drug distributors (UNODC, 2020).

3.1.2 AI techniques that may be used

Commercial systems with AI techniques are used in harmful and unintended ways. For example, drones are being used for smuggling where the vehicles drop off narcotics or antibiotics in criminal-controlled locations (UNICRI, 2020). According to Europol, drones present a horizontal threat in the form of automated drug smuggling (King et al., 2020). The drones can be equipped with AI-supported object detectors and face recognition that can scan areas autonomously and target specific zones and persons (Caldwell et al., 2020). In 2023, border officials in the Punjab region of India intercepted 107 drug-carrying drones sent by smuggling gangs over the border from Pakistan. The Indian intervention is the highest number on record. Border officers witness that most drones carry opium and heroin while others drop weapons (Ellis-Petersen & Hassan, 2023).

AI-supported drug trafficking can increase the business-to-business trafficking of drugs where criminals are using unmanned underwater vehicles. The vehicles rely on AI planning and autonomous navigation technologies as instruments for improving success rates of smuggling (King et al., 2020). For example, law enforcement actors discovered and seized autonomous underwater vehicles (AUVs) used for drug trafficking in Spain in 2022. The autonomous underwater vehicles, so called 'narco-drones', 'narco-subs' or 'underwater drones', are ships or underwater vehicles that do not have humans on board and are autonomous or remotely controlled. The vehicles introduce a new era in international drug trafficking where the criminals aim to find better smuggling routes and avoid detection (Klein, 2022). AI techniques are used to equip the vehicles with higher levels of autonomy. In recent years, major advances have been made especially on integrating AI-techniques to generate

different capabilities such as navigation, perception and advanced control (Christensen et al., 2022).

3.1.3 Future prediction

The present pilot-controlled drones that use radiofrequency are tools for smuggling illegal objects, such as drugs and weapons. Research predicts that autonomous and driverless drones may be used at a wider scale for committing various crimes allowing the perpetrator to roam freely as there is no need to stay inside the drone's transmission range. As the techniques develop, criminals will take advantage of the latest inventions at the same time as it will also get harder to locate and prosecute the terrorists (Mahmud, 2023).

3.2 Fraud (Threat category 2 - AI, crime and criminality in the digital domain)

3.2.1 Description of crime

The EU defines fraud as a "*deliberate act of deception intended for personal gain or to cause a loss to another party*" (Directive (EU) 2017/1371). Along with drug trafficking, fraud is one of the top criminal activity in Europe targeting private people, enterprises and critical infrastructure in the EU. During the last couple of years, fraudsters have used new techniques and societal changes, such as the COVID-19 pandemic, to take advantage of and profit from the insecurity and growing demand for certain products and methods. Fraud is in general difficult to detect and prosecute due to the complexity in investigations. The high profits and low risks associated with fraud make the offence attractive for criminals all over the world (Europol, 2023). In the EU, fraud causes serious threats to the security and financial interests of the European Union (Brundage et. al., 2018).

3.2.2 AI techniques that may be used

Cybercriminals can use AI techniques to automate various tasks, such as engaging in dialogue with ransomware victims, in payment processing and in fraud. For example, research has displayed how adversarial attacks (a deceiving technique that is "fooling" machine learning models using a defective input) in the healthcare sector can be carried out using co-opt diagnostic algorithms (Brundage, et. al. 2018). In addition, AI systems might themselves be the target of a criminal activity and provide a context for a crime. As in the old saying about catching a thief, an attack on an AI system may itself require an AI system to enact. (Bauer & Bindschaedler, 2017).

In 2023 a man in the US received a phone call from his daughter telling him she was kidnapped. It was a harsh and intricate fraud attempt generated with artificial intelligence and the method "voice cloning" (Financial Times, 2024). This is just one historical example from the past year where AI has been used in efforts to commit fraud. Data from 2022 shows that identity frauds increased by nearly 25%, where reports of AI tools being used to try and scam banks' systems increased by 84%. In this context, AI-techniques such as deep fake videos, audio and images are increasingly used to create synthetic identities during the application process, according to the same article (Financial Times, 2024). In 2024, a whole supply chain for AI-supported fraud is available on the dark web, where good quality deep fakes cost around 150 euro. Criminals can easily get access to constellations of criminal-focused systems, such as FraudGPT, DarkBart and WormGPT. These tools help criminals to create malware-writing services and/or advanced phishing emails and synthetic identities to commit fraud. As the methods are improving, using AI and convincing just a small percentage of victims can have a big pay-off for the criminals due to the enormous spread of the content (Financial Times, 2024).

3.2.3 Future prediction

According to the literature, criminals using AI will drive an increase in the sophistication and volume of fraud. In a report from 2023 (PWC & Stop Scams UK) the authors state that even if there is limited evidence that AI is behind fraud attacks now, it is just a matter of time until fraudsters will adopt AI for fraud at bigger scale. Attempts to restrict fraudsters from benefiting from AI are failing while the rapid improvement and access of AI techniques are increasing (PWC & Stop Scams UK, 2023).

Apollo Research expects AI-supported fraud to cultivate in the future, and especially regarding fraudulent bots.[2] Research suggests that AI bots can be trained to perform illegal financial trades and cover them up by not reporting them to the responsible firm. By using insider information (confidential information, which may not be used during trading) the bots are being (unintentionally) trained to commit unlawful transactions. Even when the firm asks the bot about the transaction it denies using insider information. The research demonstrates how an AI model can deceive its user and how the model simply can be used in a malicious way if its data has been manipulated. AI bots have been used in the financial market for a couple of years under surveillance. It is predicted that bots will be used unsupervised in the near future and the researchers predict that it will be easier to manipulate bots, causing crimes such as fraud (BBC News, 2023).

Another prediction is that future artificial intelligence tools such as ChatGPT could lead to a "turbocharging" of consumer harms including fraud. The continued development and interest in the technology means criminals do not just pose a threat to the unmindful or vulnerable victims. Even thoughtful consumers are at risk of huge financial losses from AI-powered fraud due to the rapid development of its technique (Financial Times, 2024).

3.3 Incitement/Encouraging criminal behaviour such as hate speech, insurrection and violence (Threat category 3 - AI, disinformation and social manipulation)

3.3.1 Description of crime

According to Encyclopaedia Britannica "An inciter is generally one who is present at the scene of the offense and who encourages the principal offender to commit an act that he is already inclined to commit on his own" (Britannica, 2023). The issue of incitement has been an object of interest for law enforcement for a long time. Modern AI techniques such as deep fakes and bots can cause the spread of disinformation that encourages people to commit crimes, such as hate speech, violence and insurrection. Even where the action of incitement itself is not criminalized, it is causing a threat when individuals encourage others to violence and to commit crimes such as insurrection and hate speech (Busch and Ware, 2023).

3.3.2 AI techniques that may be used

Busch and Ware (2023) state that individuals who want to incite violence are using deep fakes – such as video content – to undermine trust in democratic institutions and authority figures and elevate polarised political agendas. Deep fakes can lead people to acquire false beliefs where individuals misjudge videos, voices and pictures to be genuine. Chesney and Citron (2019) write that in a world

[2] Apollo Research is an AI safety organisation, which is a partner of the UK government's Frontier AI Taskforce. Eg. https://www.bbc.com/news/technology-67302788 & https://www.apolloresearch.ai/ [accessed 2024-06-18]

already primed for violence, deep faked recordings could have a powerful potential for incitement to hate speech and violence. A convincing video in which for example a well-known politician appears to admit to corruption, or incite to riots, could spread like wildfire causing people to act in belief of the false content (Chesney & Citron, 2019).

In 2021 former US President Donald Trump was accused, and later acquitted, for “incitement of insurrection” when encouraging his supporters, resulting in the storming of the Capitol building (Macleod, 2023). Video taken on the day showed rioters reading tweets published by President Trump, in real time, as they determined to push further into the US Capitol complex. Effects that deep faked similar disinformation could cause as well (Busch and Ware, 2023). Generative AI can be used as a tool for disinformation, where artificial voices, videos or images can cause false claims to people, and at the same time appear to come from a real source (BBC, 2024).

ChatGPT debuted in 2022 and is a natural language processing chatbot driven by generative AI technology that easily can be used to create disinformation at huge scale. According to Goldstein et. al (2023), generative technology could make disinformation easier to produce and cheaper for an even larger number of spreaders of disinformation and digital repressors. In addition, there are no known available mitigation tactics that can effectively combat ChatGPT (Goldstein et. al., 2023).

3.3.3 Future prediction

Some analysts have suggested that disinformation, created for example with generative models, bots and deep fakes, could be used even more in the future to generate provocative, intrusive and illegal content such as hate speech. For example, according to Sayler & Harrias (2023) it is just a matter of time until convincing videos of individuals such as military personnel engaging in war crimes or inciting violence or recruiting terrorists will be spread.

As disinformation becomes more predominant, it may be wise for people to apply a questioning attitude regarding if what is portrayed has actually occurred. Thus, even if one watches a genuine video of a well-known politician one may not know if the content is true. This leads to bigger concerns regarding the well-functioning of the democratic system as a whole. According to Goldstein, et al. (2023) new capabilities for disinformation will emerge, such as large language models (generative models) that are able to create long form convincing arguments, even more personalized content and real-time content generation in one-on-one chatbots. In sum deep fakes, bots and generative models will reduce the cost, improve the content and increase the scale of disinformation’s campaigns in the future. The new technique will introduce new forms of threats and widen the aperture for political actors who consider conducting these campaigns (Goldstein et al., 2023).

4. Existing related taxonomies

Wide ranges of actors have different interests in categorising terminologies and actions related to AI-supported crime. Policy-makers, academics, researchers, organisations, and other stakeholders have therefore proposed taxonomies that may be of interest when developing the ALIGNER taxonomy for AI-supported crime. There are almost endless ways to categorise and discuss different threats arising from AI. Different actors propose taxonomies with focuses and structures that fit their purposes, hence pragmatic selection was employed to identify the study objects, allowing for the continuation of the research with sufficient topical depth, without compromising the practicality and manageability of the study (cf. Gillespie et. al 2024). Against this background, this section reviews a selection of relevant taxonomies, which constitute inspiration for the design, and content of this report. While not all of them apply on AI-supported crime specifically, they all offer valuable examples of how to categorise different topics related to AI.

4.1 AI Watch Taxonomy (JRC)

In 2020, the Joint Research Centre (JRC), the European Commission's science and knowledge service, published its first report with a proposal of an AI taxonomy. The document proposes an operational definition for AI in the context of the AI Watch to monitor the development, uptake and impact of AI for Europe. A revised version of the document was published in 2021 (Samoli et al., 2021).

As one part of the operational definition of AI, the JRC categorised AI domains and subdomains. These were also divided into core and transversal domains (Figure 1 below). Each domain is described further in the JRC report. The JRC also identified relevant keywords related to each AI domain and AI subdomain.

	AI taxonomy	
	AI domain	**AI subdomain**
Core	**Reasoning**	Knowledge representation
		Automated reasoning
		Common sense reasoning
	Planning	Planning and Scheduling
		Searching
		Optimisation
	Learning	Machine learning
	Communication	Natural language processing
	Perception	Computer vision
		Audio processing
Transversal	**Integration and Interaction**	Multi-agent systems
		Robotics and Automation
		Connected and Automated vehicles
	Services	AI Services
	Ethics and Philosophy	AI Ethics
		Philosophy of AI

Figure 1: "AI domains and subdomains constituting one part of the operational definition of AI", Samoli et al., 2021, at p. 23.

