The future of Cybercrime

AI and Emerging Technologies are creating a Cybercrime tsunami.

Philip Treleaven[1], Jeremy Barnett[1,6], Daniel Brown[1,4], Andrew Bud[3], Enzo Fenoglio[1],
Charles Kerrigan[1], Adriano Koshiyama[2], Sally Sfeir-Tait[1,5], Martin Schoernig[1]
[1]University College London, [2]HolisticAI, [3]iProov, [4]MegaNexus, [5]RegulAItion, [6]Resilience

Executive Summary

It is generally agreed that society is on the threshold of an 'explosion' of cybercrime from AI and emerging technologies, and that law enforcement, (financial) regulators, and institutions are ill prepared. The key challenge is **awareness**: since cybercrime operates in a criminal ecosystem (i.e., parallel universe). In particular, law enforcement requires awareness training and radical restructuring of its operational model to detect and prosecute emergent and previously unseen cybercrimes.

A notable driver is generative AI (e.g., ChatGPT). GPT-4, trained on 170 trillion parameters, is just one emerging technological but a quantum leap (cf. iPhone). Plug-ins are now available using Microsoft 365 Copilot and GitHub, with numerous companies launching generative AI add-ins to their products, such as Bloomberg GPT (Bloomberg, 2023). And on the horizon is Algorithmic Superintelligence (ASI) far surpassing most gifted human minds.

The current tsunami of digital legitimate innovation is matched by AI deep fakes, blockchain NFT fraud, smart contract vulnerabilities, denial-of-service infrastructure attacks, cryptocurrency ransomware, abusive metaverse avatars, etc., *a digital Pandora's box*. As a portent, cybercriminals are using ChatGPT to write crimeware programs and using data analytics to profile potential victims. Researchers at Microsoft demonstrated a text-to-audio tool that having heard just 3 seconds of audio can fully replicate your voice (Edwards, 2023). So much for identity theft and secure online banking platforms that use popular voice recognition "my voice is my password"! Cybercrime is also *industrializing*; increasingly sophisticated cybercriminals are collaborating, and also partnering with rogue governments for the assemblage of social media misinformation, autonomous agents and big data directed towards the manipulation of public opinion through computational propaganda (Chessen, 2017).

All emerging technologies challenge society to balance *innovation* and *regulation*; and address emergent unforeseen abuses. Some illegal, some opportunistic. Traditionally, cyber 'crime' covers illegal activities in cyberspace, but arguably needs to cover a growing spectrum of future opportunistic unregulated dark or 'sludge' practices. Examples include (foreign) government propaganda and social manipulation, surveillance, jurisdictional arbitrage, utility companies 'harvesting' customer bank accounts, inflating customer renewals, AI training data involving copyright infringement, online platforms encouraging digital addiction, market manipulation, paid influencer promotions, reputational and abuse attacks, or using AI to generate crimeware, etc. (see Figure 1).

More importantly, law enforcement and regulators traditionally operate a) retrospectively, b) with identifiable individuals and organizations, and c) in national jurisdictions. Cybercrime is changing all of this. Firstly, the dynamic nature of emerging technologies requires near real-time intervention using authentication and anomaly detection. Examples being misinformation or deepfake impersonation. Secondly, participants are increasingly anonymous: humans, algorithms, avatars, and organizations. Thirdly, innovations and abuses frequently occur in cyberspace domains unfamiliar to regulators and law enforcement. An example being young TikTok influencers offering financial advice to young naïve fans.

	Algorithms and AI	User Interfaces	Blockchain Technologies	Decentralized Infrastructure
Cybercrime	Deepfakes	Impersonation	Crypto & NFT scams Smart contract vulnerabilities	Denial-of-service Ransomware
Crimeware	Crimeware programs Victim data mining		Fake apps	
Dark web	Cyberstalking			Dark contents
Governments	Spyware		Crypto theft	
Corporates			ICO scams	Jurisdiction arbitrage
Individuals	Deepfakes	Online abuse Rogue avatars		

Figure 1: Cyberspace activities exploiting Emerging Technologies

For society, this is a technological *singularity* - a future point in time at which technological growth may become uncontrollable and irreversible, resulting in unforeseeable changes. Issues to be addressed include:

- **Agents/actors** – participants moving from the realm of humans to algorithms, avatars, androids in virtual environments.
- **Algorithms** – AI already embraces generative AI; on the horizon is artificial general intelligence (AGI) and Superintelligence (ASI), with society potentially losing control.
- **Deepfakes** – AI deep learning algorithms are now capable of creating totally convincing texts, images, speech, and video.
- **Globalization** – participants moving from identifiable humans and institutions operating in national jurisdictions, to digital agents/actors operating anonymously in global virtual environments.
- **Smart devices** – the proliferation of 'smart' autonomous networked devices including smartphones, computers, Bluetooth devices, and internet of things (IoT) sensors in vehicles, machines, and the built environment etc.

In confronting future cybercrime, law enforcement needs to utilize the very same AI and emerging technologies to automate. As illustrated by Figure 2, to move from a traditional 'physical' world to the new 'digital' ecosystem, of anonymous algorithms, inaccurate information, real-time interventions, global jurisdictions, and autonomous devices.

	Traditional	Future
Agents/actors	Humans, Institutions	Algorithms, avatars, androids, DAOs
Information	Data	NLP text, images, speech, video
Interventions	Retrospective analysis	Real-time analysis of previously unseen crime patterns
Jurisdictions	National, identifiable Agents	Global, anonymous Agents
Networked devices	Individual phones, computers	Networked smart devices, IoT infrastructure devices

Figure 2: Globalization of Cybercrime and Law Enforcement

We argue that the immanent rise of cybercrime requires law enforcement and regulators to radically rethink their operational model. In particular, law enforcement needs to replicate the innovation and automation of (financial) regulators, notably the pioneering UK Financial Conduct Authority (FCA), who have leveraged AI and emerging technologies for data science and automation, through radical tech sprints (cf. hackathons) and experimental sandboxes to understand and support rapid innovation. Care must be taken to ensure that a distinction is made between automation of enforcement/litigation and automation of the judicial/regulatory decision-making processes.

This paper is a review of AI and emerging technologies from the perspective of cybercrime and law enforcement:

- **Emerging technologies** (**DeepTech**) – introduction to AI and emerging technologies: hijacked by criminals and by necessity utilized by law enforcement and regulators to combat cybercrime.
- **Cybercrime innovation (CrimeTech)** – what we have dubbed 'CrimeTech' is AI and emerging technologies exploited for criminal activities, either for abuse, to make money or cause damage (cf. FinTech for criminals).
- **Information Security Technology** (**InfoSec**) – covers the tools and processes that organizations will use to protect information, devices and IoT infrastructure from future cybercrime.
- **Law Enforcement (LawTech) -** using AI and emerging technologies to support law enforcement, regulation, and legal services: *PoliceTech* the wide range of scientific and technological methods, techniques, and analytics used in policing; *SupTech* supporting 'supervisors' (e.g., regulators, police); *RegTech* regulatory monitoring, reporting, and compliance; *LegalTech* supporting the legal services firms and *JudicialTech* an extension of the virtual court movement using decision making methods to narrow the issues and decide fault/culpability/sanction.

The paper's contribution is firstly to raise **awareness**: alert readers to this 'parallel universe' of cybercrime and secondly to suggest an appropriate response for government and regulators . Given the scope, appendices list definitions of key terms for DeepTech, CrimeTech, InfoSec and LawTech.

1. Cybercrime Perspectives

As discussed, society is on the threshold of an explosion of cybercrime, both illegal (e.g., malware, impersonation, denial-of-service) but also emergent (e.g., misinformation, AI hallucinations, digital addiction), candidates for future regulation.

Notably, cybercrime will drive AI and emerging technology innovation (e.g., deepfakes), just as adult entertainment has often been the hidden engine that has driven digital innovation (e.g., Internet streaming, online payments, live video chat, etc.) The major societal challenge is awareness, but also to balance *innovation* with *regulation*. This is the reason for us broadening cybercrime to cover traditional illegal activities and well as future cyberspace activities, likely to require regulation:

- **Cyber 'crimes'** – illegal criminal activities carried out using computers or internet.
  - *Devices-as-Targets:* phishing, infrastructure vulnerabilities, crypto ransomware.
  - *Devices-as-Tools:* deepfakes, crimeware software, victim profiling.
- **Dark practices** – online platforms and user interfaces carefully crafted to trick users.
  - *Dark patterns:* utilities 'harvesting' customer bank accounts, overpriced insurance etc.
  - *Sludge practices:* discouraging customers from taking actions, such as switching provider, or designing obscure or overly long-winded complaints processes.
  - *Dark content:* misinformation, dark web, deviant content etc.
  - *Digital addition:* encouraging addictive use of an online application.
- **Institutions** – governments, organisations or individuals using cyberspace to monitor, control or influence.
  - *Social 'norm':* promoting a social or political agenda, cyber bullying.
  - *Surveillance:* security services, China Social Credit System, etc.
  - *Subversion:* (foreign) governments or organisations seeking to influence or impact society or markets.
  - *Predictive 'policing':* identifying potential 'illegal' activity, crime hotspots.

- **Algorithms** – the rise of nefarious algorithm either deliberately created or evolving.
    - *Opaque algorithms:* where the behaviour is unpredictable and uninterpretable.
    - *Feral algorithms*: that evolve unintentionally into cybercriminals and corrupt/conspire with other Superintelligence algorithms.
    - *Virus-like algorithms:* deliberately created criminal algorithms that replicate in uncontrollable ways.

Since the contribution of this paper is to raise awareness, rather than reviewing traditional cybercrime (see Appendix 2), the paper focuses largely on future developments. Of the numerous reports on the future of cybercrime Forbes lists 5 Trends Shaping the Future of Cybercrime Threat Intelligence (Forbes, 2021):

- Cybercriminals are *industrializing*, becoming more collaborative and specialized, creating a criminal ecosystem.
- Collaboration between state-sponsored operatives and cybercriminals is on the rise (e.g., Iran, North Korea).
- Cyberattacks especially on critical IoT infrastructure are on the rise and becoming more expensive.
- Botnets and automated malware deployment tools are becoming more sophisticated by utilizing AI and emerging technologies.
- Organizations of all sizes are in danger due to lack of awareness, but especially SMEs who frequently lack sophisticated resources for anomaly detection.

In a similar vein, the Rand Corporation's report: The Future of Cybercrime in Light of Technology Developments (Bellasio et al., 2020) provides interesting classes of incidents, drivers, agents, motivations, and costs (see Figure 3). Rising threats include:

- **Cyberterrorism** - the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society. Notable is the increasing attacks on IoT infrastructure.
- **Deepfakes** - deep learning used to create convincing texts, images, speech, and video fakes for hoaxes and impersonations.
- **Economic instability** – market risk, volatility, and crises due to unpredictable or deliberate algorithm behaviour (cf. flash crash 2010).
- **Misinformation** – inaccurate or deliberately misleading information leading to algorithmic misinformation caused by bad or deliberately biased training data.

Figure 3: The Future of Cybercrime in Light of Technology Developments (Bellasio et al., 2020)

- **Social manipulation** – social and political manipulation through AI algorithms and misinformation information.

- **Social surveillance** – surveillance with emerging technology, such as China's Social Credit System (e.g., ChinaSCS, 2023).
- **Weaponization** – autonomous weapons androids powered by AI.

Criminal Algorithms

Of all the emerging technologies, generative AI has garnered the most public interest and comment.

As an illustration, we may add new cybercrime variants originated with the introduction of Large Language Models (ChatGPT) such as:

- **Social engineering** – malware distribution campaigns organized by malicious actors using false promises of uninterrupted and free access to premium generative AI models in order to deceive users into installing malware on their devices or to obtain their account credentials.
- **Prompt engineering** – manipulation of generative AI language models by crafting specific prompts (jailbreak prompts) to bypass content moderation and generate potentially harmful content exploiting the system's limitations and producing malicious or misleading information.

With the rise of increasingly sophisticated AI algorithms, avatars and androids, arguably the future is 'criminal' algorithms (EU AI, 2022):

- **Feral algorithms -** that unintentionally evolve into cybercriminals and corrupt/conspire with other algorithms.
- **Virus-like algorithms** - algorithms deliberately created to commit crimes.
- **Superintelligence algorithms** – AI solving all problems better than people, with the potential of humans losing control.