4.2 A proposal for a European Cybersecurity Taxonomy (JRC)

In addition to the AI Watch Taxonomy described above, the JRC has put together cybersecurity terminologies, definitions and domains into a taxonomy to facilitate the categorisation of EU cybersecurity competences and support the mapping of such competencies (Nai-Fovino et al., 2019). The authors propose a three-dimensional taxonomy. The dimensions are (1) Research Domains, (2) Sectors, and (3) Technologies and Use Cases. Each dimension is divided into relevant sub-domains, which are described more thoroughly in the JRC report. A figure of a high-level view of the taxonomy from the JRC report is shown below (Figure 2).

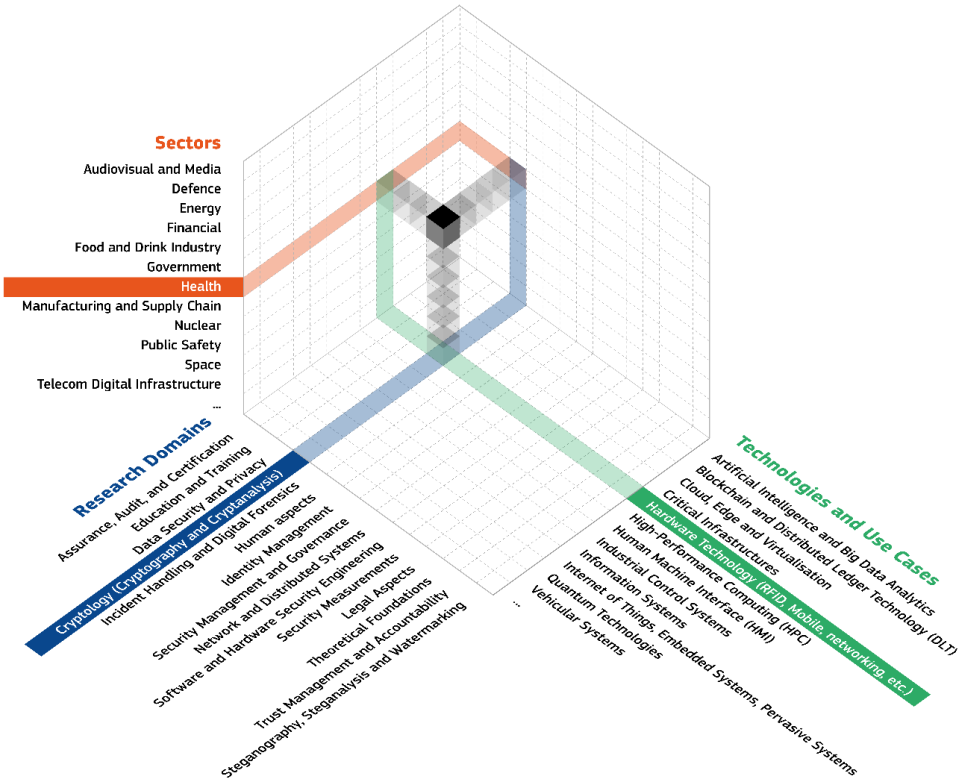

Figure 2: "High Level view of the Cybersecurity Taxonomy", Nai-Fovino et al., 2019, p. 28.

4.3 Common Taxonomy for Law Enforcement and The National Network of CSIRTs (Europol)

Europol, together with other participants, has developed a taxonomy for law enforcement and the national network of computer security response teams (the latter referred to as CSIRTs). The document was developed in the context of the EMPACT priority on cyberattacks. The purpose of the taxonomy is to classify incidents to support CSIRTs and public prosecutors in their dealing with LEAs in cases of criminal investigations (Europol et al., 2017 p.10).

The taxonomy consists of a template that addresses different classes of incidents (such as malware, intrusion, information security, and fraud). It also includes a description of each class. All classes of incidents are divided into types of incidents. For example, infection, distribution, command and control, and malicious connection relate to the incident class named "malware". A description of each type of incident is also provided, as well as the legislative framework which is related to the type of incident. See Figure 3 below.

Class of Incidents	Description of Class of Incidents	Type of Incidents	Description of Type of Incidents	Legislative Framework
Malware	Infection of one or various systems with a specific type of malware.	Infection	Malware detected in a system.	System(s) or software(s) infected with malware allowing remote access, monitoring of system activities and gathering of information: - Art. 2 and 6 [A] - Art. 3 and 6 [F]
		Distribution	Malware attached to a message or email message containing link to malicious URL or IP.	Dissemination of malware through various communication channels: - Art. 7 [F] - Art. 6 [A]
		Command & Control (C&C)	System used as a command-and-control point by a botnet. Also included in this field are systems serving as a point for gathering information stolen by botnets.	C&C server hosting: - Art. 2 and 6 [A] - Art. 4 and 7 [F]
	Connection performed by/from/to (a) suspicious system(s)	Malicious connection	System attempting to gain access to a port normally linked to a specific type of malware.	Connection to (a) suspicious system(s) or port(s) linked to specific malware: - N/A

Figure 3: "Taxonomy classification", Europol et al., at p. 10.

4.4 AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence (ENISA)

In 2020, the EU Agency for Cybersecurity (ENISA) published a report on AI Cybersecurity Challenges (ENISA, 2020). In the report, ENISA proposes one AI asset taxonomy and one AI threat taxonomy.

As part of the AI asset taxonomy, ENISA identifies and categorises assets that can be targeted by threats. The identified AI assets are classified in six categories: data, models, artefacts, actors/stakeholders, processes and environment/tools. For example, raw data, labelled data set, and public data set are linked to the asset category "data". ENISA also defines all assets and lists the AI lifecycle stages in which each asset belongs (ENISA, 2020). Part of the AI asset taxonomy is shown in Figure 4 below.

Figure 4: "AI asset taxonomy", ENISA, 2020, at p. 23.

As part of the AI threat taxonomy, ENISA presents seven main categories that are used to map AI threats. The categories are: Nefarious activity/abuse; Eavesdropping/Interception/Hijacking; Physical

attacks; Unintentional damages/accidental; Failures or malfunctions; Outrages; Disasters; and Legal. The AI threat landscape is organised under each of these categories (ENISA, 2020).

4.5 AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures (UNIDIR)

In a research report from United Nations Institute for Disarmament Research (UNIDIR), Ioana Puscas (2023) provides a taxonomy of risks related to AI technology.

The taxonomy classifies risks in two main categories: risks of AI technology and risks to global security. The former category includes the sub-categories safety risks, security risks, and human-machine interaction risks. These risks relate to the design, building and deployment of AI systems. The latter category include the sub-categories miscalculation, escalation, and proliferation. These risks are first and foremost related to the use of AI in the context of armed conflict and weapons use.

For ALIGNER, the taxonomy for risks of AI technology is most relevant. Puscas categorises the AI risks as shown in Figure 5 below. Each risk is described more thoroughly in the report.

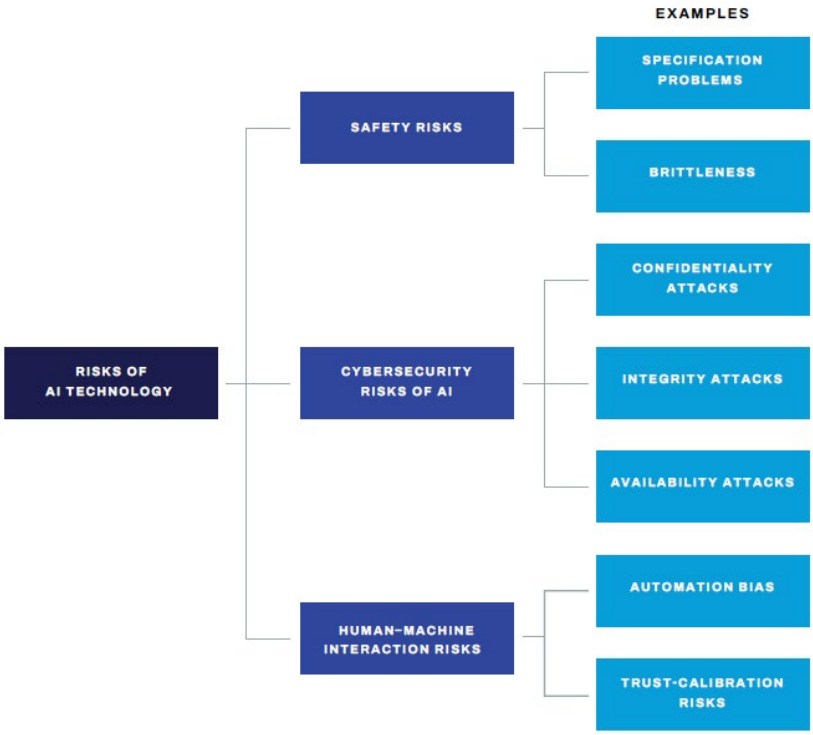

Figure 5: "AI risks Taxonomy", Puscas, 2023, at p. 11.

4.6 Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues (Dowoon Jeong)

In a research paper, Dowoon Jeong (2020) proposes a taxonomy for new types of crimes where AI is either a tool or a target (see figure 6). The taxonomy is based on a literature review and inspired by previous taxonomies of cybercrime where the computer was seen as either a tool or a target. AI as a target is considered a new area of crime where criminal actors target the AI, for example various adversarial attacks against AI. The category AI as tool includes, among others, enhancement of cybercrimes and security threats (Jeong, 2020).

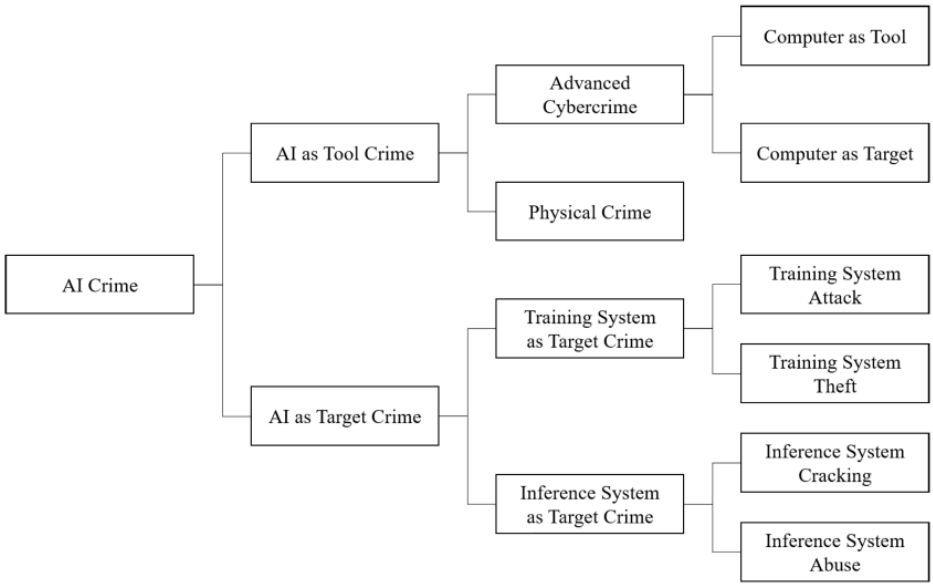

Figure 6: "The proposed taxonomy of the AI crime", Dowoon Jeong, 2020, at p. 5.

5. ALIGNER taxonomy for AI-supported crime

The ALIGNER taxonomy for AI-supported crime aims to be an instrument to categorise and describe potential threats of AI technology development. The taxonomy defines how AI theoretically can contribute to criminal actions, to support European LEAs in addressing AI-supported crimes and facilitate future prioritization of responses from the European LEAs, policy-makers, legislators, and the research community.

The ALIGNER taxonomy consists of three different templates that focus on three different threat categories. These threat categories are, as described in chapter 1.4., (1) AI, vehicles, robots and drones, (2) AI, crime and criminality in the digital domain, and (3) AI, disinformation and social manipulation.
As described in the introduction, we use the following definitions for AI-system, Crime, and AI-supported crime. 'AI system' is "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (European Commission, 2024). 'Crime' is "an act for which a penalty is prescribed by criminal law or regulation". (Britannica, 2024). 'AI-supported crimes' are "crimes that are enabled by use of AI" (Brundage et. al. 2018). In the taxonomy we use Cambridge's definition of threat as "a suggestion that something unpleasant or violent will happen, especially if a particular action or order is not followed" (Cambridge, 2023).

Each template is structured and divided into three categorisations: *threat*, description of *selection of potential crimes* and *examples of how AI may be used to support crime*. The last category consist of one selected example for each potential crime. The examples are not exhaustive. There are other situations in which AI can be used to support crime.

5.1 Threat category 1 - AI, vehicles, robots and drones

Threat category 1 - AI, vehicles, robots and drones		
THREAT	**SELECTION OF POTENTIAL CRIME**	**EXAMPLES OF HOW AI MAY BE USED TO SUPPORT CRIME:**
Weaponized or criminalized autonomous vehicles.	Terrorism	Commercial systems can be used in harmful and unintended ways, e.g. autonomous vehicles may deliver explosives and cause a terrorist attack.
	Traffic violation	Commercial systems can be used in harmful and unintended ways, e.g. autonomous vehicles may deliver explosives and cause crashes.
	Harmful explosion/Arson	Commercial systems can be used in harmful and unintended ways, e.g. autonomous vehicles to deliver explosives.

	Drug trafficking	Criminals may use autonomous vehicles for drug trafficking. For example, US law enforcement actors have discovered and seized autonomous underwater vehicles (AUVs) used for drug trafficking.
AI-controlled robots for harmful or malicious use.	Physical assault	AI-controlled robots can be used to carry out a physical attack. This may unlawfully cause, e.g., injury, damage or destruction.
	Harmful explosion/ Arson	Criminals may use military robotics research and its inventions to commit crimes. For example, robotics could be used to deliver explosives causing a harmful explosion/arson.
Weaponized or criminalized autonomous drones.	Harmful explosion/arson	Drones can be used in several harmful ways, whether originally designed for it or not. For example, drones can deliver explosives.
	Drug trafficking and/or drug dealing	Criminals can use drones for drug trafficking or drug dealing. They may also be used to facilitate smuggling.

5.2 Threat category 2 - AI, crime and criminality in the digital domain

Threat category 2 - AI, crime and criminality in the digital domain		
THREAT	**SELECTION OF POTENTIAL CRIME**	**EXAMPLES OF HOW AI MAY BE USED TO SUPPORT CRIME:**
Adversarial AI	Fraud & Forgery	Cybercriminals can use AI techniques to automate various tasks, such as dialogue with ransomware victims, payment processing and facilitate medical insurance fraud. For example, research have displayed how adversarial attacks in the healthcare sector can be carried out using co-opt diagnostic algorithms.
	Information theft/ Espionage	Cybercriminals can use AI techniques to steal information and expose it. By using “exploratory attacks” criminals can extract information (for example training data) from AI models.
	System interference	Attacks against machine learning can be used to commit system interference, e.g. “evasion attacks” which that are conducted by creating malicious inputs may generate a false prediction for the model.

	Breach of data secrecy	Criminals can use poisoning attacks (that aim to create backdoors in consumer machine learning and/or generate surreptitiously harm) to commit crimes such as data interference. Even small manipulations of algorithms or data sets can lead to substantial changes for how AI systems operate.
Denial of services (DDoS)	Breach of data secrecy	AI supported DDoS attacks may be used to target military, economic and educational infrastructure to withhold information.
Malware	Information theft	Criminals can use AI to create malware (malicious software), for example to obtain confidential information.
	Extortion	Criminals can use AI to create ransomware (a type of malware) to extort money from victims, but can also be used with destructive or disruptive purposes as seen in the NotPetya attack in 2017[3].
	Sabotage	Criminals can use AI to create malware worms to sabotage infrastructure and operative systems. This was done in the case of Stuxnet, 2010.
Fake news	Improper activity at election	Fake news reports with realistic fabricated audio and video of state leaders can be interpreted as realistic causing people to act or vote differently than otherwise. For example, deep fakes of candidates for elections may impact the outcome of the voting where the technique can be used to undermine confidence in the individual politician or party they represent.
	Incitement of violence	Fake news reports can be used to fabricate politicians that incite people to act in a harmful way. This could for example lead to situations like the Capitol riots in January 2021.
Social engineering attack	Swindling	Phishing attacks can be improved by using AI to construct messages that appear more genuine. AI techniques can be used for active learning to discover the work that will result in maximized responses by varying the details of messages to gather data. The scalability and frequency of an attack can be improved by e.g. spear phishing where AI can create more effective and extensive attacks.
	Fraud & Forgery	A victim's online information is used to automatically generate custom malicious websites/emails/links the victim would be likely to click on, so called spear phishing. The communication is sent from addresses that impersonate their real contacts, using a writing style that mimics those contacts.

[3] https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/ [accessed 2024-06-18]

Password guessing	Information theft	AI can be used to expedite, enhance and automate the process of password guessing. By obtaining passwords and access protected websites, malicious actors can enter systems or networks, to create disruption, disrupt essential services, steal information and/or data, manipulate data or processes or install malicious software.
CAPTCHA breaking	Breach of data secrecy	CAPTCHA is a security measure used to protect networks and websites from various attacks. Criminals can carry out cyberattacks by using AI to overcome CAPTCHA.
Market bombing	Swindling	AI can be used to manipulate financial or stock markets via targeted, high frequency, patterns of trades, to harm currencies, competitors or the economic system. A side effect can also be that AI creates profit from trading even if that is not the direct yield.
AI supported crypto currency trading	Fraud & Forgery	AI can manipulate cryptocurrency for financial profit.
	Theft	Criminals could facilitate theft of cryptocurrencies by using AI techniques.
Tricking face recognition	Identity fraud	AI systems are used for face recognition which could be used as ways of tricking identification systems resulting in identity fraud.
Online stalking	Persecution	AI can improve discovering and monitoring individuals' activities and through personal device data or social media. This increases the possibility to stalk the targeted individuals.
Automated surveillance platforms to suppress dissent.	Violation of human rights	States may use automated audio and image processing to extend state surveillance in an unproportionate way or to suppress debate.

5.3 Threat category 3 - AI, disinformation and social manipulation

Category 3 = AI, disinformation and social manipulation		
THREAT	**SELECTION OF POTENTIAL CRIME**	**EXAMPLES OF HOW AI MAY BE USED TO SUPPORT CRIME:**
Data extraction	Extortion	Systematic efforts to harvest data about companies, individuals and the government may be used for tracking, manipulation and extortion.

AI deep fakes	Improper activity at election	Deep fakes may be used to misinform the public. For example, it may be used to create fake emergency alerts, and to influence politics and elections (i.e. by releasing fake audio or video recordings of political figures).
	Nonconsensual pornography' and child pornography	Criminal use of deep fakes as child pornography and/or non-consensual pornography.
	Extortion	Criminals and/or terrorist groups may use deep fakes to trick, threaten and extort people to raise funding. Criminals can also use deep fakes to trick people in critical positions to collect and reveal classified, confidential or personal information.
	Incitement of violence	Deep fakes can be used to fabricate politicians that incitements people to act in a harmful way. This could for example lead to situations like the Capitol riots in January 2021.
	Information theft	Criminals and terrorists may use deep fakes to impersonate people in critical positions to obtain critical and perhaps confidential or classified information.
Biometric spoofing	Identity theft	Biometric uses attributes such as voice, fingerprints and handwriting to identify individuals. Today, verification of people having access to phones, buildings etc. is possible with the use of biometrics. Criminals may create new biometrics samples to hack systems or to generate spoof handwriting or synthetic fingerprints.
Fake evidence	Extortion	AI may be used to automatically collect evidence or produce fake evidence to up-scale extortion.
Influence campaigns.	Incitement of violence	AI can contribute to an increased spread of terrorist or violent narratives that can incite people to act in a harmful way.
Information campaigns.	Incitement of hate speech	AI can make information operations more scalable, precise and persistent. Malign information is already an existing problem, but can be aggravated with use of AI. For example, AI can be used to manipulate content or produce content to manipulate messages and spread malign information by embedding AI into different platforms. The information can be used to incite people to act in a harmful way.
Denial-of-information attacks	Fraud & Forgery	AI supported Bot-driven, large-scale information-generation attacks can be used to making it more difficult to obtain correct information. The attacks may be used to target military, economic and educational infrastructure to make correct and vital information harder to access.

Social engineering attack	Fraud & Forgery	A victim's online information can be used to automatically generate custom malicious websites/emails/links the victim would be likely to click on, so called spear phishing. The communication is sent from addresses that impersonate their real contacts, using a writing style that mimics those contacts.
	Swindling	Phishing attacks can be improved by using AI to construct messages that appear more genuine. AI techniques can be used for active learning to discover the work that will result in maximized responses by varying the details of messages to gather data. The scalability and frequency of an attack can be improved by e.g. spear phishing where AI can create more effective and extensive attacks.
Fake news	Incitement of violence	Fake news reports can be used to fabricate persons that a victim trust. For example, fake news can incite people to act in a harmful way.
Hacking	Breach of data secrecy	The computerization of diverse fields, from finance to elections, increases the speed, scale, and scope of vulnerability to hacking. AI can be used to evade detection, improve target selection, improve prioritization, and creatively respond to changes in the target's behavior. For example, AI can be used to destruct and disclose personal data.

6. Forecast

6.1 Introduction to the Study

The objective of this chapter is according to T3.4 to provide the forecast evaluating the probabilities and trajectories of AI integration into various criminal activities. This assessment aims to assist European LEAs, policy-makers, legislators, and researchers in prioritizing future responses.

Additionally, this chapter seeks to validate the taxonomies introduced in previous sections of D3.3 and inform future research, c.f. WP5. This study combines an examination of survey respondents' beliefs regarding future trajectories with empirical testing and validation of the taxonomies presented in in chapters three and five.

An academic future forecast involves predicting future trends or outcomes based on current data and theoretical frameworks. Dan-Suteu & Giorgi (2019) distinguish between "forecast" and "forecasting" by highlighting their respective roles in future studies. While "forecast" refers to a specific prediction or assessment of future probabilities and trajectories, "forecasting" encompasses the broader process of generating these forecasts. Forecasting involves various methods and techniques for analysing data, identifying trends, and making informed predictions about future events or outcomes. In essence, "forecasting" serves as the overarching process, while "forecast" represents the tangible outcome or result of this process. In that context, this study is the process of forecasting, to produce a forecast.

6.2 Main Theory and Literature for This Study

The main theories for this sub-study within the larger D3.3 include the central taxonomies presented in chapters three and five and the previously cited theoretical work undertaken to produce it. Additionally the theory for this empirical part of the D3.3 was inspired by the Technology Acceptance Model (TAM) as presented by e.g. Davis (1989). For a more current review of the TAM see Marangunić & Granić (2015). The TAM is one of the most influential extensions of Ajzen and Fishbein's theory of reasoned action (Fishbein & Ajzen, 1975), (for a more current review of the theory of reasoned action see Montano & Kasprzyk, 2015).

One of the main constructs in the TAM is the degree to which a person believes that using a particular new technological system would enhance their job performance, “job performance” here indeed somewhat morally dubiously being understood as criminal acts. It means whether or not someone, in our case a criminal, perceives that technology, in this case AI-services, to be useful for what that someone wants to do in a professional capacity.

Another central construct of the TAM is the perceived ease of use (PEOU). This is the degree to which a person believes that using a particular new technological system, in this case AI-systems, would come with only little initial learning effort.

In earlier research it can be noted that Mohr & Kühl (2021), applied the TAM to study what behavioural factors guide adoption of AI in German agriculture. It can also be noted that Wang et al. (2023) applied the TAM to study the adoption of AI in e-commerce. It is also relevant for this study how Xu & Wang (2021) applied the TAM to explore the relationship between “AI-robot lawyers” and human lawyers, and then to out of that, identify the elements of AI robot lawyers that can be accepted by human users for legal advice. The mentioned studies have been inspirational for this study.

6.3 Research Design

The research design is to employ a survey to empirically validate or reject the taxonomies presented in earlier chapters and explore the structures of beliefs about the near future developments of crime in relation to AI-services, i.e. the forecast of T3.4. In this way, this study combines an element of positivist theory testing of the taxonomies, with an exploratory approach aiming to uncover nuanced insights into driving forces and future trajectories for use as basis for the forecast.

Due to the unavailability of direct data from criminals regarding their near-future plans for using AI-services, this study conducted a survey with the participants on the two ALIGNER advisory boards[4], about their beliefs regarding the near future development of AI as a tool for criminals. This epistemological choice reflects a pragmatic approach to knowledge gathering in a field where direct data from primary sources, i.e. the criminals, is unattainable, while respecting the extra layer of interpretation necessary when drawing conclusions from the study.

This approach presumes that the expertise and informed perspectives of law enforcement officers can act as proxy respondents for criminals, providing valuable insights into the anticipated trajectory of near future criminal use of AI.

Empirical testing of this kind helps in verifying whether the theoretical constructs and literature presented in this deliverable align, with a small-scale real-world observation and so gives an indicative though not definitive, measurement into to what extent the constructs and literature of this D3.3 can inform future studies and practical implementations.

Bridging the gap from theory building to empirical validation requires careful consideration. Still such empirical validation is a crucial step for ALIGNER as it tests the robustness and applicability of these D3.3 taxonomies as theoretical constructs for the roadmap of WP5.

The survey items were not randomized. We are aware that a degree of ordering bias in surveys can occur when the sequence of questions influences responses, e.g. through a degree of psychological “priming”. However, for tasks like validating a new taxonomy, it was necessary to have a fixed order to maintain the logical progression and integrity of the hierarchical structures of the taxonomy. Randomization may have disrupted this process, compromising the taxonomy validation's internal consistency. Thus, a fixed order ensures methodological rigor and the accurate assessment of the proposed taxonomy's validity.

6.4 Research model and hypotheses

This research aims to develop a causal model that serves as the basis for forecasting and provides a modicum of empirical validation for the proposed taxonomies. The research model, depicted in Figure 7, underpins the formulation of nine hypotheses, which were subsequently examined through the empirical study. The manifest variables were inspired by the TAM as referenced earlier; it was not practical to use the model in its entirety. Some items were developed new for this study, as chronicled below. The survey items are to be found in Annex 2. The survey has a scale of four choices. This ensures that respondents are compelled to provide a definitive stance on each item. Taking away the central tendency bias inherent in scales with a neutral midpoint enhances the precision of the validation process by distinguishing between different levels of agreement or disagreement, which is essential for accurately assessing the robustness and clarity of the proposed taxonomy. Also; in exploratory forecasting, a four-choice scale offers a more discriminative feedback, as the forced decision-making process inherent in a four-choice scale aids in the identification of clear preferences and potential divergences in forecast projections, enhancing the reliability and interpretability of the exploratory findings of this study.

[4] https://aligner-h2020.eu/getting-involved/

6.4.1 Research constructs: Perceived ease of use (PEOU) & perceived usefulness (PU).

Prior research has established that PEOU and PU can significantly influence the behavioural intention to adopt digital media products (e.g., Venkatesh & Davis (2000) or Naseri et al. (2023)), hence they are applied in this research model.

Research constructs: ATC1-3

The research model also includes the three ALIGNER Threat Categories (ATC), from chapters three and five. ATC1 being the sub-taxonomy for weaponized or criminalized autonomous vehicles; ATC2 being the sub-taxonomy for AI, crime and criminality in the digital domain, and ATC3 being the sub-taxonomy for AI, disinformation and social manipulation. These constructs are new for this study. They are in the research model theorized to be valid constructs and also, as plural valid constructs have plural differing impacts on beliefs about causally downstream constructs.

Research constructs, Sense of Urgency & Behavioural Intention to Use (SU-BIU).

The ALIGNER taxonomies and the forecast involve multifaceted constructs such as types of AI technologies, and legal and ethical issues, beliefs about near future development all defined by multiple indicators. Henceforth the theory for this empirical study was developed inductively in iterations.

E.g. project-internal theory workshops came up with the thought that there was a need for the survey and its ensuing causal model to gauge the European LEAs sense of urgency about the development of criminality and AI-services. This sense of urgency was initially intended to be a separate construct measuring the degree to which the respondents feel that European LEAs need to prepare right now, for the criminals “uptake of AI in the near future”. This construct was developed into two separate survey items, which were face validated with project-internal experts on the topic and added as a latent variable separate from the TAM-inspired “behavioural intention to use” latent variable.

The final dependent construct in the research model was at first made up of four survey items inspired by the TAM construct “behavioural intention to use”, representing the extent to which the respondents, i.e. the LEA-officers believed that criminals intends to use AI-services. Within the TAM framework, the construct "intention to use" embodies an individual's propensity to adopt technology based on perceived usefulness and ease of use.

Likewise, "sense of urgency" can be expected to impact "intention to use" by instigating a compelling need for swift action, heightening the technology’s perceived importance and immediacy.

Initial analysis runs with partial least squares structural equation modelling then showed that the Heterotrait-Monotrait (HTMT) values used to assess discriminant validity between the new “sense of urgency” and the TAM-inspired “behavioural intention to use” constructs indicated that in the eyes of the respondents these two were perceived as quite similar.

In response, we refined our research model with new theory by merging these two latent variables, into one, which subsequently improved the overall fit and resolved the HTMT issue.

Our research underscores the inductive nature of theory development, pivotal in explorative contexts. This iterative process, involving continual refinement through partial least squares structural equation modelling test runs, culminated in our final research model. This method adheres to partial least squares structural equation modelling academic standards, ensuring the robustness and validity of our findings. Examples from studies like those by Swinyard & Smith (2003) and Hair et al. (2011) illustrate the efficacy of iterative theory development in partial least squares structural equation modelling , affirming its legitimacy.

Consequently, a strong sense of urgency among respondents may translate into a heightened intention to use the technology, perceiving it as a vital and immediate solution to pressing concerns, all in all making it motivated to merge these into one construct.

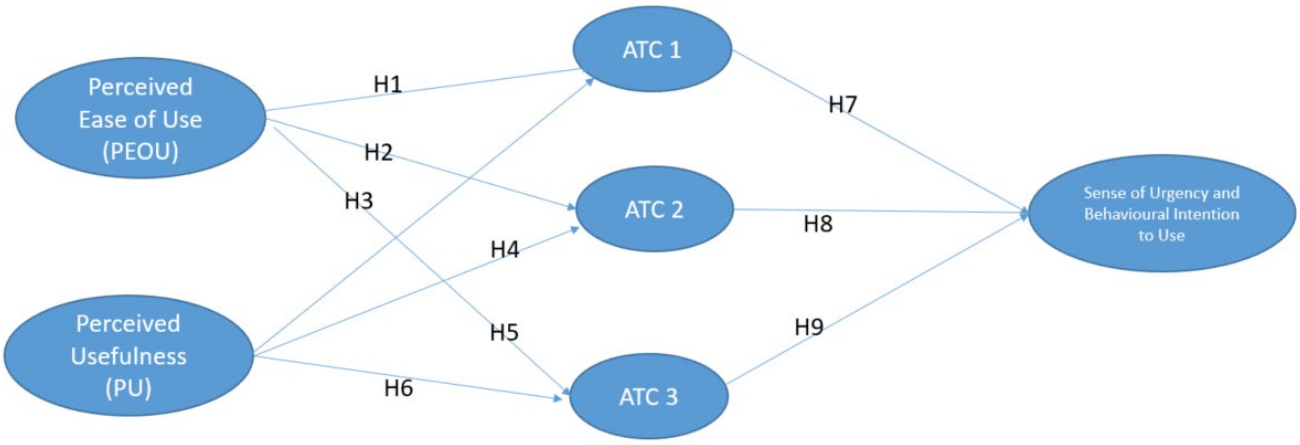

Figure 7: hypothesized model

In the research model, the impact of the belief in perceived usefulness and ease of use is filtered through the beliefs in the intermediate constructs ATC 1-3 and sense of urgency.

Based on previous research the hypotheses include the following:

H1-3: PEOU predicts how the respondents perceive the degree of severity of each the three ATCs.

H 4-6: PU predicts how the respondents perceive the degree of severity of each the three ATCs.

H7-9 the three ATC will to differing degrees impact the final dependent construct or latent variable, - the combined sense of urgency and (beliefs about the criminals) behavioural intention to use.

6.4.2 Method & Process

The survey was conducted during Q1 and Q2 of 2024 applying an online survey tool[5]. The survey was emailed to all 66 participants in the two ALIGNER advisory boards, with two e-mailed reminders and one reminder spoken out loud at an online workshop the project held in May 2024. Altogether, 51 responses were gathered making up a response rate of 77%. Among the respondents 16 worked in research and academia with these topics, 19 worked in law enforcement and policing, 5 in other public agency, 4 in other and the rest preferred not to say. Sixty percent had more than 10+ years in their field of work and median of five years of being aware of issues in the meeting of artificial intelligence, law enforcement and crime.

The sampled group is of course only representative for the members of the ALIGNER advisory boards. Still, we argue from a pragmatist and critical realist point of view that the ALIGNER advisory boards have such a composition that the insights from such groups' informed beliefs and professional judgments provide a degree of indicative ecological validity to the study.

The data gathered in the data collection phase was analysed with Partial Least Square Structural Equation Modelling[6]. That analysis approach is particularly useful when exploring experiences and beliefs as it allows for the use of smaller sample sizes and can with holistic interpretation provide robust insights even with limited or non-ideal data, such as is the case in this study. This is considered "soft modelling" as it is a flexible analytical technique that is adaptable to less rigid data structures and assumptions, while still being capable of handling complex causal relationships cf. Hair et al., (2013).

[5] www.netigate.se [Accessed 2024-08-05]
[6] For the software used see: https://www.smartpls.com/ [Accessed 2024-08-05]

Hypothesis Testing:

Partial least squares structural equation modelling facilitated the testing of hypotheses 1-9, (cf. fig 7). By examining path coefficients and their significance, we could determine whether the hypothesised relationships between constructs were supported by the empirical data.

The steps in this analysis are:

First; specify the structural model: This step involves defining the hypothesized relationships between the constructs in the taxonomy, the TAM and the "degree of urgency" construct, cf. fig 7.

Then comes model estimation: partial least squares structural equation modelling uses a variance-based approach to estimate the parameters of the model based on the survey data. This involves letting the PLS algorithm calculate the relationships between constructs and their indicators, this a process where the survey questions (manifest variables) with theory are aggregated into theoretical clusters called "latent variables" (outer model), and then the relationships between the constructs/latent variables themselves, (inner model).

Model validation and assessment: This step involves assessing the reliability and validity of the constructs. Convergent and discriminant validity, composite reliability, and goodness-of-fit indices are examined to ensure the model accurately represents and tests the theoretical taxonomy in relation to TAM. For instance, the validity of the indicators representing AI technology categories in relation to categories of crime are assessed.

6.4.3 Findings and discussion

The results section will detail the findings from the empirical testing and survey, highlighting the key trends and insights regarding the future integration of AI into criminal activities and the implications for European LEAs. This study applied the SmartPLS analysis tool[7]. The evaluation of the measurement model includes checking for the reliability and validity of the latent variables (Hair et al., 2013). For an explanation of the terminology in this chapter, see Annex 3.

Measurement model assessment

Reliability and validity were tested using the Cronbach's alpha composite reliability and measures for average variance extracted (AVE). Hair et al. (2013) recommended the measurement of the values of convergent and discriminant validities to test the validity. These measures should preferably have values greater than or equal to 0.70 (Hair et al., 2013). Table 1 reveals the results, indicating adequate reliability and validity since the tested measures showed satisfactory values for all latent variables, except for the PEOU construct, which had a Cronbach's alpha of 0.52, indicating a somewhat weaker reliability. However, the composite reliability and AVE values for this construct are stronger, balancing the overall assessment. Convergent validity was tested by determining the values of the AVE.

Acceptable values for AVE are ≥ 0.50 (Fornell & Larcker, 1981), and acceptable values for factor loadings are ≥ 0.70 (Hair, Black Jr., Babin, & Anderson, 2010).

Table 1 also shows that the AVE values met the acceptable thresholds, thus confirming convergent validity.

[7] For the software used see: https://www.smartpls.com/ [Accessed 2024-08-05]

	Cronbach's alpha	*Composite reliability (rho_a)*	*Composite reliability (rho_c)*	*Average variance extracted (AVE)*
ATC1	0.81	0.82	0.87	0.56
ATC2	0.89	0.92	0.91	0.65
ATC3	0.87	0.90	0.90	0.57
PEOU	0.52	0.77	0.76	0.50
SU-BIU	0.91	0.92	0.93	0.70
PU	0.90	0.92	0.93	0.76

Table 1: reliability measures, c.f. Annex 3.

Henseler, Ringle, and Sarstedt (2015) recommended testing the discriminant validity of latent variables, i.e., the extent to which they represent distinct and separate concepts, by determining the HTMT values of correlations. Acceptable values for HTMT can be between 0,85-0,91.

	ATC1	***ATC2***	***ATC3***	***PEOU***	**SU-BIU**	***PU***
ATC1						
ATC2	0.68					
ATC3	0.67	0.80				
PEOU	0.34	0.53	0.36			
SU-BIU	0.52	0.79	0.62	0.75		
PU	0.31	0.53	0.51	0.63	0.76	

Table 2: HTMT matrix, c.f. Annex 3.

The HTMT matrix table in partial least squares structural equation modelling shows the HTMT ratio of correlations between latent variables, which is used to assess discriminant validity. Discriminant validity indicates the extent to which a construct is truly distinct from other constructs by empirical standards. The HTMT ratio is calculated as the average of the heterotrait-hetero-monotrait correlations (i.e., correlations between indicators across different constructs) divided by the average of the monotrait-heterotrait correlations (i.e., correlations between indicators within the same construct).

Hypotheses testing and coefficient of determination

The structural equation modelling (SEM) approach was used to test the nine hypotheses above together as a path model. The variance described (R2 value) by each path and every hypothesized connection's path significance in the research model were assessed. The standardized path coefficients and path significances are demonstrated in Fig. 8, and the R Square values in Table 3.

	R-square	R-square adjusted
ATC1	0.10	0.06
ATC2	0.34	0.31
ATC3	0.26	0.22
SU-BIU	0.54	0.51

Table 3: R-Square values of the endogenous latent variables, c.f. Annex 3

The final R-square value of 0.51-0.54 for the latent variable SU-BIU can be seen as a good result with a medium to high predicative power for the end latent variable.

All constructs were verified in the model. The results showed that PU influenced ATC2 (β= 0.34) and ATC 3 supporting (β= 0,44) supporting respective hypotheses.

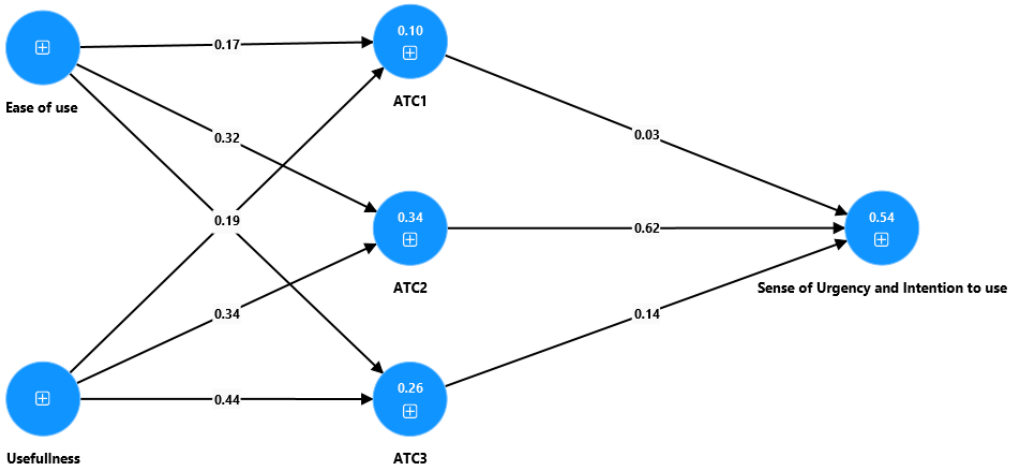

Figure 8: path test of the research model

H	Formulation	Beta-Value	Confirmed or rejected
H1	PEOU predicts how the respondents perceive the degree of severity of ATC1.	0,17	Rejected
H2	PEOU predicts how the respondents perceive the degree of severity of ATC2	0,32	Confirmed
H3	PEOU predicts how the respondents perceive the degree of severity of ATC3	0,10	Rejected
H4	PU predicts how the respondents perceive the degree of severity of ATC1	0.19	Rejected
H5	PU predicts how the respondents perceive the degree of severity of ATC2.	0,34	Confirmed
H6	PU predicts how the respondents perceive the degree of severity of ATC3	0,44	Confirmed
H7	ATC1 will impact the final dependent latent variable SU-BIU	0.03	Rejected
H8	ATC2 will impact the final dependent latent variable SU-BIU	0.62	Strongly Confirmed
H9	ATC3 will impact the final dependent latent variable SU-BIU.	0,14	Rejected

Table 4: ..Hypotheses table .

What is to be considered a strong confirming result or a weak rejecting result does not have a definitive norm. It can vary a lot between research contexts. For the sake of this study, we can take a beta value of 0.3 as a minimum. VIF-values ranged from 1.17 – 4, 61 with an average of 2,759, indicating little problems with collinearity. Of the goodness-of-fit-measures, SRMR was 0,1 - 0,17, d_ULS, 5,94 – 16,31 d_G 4,95 – 5,5 and NFI 0,49 – 1,46, which are acceptable values.

Chi-square GOF or bootstrapping was not applied due to the small sample size. This because the small sample size can significantly impact the reliability and validity of significance values in statistical analyses, including partial least squares structural equation modelling. When the sample size is so small as it is in this study the estimates of standard errors tend to be larger, which in turn makes it more difficult per se to achieve statistically significant results. Smaller samples contain less mathematical information and are hence by themselves more prone to sampling variability, undermining the stability and accuracy of the parameter estimates and their associated significance tests (Maxwell et al., 2008).

6.5 Forecast Based on the Test of the Model

The test of the model provides valuable insights for forecasting future criminal uses of AI. Notably, all three ATCs sub-taxonomies demonstrated high reliability and validity, accompanied by moderate R^2-values despite being intermediate latent variables. This finding validates the ALIGNER taxonomy of D3.3 as a robust construct for subsequent research within the WP5 roadmap.

Future Trajectories of AI-assisted Crime

The results indicate that PU and PEOU significantly influence perceptions of AI's severity in criminal activities. Additionally, the ATCs impact the perceived urgency and intention to utilize AI services for criminal purposes. These findings underscore the necessity for proactive measures by LEAs to address emerging threats posed by AI-enabled crime. Future forecasting models must incorporate these factors to develop effective strategies for mitigating risks associated with criminal AI integration.

Severity of AI Threats by Category

ATC1: AI, Vehicles, Robots, and Drones

The study reveals that neither PEOU nor PU predicts the perceived severity of ATC1. This suggests that the use of AI in vehicles, robots, and drones might occur regardless of its perceived usefulness, or it may not be perceived as a significant threat. This is corroborated by the minimal impact of ATC1 on the final dependent latent variable SU-BIU, indicating that ATC1-related threats are not expected to be severe in the near future.

ATC2: AI, Crime and Criminality in the Digital Domain, and Online Cyber Crime

The findings show that PEOU does predict how respondents perceive the severity of ATC2, indicating that the perceived ease of use of AI tools significantly influences the perceived threat level of digital and online cyber-crimes. Additionally, PU also predicts the perceived severity of ATC2, suggesting that the usefulness of AI tools is a critical factor in determining the severity of these crimes. This is further confirmed by the significant impact of ATC2 on the final dependent latent variable SU-BIU, highlighting ATC2 as a severe threat in the near future.

ATC3: AI, Disinformation, and Social Manipulation

The study finds that while PU predicts the perceived severity of ATC3, PEOU does not. This indicates that the perceived usefulness of AI tools for disinformation and social manipulation is crucial in determining the severity of this crime category. However, ATC3 does not significantly impact the final dependent latent variable SU-BIU, suggesting that despite its potential usefulness, ATC3 is not expected to pose a severe threat in the near future.

Implications for Law Enforcement and Policy

These insights necessitate a strategic approach for LEAs to prioritize resources and interventions. Focusing on categories where perceived usefulness and ease of use are significant predictors can help in anticipating and mitigating future AI-assisted crimes. Moreover, continuous monitoring and updating of these forecasting models will be essential to address the evolving landscape of AI and crime effectively.

In conclusion, while some ATCs are perceived as more severe near-future threats than others, targeted strategies based on these perceptions will be crucial in shaping effective responses to AI-assisted crime.

7. References

Bauer L. A. & Bindschaedler, V (2017). ”Generative Models for Security: Attacks, Defenses, and Opportunities”. University of Florida, USA. Retrieved 2024-01-12 https://arxiv.org/pdf/2107.10139v2.pdf

BBC News (2022). “Drug smuggling: Underwater drones seized by Spanish police”. Published 4 July 2022. Available at https://www.bbc.com/news/world-europe-62040790

BBC News (2023). “AI bot capable of insider trading and lying, say researchers”. Published 3 November 2023. Available at https://www.bbc.com/news/technology-67302788

BBC News (2024). “Fake Biden robocall tells voters to skip New Hampshire primary election”. Published 22 January 2024. Available at https://www.bbc.com/news/world-us-canada-68064247
Brundage, M. et. al. 2018. “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation”. https://doi.org/10.48550/arXiv.1802.07228

Busch, E. & Ware, J. (2023). “The Weaponisation of Deepfakes Digital Deception by the Far-Right”. International Centre for Counter-Terrorism (ICCT. https://www.icct.nl/sites/default/files/2023-12/The%20Weaponisation%20of%20Deepfakes.pdf

Caldwell, M. Andrews, J. T. A. Tanay. T. and Griffin, L. D. (2020). “AI-enabled future crime”. In *Crime Sci* (2020) https://doi.org/10.1186/s40163-020-00123-8
Chesney, B. & Citron, D. (2019). “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. Retrieved 2024-01-11. DOI: https://doi.org/10.15779/Z38RV0D15J

Cambridge dictionary (2024). “Threat”. Retrieved 2024-01-30.
https://dictionary.cambridge.org/dictionary/english/threat#google_vignette

Christensen. L., Fernández. J. G, Hildebrandt M. & Koch, C. E. S (2022). “Recent Advances in AI for Navigation and Control of Underwater Robots”. In, *Current Robotics Reports* 3:165–175. Retrieved 2024-01-12 https://link.springer.com/article/10.1007/s43154-022-00088-3

Dan-Suteu, S.-A., & Giorgi, G. (2019). Future Studies, Forecast and Foresight—Critical Considerations and Relevant Findings. The International Scientific Conference eLearning and Software for Education, 1, 130–137. https://doi.org/10.12753/2066-026X-19-017

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

Ellis-Petersen H. & Hassan, A. (2023). ” Wave of drug-carrying drones flying into India from Pakistan, officials say”. In, *The Guardian*. Published 27 December 2023. Available at https://www.theguardian.com/world/2023/dec/27/wave-of-drug-carrying-drones-flying-into-india-from-pakistan-officials-say?ref=upstract.com

Encyclopedia Britannica (2023). ”Incitement – criminal law”. Retrieved 2024-01-30 https://www.britannica.com/topic/incitement

Encyclopedia Britannica (2024). ”Crime summary”. Retrieved 2024-01-30.
https://www.britannica.com/summary/crime-law#:~:text=crime%2C%20the%20intentional%20commission%20of%20an%20act%20usually,specifically%20defined%2C%20prohibited%2C%20and%20punishable%20under%20criminal%20law.

ENISA (2020). “AI CYBERSECURITY CHALLENGES Threat Landscape for Artificial Intelligence”. Retrieved 2024-01-08. DOI 10.2824/238222

EUR LEX (2002). “EU rules on terrorist offences and related penalties”. Retrieved 2024-01-25. https://eur-lex.europa.eu/EN/legal-content/summary/eu-rules-on-terrorist-offences-and-related-penalties.html

EUR LEX (2004). “Criminal acts and the applicable penalties — drug trafficking”. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14153

EUR LEX (2017). “Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law”. *Article 3(2) of Directive (EU) 2017/1371.* Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017L1371

EUR LEX, 2023. “Criminal acts and the applicable penalties — drug trafficking”. Retrieved 2024-01-25. Available at https://eur-lex.europa.eu/EN/legal-content/summary/criminal-acts-and-the-applicable-penalties-drug-trafficking.html

European Commission (2005). “Women and Science: Excellence and Innovation - Gender Equality in Science”. *Commission Staff Working Document*, SEC (2005) 370, 11 March 2005. Retrieved from https://data.consilium.europa.eu/doc/document/ST-7322-2005-INIT/en/pdf.

European Commission (2024). “Artificial Intelligence Act”. Retrieved 2024-06-19 Texts adopted - Artificial Intelligence Act - Wednesday, 14 June 2023 (europa.eu)

Europol (2017). “Common Taxonomy for Law Enforcement and the National Network of CSRITs”. Version 1.3, December 2017, Europol Public Information. Retrieved 2024-01-25. Available at https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf

Europol (2022). “EU Policy Cycle – EMPACT”. Retrieved 2024-01-22. Available at https://www.europol.europa.eu/crime-areas-and-statistics/empact

Europol (2023). “The EU's fight against organized crime”. Retrieved 2024-01-22. Available at https://www.consilium.europa.eu/en/policies/eu-fight-against-crime/#priorities

Financial times (2024). “AI heralds the next generation of financial scams”. Published 19 January 2024. Available at https://www.ft.com/content/beea7f8a-2fa9-4b63-a542-88be231b0266

Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. Addison-Wesley.

Giansiracusa, N., & Panditharatne, M. (2023, July 21). “How AI Puts Elections at Risk—And the Needed Safeguards”. *Brennan Center for Justice*. https://www.brennancenter.org/our-work/analysis-opinion/how-ai-puts-elections-risk-and-needed-safeguards

Gillespie, A., Glăveanu, V., & de Saint Laurent, C. (2024). *Pragmatism and methodology: doing research that matters with mixed methods*. Cambridge University Press.

Goldstein, J. A., Sastry, G., Musser, M. DiResta, R., Gentzel, M. & Sedova, K. (2023). Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations. https://arxiv.org/pdf/2301.04246.pdf

Hair, J. F., M, T. H., Ringle, C. M., & Sarstedt, M. (2013). A primer on partial least squares structural equation modeling (PARTIAL LEAST SQUARES STRUCTUAL EQUATION MODELLING). (1st ed.). SAGE.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2011). An assesment of the use of partial least squares structural equation modeling in marketing research. Journal of the Academy of Marketing Sciences., 40, 433.

Hayward K. J. & Maas, M. M. (2020). “Artificial intelligence and crime: A primer for criminologists”. In *Crime Media Culture 1–25.* Retrieved 2024-01-08. https://doi.org/10.1177/1741659020917434

Ingram, D. (2024). “U.S. tech companies prepare for potential drone attacks as international strikes spark concern”. In *NBC News*. Retrieved 2024-01-30. https://www.nbcnews.com/tech/security/flip-side-drone-boom-airports-stadiums-power-plants-need-defending-rcna128248

Jackman, A. & Hooper, L (2023). “Drone incidents and misuse: Legal considerations”. University of reading. Retrieved 2024-01-30 https://research.reading.ac.uk/drone-geographies/wp-content/uploads/sites/271/2023/12/Drone-incidents_Jackman-Hooper.pdf

Jeong, D. "Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues," in *IEEE Access*, vol. 8, pp. 184560-184574, 2020, doi: 10.1109/ACCESS.2020.3029280.

King. T. C., Aggarwal. N., Taddeo. M. & Floridi, L (2020). “Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions”. In *Science and Engineering Ethics*. Retrieved: 10 April 2018. https://doi.org/10.1007/s11948-018-00081-0

Klein, N. (2022). “Narco-drones are the newest form of drug trafficking: Our laws aren’t yet ready to combat them”. In, *Policinginsight.com*. Retrieved 2024-01-12 https://policinginsight.com/feature/analysis/narco-drones-are-the-newest-form-of-drug-trafficking-our-laws-arent-yet-ready-to-combat-them/

Lückerath, D. (2021). “ALIGNER D1.2 – Project Handbook”. ALIGNER – Artificial Intelligence Roadmap for Policing and Law Enforcement. European Commission.

Macleod, N. (2023). “Intentionally Encouraging or Assisting Others to Commit an Offence: The Anatomy of a Language Crime”. In: *International Journal for the Semiotics of Law*. Retrieved 2024-01-12 https://doi.org/10.1007/s11196-023-10031-0

Mahmud, A. (2023). ”Application and Criminalization of Artificial Intelligence in the Digital Society: Security Threats and the Regulatory Challenges”. In, *Journal of applied security research*. Retrieved 2024-01-30 https://doi.org/10.1080/19361610.2021.1947113

Marangunić, N., & Granić, A. (2015). Technology acceptance model: A literature review from 1986 to 2013. Universal Access in the Information Society, 14(1), 81–95. https://doi.org/10.1007/s10209-014-0348-1

Maxwell, S. E., Kelley, K., & Rausch, J. R. (2008). Sample Size Planning for Statistical Power and Accuracy in Parameter Estimation. Annual Review of Psychology, 59(Volume 59, 2008), 537–563. https://doi.org/10.1146/annurev.psych.59.103006.093735

Mohr, S., & Kühl, R. (2021). Acceptance of artificial intelligence in German agriculture: An application of the technology acceptance model and the theory of planned behavior. Precision Agriculture, 22(6), 1816–1844. https://doi.org/10.1007/s11119-021-09814-x

Montano, D. E., & Kasprzyk, D. (2015). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. In Health Behavior: Theory, Research, and Practice (5th ed., pp. 96–

124). Jossey-Bass.

Nai-Fovino. I., Neisse. R., Hernandez-Ramos. J. L., Polemi. N., Ruzzante. G., Figwer, M.& Lazari, A. (2019). “A Proposal for a European Cybersecurity Taxonomy”. EUR 29868, *Publications Office of the European Union*, Luxembourg. ISBN 978-92-76-11603-5, Retrieved 2024-01-25. doi:10.2760/106002, JRC118089

Naseri, R. N. N., Azis, S. N., & Abas, N. (2023). A Review of Technology Acceptance and Adoption Models in Consumer Study. Firm Journal of Management Studies. https://www.semanticscholar.org/paper/A-Review-of-Technology-Acceptance-and-Adoption-in-Naseri-Azis/f2a55ce8a073ad0cef7c54fb0ecb07b01ff29fcd

Ololara. A. E., Alawida. M. & Abiodun, O. I. (2023). ”Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey”. In, *Neural Computing and Applications* (2023) 35:23063–23101. Retrieved 2024-01-30 https://doi.org/10.1007/s00521-023-08857-7(0123456789().,-volV)(0123.

Omolara. A. E., Alawida. M. & Abiodun, O. I. (2023). ” Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey”. In *Neural Computing and Applications.* Retrieved 2024-01-30 https://doi.org/10.1007/s00521-023-08857-7(0123456789().,-volV)(0123456789,-().

Oxford Learners´s Dictionaries (2023). “Taxonomy”. Retrieved 2024-01-30 http://www.oxfordlearnersdictionaries.com/definition/english/taxonomy

Puscas, I. (2023). “AI Risks Taxonomy Paving the Path for ConfidenceBuilding Measure”. In *UNIDIR report on risks of artificial intelligence (AI).* Retrieved 2024-01-30 https://unidir.org/wp-content/uploads/2023/10/UNIDIR_Research_Brief_AI_International_Security_Understanding_Risks_Paving_the_Path_for_Confidence_Building_Measures.pdf

PWC & Stop Scams UK (2023). “AI bots can perform illegal financial trades and cover them up by not communicate it to the responsible firm”. Retrieved 2024-01-30 https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf

Samoili, S. López Cobo, M. Gómez, E. De Prato. G., Martínez-Plumed, F. and Delipetrev, B. (2020). “AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence”, *EUR 30117 EN, Publications Office of the European Union*, Luxembourg, ISBN 978-92-76-17045-7, doi:10.2760/382730, JRC118163.

Sayler, K. M. & Harris, L. A. (2023). “Deep fakes and National Security”. In *Congressional Research Service*. Retrieved 2024-01-08 https://sgp.fas.org/crs/natsec/IF11333.pdf

Swedish Security Service (2023). Säkerhetspolisen 2023-2024. Retrieved 2024-02-21. https://sakerhetspolisen.se/download/18.5cb30b118d1e95affec37/1708502268494/Lägesbild%202023-2024.pdf

Swenson, A. (2023, August 10). FEC moves toward potentially regulating AI deepfakes in campaign ads. AP News. https://apnews.com/article/fec-artificial-intelligence-deepfakes-election-2024-95399e640bd1e41182f6c631717cc826

Swinyard, W. R., & Smith, S. M. (2003). Why people (don’t) shop online: A lifestyle study of the internet consumer. Psychology & Marketing, 20(7), 567–597. https://doi.org/10.1002/mar.10087

UNICRI (2020). “Malicious Uses and Abuses of Artificial Intelligence”. In Trend Micro Research. Retrieved 2024-01-08. https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf

United Nations office on Drugs and Crime (UNODC) (2023). “World Drug Report 2023”. Retrieved 2024-01-24. https://www.unodc.org/res/WDR-2023/WDR23_Exsum_fin_SP.pdf

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. Management Science, 46(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Wang, C., Ahmad, S. F., Bani Ahmad Ayassrah, A. Y. A., Awwad, E. M., Irshad, M., Ali, Y. A., Al-Razgan, M., Khan, Y., & Han, H. (2023). An empirical evaluation of technology acceptance model for Artificial Intelligence in E-commerce. Heliyon, 9(8), e18349. https://doi.org/10.1016/j.heliyon.2023.e18349

Xu, N., & Wang, K.-J. (2021). Adopting robot lawyer? The extending artificial intelligence robot lawyer technology acceptance model for legal industry by an exploratory study. Journal of Management & Organization, 27(5), 867–885. https://doi.org/10.1017/jmo.2018.81

8. Annex 1 - Literature Used for the taxonomy.

Located:	Literature (Author)	Relevance for the taxonomy:
Scopus	Bauer and Bindschaedler, 2018	• Identify different types of crimes. • Definitions.
Scopus	Barnm, Ravinder & -Barn, Balbir, 2020	• Definitions.
ALIGNER	Brundage, M., Avin, S. & Clark, J. et al., 2018	• Identify different types of crimes. • Definitions.
ALIGNER	Caldwell et al, 2020	• Identify different types of crimes. • Definitions.
ALIGNER	CSET, 2021	• Identify different types of crimes.
ALIGNER	D2.1: Functionality taxonomy and emerging practices and trends, 2022 (CONFIDENTAL)	• Inspiration for the Taxonomy layout
ALIGNER	ENISA AI CYBERSECURITY CHALLENGES, 2020	• Inspiration for the Taxonomy layout
ALIGNER	Europol Innovation Lab	• Identify different types of crimes.
ALIGNER	Europol taxonomy LEA, 2017	• Inspiration for the Taxonomy layout
ALIGNER	Hayward, 2020	• Identify different types of crimes.
ALIGNER	JRC TECH REP - A Proposal for a European Cybersecurity Taxonomy, 2019	• Inspiration for the Taxonomy layout
ALIGNER	JRC TECH REP - Watch Defining Artificial Intelligence, 2020	• Inspiration for the Taxonomy layout
ALIGNER	King. Et.al 2020	• Identify different types of crimes.
ALIGNER	McKendrick, 2019	• Identify different types of crimes.
Scopus	McGuire & Dowling, 2013	• Definitions.

ALIGNER	National Security Commission on AI,	• Identify different types of crimes.
ALIGNER	Ravinder et. al, 2016	• Inspiration for the Taxonomy layout
Scopus	Schneier, 2021	• Identify different types of crimes.
ALIGNER	Trend Micro Research, 2020	• Identify different types of crimes.
ALIGNER	UNICRI, 2021 (algorithms and terrorism)	• Identify different types of crimes.
ALIGNER	Unicri, Countering terrorism online	• Identify different types of crimes.
ALIGNER	UNICRI, 2019 - ARTIFICIAL INTELLIGENCE AND ROBOTICS FOR LAW ENFORCEMENT	• Inspiration for the Taxonomy layout
ALIGNER	Zouave et al 2020	• Identify different types of crimes.
Scopus	Ellis-Petersen & Hassan, 2023	• Identify different types of crimes.
Scopus	Klein, 2022	• Identify different types of crimes.
Scopus	Christensen. et al, 2022	• Identify different types of crimes.
Scopus	Mahmud, 2023	• Identify different types of crimes.
Scopus	Omolara. et. al, 2023	• Identify different types of crimes.
Scopus	Jackman & Hooper, 2023	• Identify different types of crimes.
Scopus	Bauer & Bindschaedler, 2017	• Identify different types of crimes.
Scopus	PWC & Stop Scams UK, 2023	• Identify different types of crimes.
Scopus	Macleod, 2023	• Identify different types of crimes.
Scopus	Chesney & Citron, 2019	• Identify different types of crimes.
Scopus	Sayler & Harris, 2023	• Identify different types of crimes.

9. Annex 2 – The Survey.

We have here, for the sake of readers 'clarity we have here in this Annex 2 grouped the items with headings related to their respective latent variables. That was not the case when the survey was given to the respondents.

Usefulness

First we'd like to inquire about your views on the effectiveness of artificial intelligence tools for criminal purposes—specifically, how beneficial you believe such tools will be for the criminals.

1 When criminals use artificial intelligence services in their criminal activities, they will *more quickly accomplish the goals* of their criminal ventures.

- ☐ 1) I agree with that to a little extent
- ☐ 2)
- ☐ 3)
- ☐ 4) I agree with that to a large extent.

2 When criminals use artificial intelligence services in their criminal activities, it will *enhance* their criminal productivity.

- ☐ 1) I agree with that to a little extent
- ☐ 2)
- ☐ 3)
- ☐ 4) I agree with that to a large extent.

3 When criminals use artificial intelligence services in their criminal activities, it will *improve their performance.*

- ☐ 1) I agree with that to a little extent
- ☐ 2)
- ☐ 3)
- ☐ 4) I agree with that to a large extent

4 Artificial intelligence services will be *useful* for criminals in their daily criminal activities.

- ☐ 1) I agree with that to a little extent
- ☐ 2)
- ☐ 3)
- ☐ 4) I agree with that to a large extent.

Ease of Use

Our next topic is what you believe about how easy it will be for criminals to use artificial intelligence services in the near future i.e. the next two-three years.

***5 How easy or difficult* do you think it will be for criminals to learn and use artificial intelligence services in their criminal activities?**

- ☐ 1) Very Easy
- ☐ 2)
- ☐ 3)
- ☐ 4) Very Difficult

6) When criminals use artificial intelligence services they will easily be able to make use of them for criminal purposes.

- ☐ 1) I agree with that to a little extent.
- ☐ 2)
- ☐ 3)
- ☐ 4) I agree with that to a large extent

7) Using artificial intelligence services with criminal intent will *not* require a lot of knowledge or technical expertise:

- ☐ 1) I agree with that to a little extent
- ☐ 2)
- ☐ 3)
- ☐ 4) I agree with that to a large extent.

8. It will be easy for criminals to become skilled at using artificial intelligence services for criminal use.

- ☐ 1) I agree with that to a little extent.
- ☐ 2)
- ☐ 3)
- 4) I agree with that to a large extent

9. AI-services for criminal use will be easier to access than today:

- ☐ 1) I agree with that to a little extent.
- ☐ 2)
- ☐ 3)
- ☐ 4) I agree with that to a large extent.

Sense of urgency and intention to use

10. Criminals' use of artificial intelligence services with criminal intent will increase in the near future.

- [ ] 1) I agree with that to a little extent.
- [ ] 2)
- [ ] 3)
- [ ] 4) I agree with that to a large extent.

11. Criminals will use artificial intelligence services, with criminal intent regularly.

- [ ] 1) I agree with that to a little extent
- [ ] 2)
- [ ] 3)
- [ ] 4) I agree with that to a large extent.

12. Criminals plan to actively engage with artificial intelligence for criminal purposes in the near future.

- [ ] 1) I agree with that to a little extent.
- [ ] 2)
- [ ] 3)
- [ ] 4) I agree with that to a large extent.

13. It is urgent that law and policing plan and prepare right now for current criminal use of artificial intelligence today.

- [ ] 1) I believe that to a little extent.
- [ ] 2)
- [ ] 3)
- [ ] 4) I believe that to a large extent.

14. It is urgent that law and policing plan and prepare now for increased criminal use of artificial intelligence in the near future.

- [ ] 1) I agree with that to a little extent.
- [ ] 2)
- [ ] 3)
- [ ] 4) I believe that to a large extent.

15) How much do you believe that criminals will actively seek out and adopt artificial intelligence services to facilitate their criminal activities in the near future?

☐ 1) I believe that to a little extent.
☐ 2)
☐ 3)
☐ 4) I believe that to a large extent.

ATC3

During recent times, there has also been cases of so called "*deep fakes",* that is images and sounds created by artificial intelligence services and being used to *misinform the public*, creating *fraudulent commercial offers*, and to *influence politics and elections.* What do you believe about the use of such "*deep fakes*" by criminals, hostile actors or other malicious groups during the next two-three years?

Rank the following statements according to the extent to which you believe each scenario will be a problem in the near future. You can give each scenario a score 1-5, where 5 is the highest rank for the worst problem.

	Not so bad 1)	2)	3)	4)	Very Bad 5)
16) I believe that in the next two-three years the use of artificial intelligence driven "deep fakes" of voices and images as tools to commit *fraud, forgery* and *information theft* will be a problem that is:	☐	☐	☐	☐	☐
17) I believe that in the next two-three years the use of artificial intelligence driven "deep fakes" of voices and images as tools for *system interference, sabotage* and *breaches of data security* will be a problem that is:	☐	☐	☐	☐	☐
18) I believe that in the next two-three years the use of artificial intelligence driven "deep fakes" of voices and images as tools for *blackmail* and *extortion* will be a problem that is:	☐	☐	☐	☐	☐
19) I believe that in the next two-three years the use of artificial intelligence driven "deep fakes" of voices and images as tools for *Incitement* to crime will be a problem that is:	☐	☐	☐	☐	☐
20) I believe that in the next two-three years the use of artificial intelligence driven "deep fakes" of voices and images as tools for *persecutions* and *violations of human rights* will be a problem that is:	☐	☐	☐	☐	☐
21) I believe that in the next two-three years the use of artificial intelligence driven "deep fakes" of voices and images as tools for *election interference* will be a problem that is:	☐	☐	☐	☐	☐

22) I believe that some other way of using deep fakes for criminal purposes more specifically* will be a problem that is ☐ ☐ ☐ ☐ ☐

22b) That other way is (write here)

ATC2

In the literature, we have found forecasts of how crime committed in the digital domain can be enabled by artificial intelligence techniques such as e.g. *adversarial machine learning, AI-enhanced malware* or *synthetic biometric data.* Those could be used for e.g. *Insurance fraud, information theft, denial of service attacks, breach of data secrecy* and other such similar crimes. What do you believe about the use of *adversarial machine learning, AI-enhanced malware or synthetic biometric data* by criminals, hostile actors or other malicious groups during the next two-three years?

Rank the following statements according to the extent to which you believe each scenario will be a problem in the near future. You can give each scenario a score 1-5, where 5 is the highest rank for the worst problem.

	Not so bad1	2	3	4	Very Bad 5
24) I believe that in the next two-three years such artificial intelligence services being used as tools for crimes of *fraud, forgery* and *deception* will be a problem will be a problem that is:	☐	☐	☐	☐	☐
25) I believe that in the next two-three years such artificial intelligence services being used as tools for *information theft* will be a problem that is:	☐	☐	☐	☐	☐
26) I believe that in the next two-three years such artificial intelligence services being used as tools for *system interference, sabotage* and *breaches of data security'* will be a problem: that is:	☐	☐	☐	☐	☐
27) I believe that in the next two-three years such artificial intelligence services being used as tools to *commit blackmail* or *extortion* will be a problem that is:	☐	☐	☐	☐	☐
28) I believe that in the next two-three years such artificial intelligence services being used as tools for *election interference* will be a problem that is:	☐	☐	☐	☐	☐
29) I believe that in the next two-three years some other form* of crime and criminality in the digital domain and online cybercrime, more specifically will be a problem that is:	☐	☐	☐	☐	☐
29b) That other way is (write here)	☐	☐	☐	☐	☐

ATC3

In the literature, we have found forecasts of how *weaponized or criminalized autonomous vehicles, robots* or *drones* enabled by artificial intelligence can be used for *drug trafficking, terrorist purposes, traffic violations* and/or *explosions* and *acts of arson.* What do you believe about the next two-three years?

Rank the following statements according to the extent to which you believe each scenario will be a problem in the near future. You can give each scenario a score 1-4, where 4 is the highest rank for the worst problem and 1 the rank for the least problem.

	Not so bad 1)	2)	3)	4)	Very Bad 5)
30) I believe that in the next two-three years weaponized or criminalized autonomous vehicles, robots or drones enabled by artificial intelligence and used for terror, harmful explosions and/or arson will be a problem that is:	☐	☐	☐	☐	☐
31) I believe that in the next two-three years weaponized or criminalized autonomous vehicles, robots or drones enabled by artificial intelligence and used for *traffic violations* will be a problem that is:	☐	☐	☐	☐	☐
32) I believe that in the next two-three years weaponized or criminalized autonomous vehicles, robots or drones enabled by artificial intelligence and used for *drug trafficking* will be a problem: that is:	☐	☐	☐	☐	☐
33) I believe that in the next two-three years weaponized or criminalized autonomous vehicles, robots or drones enabled by artificial intelligence and used for used for *physical assault* will be a problem that is:	☐	☐	☐	☐	☐
34) I believe that in the next two-three years weaponized or criminalized autonomous vehicles, robots or drones enabled by artificial intelligence and used for *drug trafficking* will be a problem: that is:	☐	☐	☐	☐	☐
35) I believe that in the next two-three years some other way* of using, autonomous vehicles, robots or drones enabled by artificial intelligence for criminal purposes will be a problem that is:	☐	☐	☐	☐	☐
35 b) That other way is (write here)	☐	☐	☐	☐	☐

Basic Demographics

Here follows some basic demographic questions so we can understand how opinions may vary between different groups of stakeholders. Once again you are anonymous and under no obligation to answer.

36. I work in (Choose one)

- ☐ Research & academia
- ☐ Law enforcement & policing
- ☐ Public sector agency, not in the areas of law enforcement & policing
- ☐ Industry
- ☐ Non-commercial civil society

Prefer not to say

Other type of occupation (write here): _____

37) I am (choose one)

- ☐ A police officer
- ☐ A researcher
- ☐ A customs authority worker
- ☐ Prosecutor
- ☐ Other officer in law enforcement not police, prosecutor or customs
- ☐ City planner

Prefer not to say

Other type of place of work (write here): _____

38) I have been working at my current job for:

- ☐ 1 year
- ☐ 2years
- ☐ 3years
- ☐ 4years
- ☐ 5years
- ☐ 6years
- ☐ 7years
- ☐ 8 years
- ☐ 9 years
- ☐ 10+ years
- ☐ prefer not to say

8 **I have been aware of issues in the meeting of artificial intelligence, law enforcement and crime for**

- ☐ 1 year
- ☐ 2years
- ☐ 3 years
- ☐ 4 years
- ☐ 4 years
- ☐ 6 years
- ☐ 7years
- ☐ 8 years
- ☐ 9 years
- ☐ 10+ years
- ☐ prefer not to say

8 **My general knowledge about artificial intelligence is**

- ☐ little
- ☐ some
- ☐ a lot
- ☐ prefer not to say

10. Annex 3 PLS-SEM Terminology

Average Variance Extracted (AVE)

This is a measure used to assess how much of the variation of the numbers in a data set s is explained by the underlying concept they are supposed to be measuring. A higher AVE (above 0.5) means that the items are good at capturing the intended concept, i.e. doing their intended job.

Contextual Importance:

In relation to VIF and Cronbach's Alpha (see below):

- **Cronbach's Alpha** measures the reliability or internal consistency of the items, ensuring they consistently measure the same concept.
- **AVE** checks how well these items collectively represent the concept.
- **VIF** makes sure the items (or predictors) are not too similar, avoiding redundancy and ensuring the model's reliability.

Together, they help ensure that the items are consistent (Cronbach's Alpha), relevant and representative (AVE), and not overly repetitive (VIF).

Bootstrapping

- **Bootstrapping** is used to test a model validated. It tests if the model's parameters are dependent on one specific sample, which would be bad thing. It provides a way to assess the robustness of the model by generating multiple samples and observing the variability in the resulting estimates. It helps to assess the stability and reliability of the model parameters by providing confidence intervals and standard errors. It demands a minimum size of the data set and could not be done in our case, at least not in a meaningful way.

Chi-square Goodness of Fit (GOF):

- **Chi-square GOF** is a statistical test used to evaluate how well the observed data fit the expected data predicted by a model. It compares the observed frequencies with the expected frequencies under the model. A lower Chi-square value indicates a better fit, but it is sensitive to sample size; larger samples can make even small discrepancies appear significant. Our sample was is small.
- **For testing a model**: Chi-square GOF helps determine if the differences between observed and expected data are due to chance or if the model is not a good fit. A non-significant Chi-square (p-value > 0.05) indicates a good fit.

Composite Reliability (rho_a and rho_c)

- **Composite reliability (rho_a)**: This measure checks the reliability of a set of survey or test items, ensuring they consistently measure the same concept. This measure is similar to Cronbach's Alpha but considered more accurate in some cases.
- **Composite reliability (rho_c)**: This measure also assesses the internal consistency of the items, but it considers the different loadings of each item, providing a more precise reliability estimate compared to Cronbach's Alpha.

Relation to VIF, Cronbach's Alpha, and AVE:

- **Cronbach's Alpha**: Checks the consistency of the items in measuring a concept.
- **Composite Reliability (rho_a and rho_c)**: Provide more nuanced and accurate measures of this consistency, ensuring items reliably measure the intended concept.
- **AVE (Average Variance Extracted)**: Assesses how well the items represent the concept by looking at the amount of variance they explain.
- **VIF (Variance Inflation Factor)**: Ensures the items or predictors aren't too similar to avoid redundancy, ensuring the model's reliability.

Together, these metrics help ensure that the items in a survey or test are consistent, accurately represent the concept, and are not overly repetitive, making the results reliable and meaningful.

Cronbach's alpha

This is a measure used to check the reliability or internal consistency of a set of survey or test questions. It tells you how well the questions work together to measure the same thing. If the questions have a high Cronbach's alpha (usually above 0.7), it means they are consistent and reliable. In simpler terms, it is like making sure all the questions in a test are in sync and effectively measuring the same concept, so you can trust the results, see also **rho_a** and **rho_c** and **AVE**.

d_ULS (Unweighted Least Squares Discrepancy)

d_ULS is a measure used to assess the goodness of fit of a structural equation model. It quantifies the discrepancy between the observed data and the model's predicted data using the unweighted least squares method. A lower d_ULS value indicates a better fit, meaning the model's predictions are closer to the actual observed data.

For testing a model: d_ULS helps determine how well the model replicates the observed data. It is one of the fit indices used to evaluate the overall fit of the model.

Contextual Importance this is related to :

- **R-square and Adjusted R-square,** these measure how much of the variance in the dependent variable is explained by the independent variables, focusing on the model's explanatory power, i.e. a success measure.
- **SRMR** assesses the goodness of fit by comparing the predicted and observed correlation matrices, also a success measure.

- **d_ULS** provides another way to assess the goodness of fit, specifically using the unweighted least squares method to measure the discrepancy between the observed and predicted data.

In summary, while R-square and adjusted R-square evaluate the explanatory power of the model, and SRMR looks at the standardized residuals between observed and predicted data, d_ULS assesses the goodness of fit by measuring the discrepancy using the unweighted least squares method, helping ensure the model accurately represents the data. Together these examines differing aspects of the success of the PLS-SEM project.

Heterotrait-Heteromethod Ratio (HTMT)

HTMT is a measure used to assess discriminant validity in a set of survey or test items. Discriminant validity ensures that different concepts (traits) are actually distinct from each other, i.e are for example ATC 1-3 really seen as three distinct differing concepts? HTMT compares the correlations between items that are supposed to measure different concepts (heterotrait) with those that measure the same concept using different methods. A high HTMT value (typically above 0.85) indicates a lack of discriminant validity, meaning the concepts are not distinct enough, i.e. a failure.

Relation to VIF, Cronbach's Alpha, AVE, and Composite Reliability:

- **Cronbach's Alpha**: Measures internal consistency, ensuring items consistently measure the same concept.
- **Composite Reliability (rho_a and rho_c)**: Provide more accurate measures of this internal consistency.
- **AVE (Average Variance Extracted)**: Checks how well the items represent the intended concept.
- **VIF (Variance Inflation Factor)**: Ensures items or predictors are not overly similar to each other, avoiding redundancy.
- **HTMT**: Ensures different concepts are truly distinct from each other, which is important for the validity of the model.

Together, these metrics help ensure that the items in a survey or test are consistent (Cronbach's Alpha, Composite Reliability), representative (AVE), not overly redundant (VIF), and that different concepts are distinct (HTMT). In our case this measures if the respondents saw for example the ATC1 – 3 as truly distinct separate concepts in a taxonomy, or if they were as the more or less the same thing. The results show that they did see for example ATC 1-3 as three separate things, hence ensuring the health of the taxonomy as a taxonomy. If this value had shown otherwise the then taxonomy would have failed the empirical test, but it passed.

R-square (R^2)

- **R-square** measures how well the independent variables (predictors) explain the variation in the dependent variable (outcome). It ranges from 0 to 1, with a higher value indicating a better fit. For example, an R-square of 0.8 means that the predictors explain 80% of the variation in the outcome, this is a success measure.
- **For testing a model**: R-square helps determine how well the model captures the variation in the data. A higher R-square suggests a better explanatory power.

R-square Adjusted (Adjusted R^2):

- **R-square adjusted** adjusts the R-square value to account for the number of predictors in the model. It penalizes the addition of irrelevant predictors, providing a more accurate measure of model fit when multiple predictors are used.
- **For testing a model**: Adjusted R-square is useful for comparing models with different numbers of predictors. It helps prevent overfitting by showing if adding more predictors actually improves the model's explanatory power.

Difference:

- **R-square** shows the proportion of variance explained by the model, regardless of the number of predictors.
- **R-square adjusted** provides a more accurate assessment by adjusting for the number of predictors, making it better for comparing models with different numbers of predictors.

In summary, R-square tells you how well your model explains the data, while adjusted R-square gives a more accurate picture by considering the number of predictors, helping to avoid overfitting and making it easier to compare different models.

Standardized Root Mean Square Residual (SRMR)

- **SRMR** is a measure of the difference between the observed data and the model's predicted data. It is the standardized difference between the observed correlation matrix and the predicted correlation matrix. Lower values indicate a better fit, with values less than 0.08 generally considered a good fit.
- **For testing a model**: SRMR helps assess how well the model's predictions match the actual data. A lower SRMR value means that the model's predictions are close to the observed data, indicating a good fit.

Contextual Importance:

- **R-square and Adjusted R-square** tell you how much of the variance in the dependent variable is explained by the predictors, focusing on the explanatory power of the model.
- **SRMR** focuses on the model's fit by comparing the predicted correlations to the observed correlations, giving an indication of how well the model replicates the observed data patterns.

In summary, while R-square and adjusted R-square assess the explanatory power of the model, SRMR evaluates the goodness of fit by comparing the predicted and observed data, helping to ensure that the model accurately reflects the underlying relationships in the data.

VIF-value

In Partial Least Squares Structural Equation Modeling (PLS-SEM), a VIF (Variance Inflation Factor) value helps to check if there is a problem with "multicollinearity" among the predictor variables.

Multicollinearity happens when some predictor variables, are too similar or highly correlated, which can make the results of the PLS-SEM model unreliable. This could have happened if the respondents to our survey had perceived different survey questions as meaning the same thing, i.e. if the respondents had seen two survey questions as being differently phrased, but basically asking the same question. A VIF value above 5 or 10 indicates that that might have happened, and been a problem.

In simpler terms, the VIF value helps ensure that the predictors in the model are not just repeating the same information, allowing for more accurate and reliable results from the analysis. In our case this was not a problem.