In response we recommend a comprehensive future approach to algorithms:

- **Algorithm awareness** – educating the public, organizations, and law enforcement on the capabilities and drawbacks of emerging AI algorithms.
- **Algorithm authentication** – the process of verifying the identity and trust of algorithms and avatars.
- **Algorithm audit** – auditing algorithms from checking governance processes, to testing an algorithm's outputs, to inspecting its inner workings.
- **Algorithm conduct** – need for a new class of machine learning models with a built-in understanding of bias, ethics, fairness, risk, and legality etc. Interestingly, GPT-4 (GPT 4, 2023) now 'blocks' many requests for inappropriate content that attempts to generate code that is designed to disrupt, damage, or gain unauthorized access to a computer system.

With the algorithm ecosystem attempts to slow down or stop nefarious algorithm development will fail, as rogue states, corporations and individuals will simply not comply. What is required is work on overall ecosystems, to ensure the efficacy and success of evolution of morally-encoded and human-altruistic systems; which after all is broadly how humans have evolved. Benign AI must learn how to deal with its malign counterpart. We see less a stockpiling arms race, more a long-term contest between good and evil. Rather than preventing development, the task for regulators and government is for the appropriate incentives to be put in place for good to win out.

Indeed, implementing a moratorium solely by the actions of ethical actors could have significant drawbacks. While the intention behind a suspension might be to address the risks associated with AI development, it could unintentionally hinder progress, innovation, and the potential societal benefits

that AI can bring. In the context of AI systems going rogue, it is worth noting that the current judicial decision-making system in courts may serve as a valuable foundation to address these concerns. While AI introduces unique challenges, the principles of fairness, accountability, and justice underpinning the judicial process can be adapted to AI governance. Just as judges interpret laws and make decisions based on moral and societal values, a similar framework can be established to evaluate and regulate AI, ensuring that its development and deployment align with altruistic values and uphold the interests of humanity. Of course, this also requires a reconceptualization of how algorithms for legal decision-making (or for aiding legal decision-making) should be structured (Brozek, 2023).

At a research level:

- **Algorithm hallucination** – generation of outputs that may sound plausible but are either factually incorrect, or unrelated to the given context; with the algorithms generating additional nonsensical content when challenged by the user.

In summary, like human knowledge in modern societies, some aspects of AI decision-making may always remain opaque or difficult to understand. Thus, decisions made by AI algorithms can be already rational, when an appropriate (acceptable) justification can be adduced in their favor (Brozek, 2023).

2. Emerging Technologies (DeepTech)

The term emerging technologies spans a growing range of (DeepTech) technologies: Big data; AI algorithms; blockchain technologies; Web 3.0 and IoT decentralized environments; and user interfaces involving avatars, and metaverse environments, etc. Figure 3 is a simplistic tech stack for these emerging technologies involving:

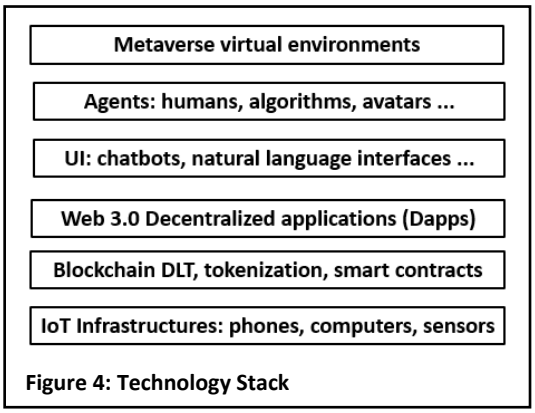

Figure 4: Technology Stack

- **Agents** – now humans, algorithms, avatars, androids, and organizations; often intermingled, anonymous and global.
- **Algorithms** – traditional machine learning systems for automation, now generative AI for user interaction, and in future algorithmic Superintelligence.
- **User Interface (UI)** – chatbots, natural language interaction (e.g., text, images, speech, video), avatars, VR/AR and metaverse virtual environments etc.
- **Blockchain DLT** – using distributed ledger, cryptocurrencies, tokenization, and smart contracts.
- **Decentralized infrastructures** – firstly Web 3.0 decentralized application systems (i.e., Dapps) and secondly IoT infrastructures of autonomous smartphones, computers, and devices in vehicles, machines, and buildings etc.

Importantly, it's not just individual technologies raising cybercrime to new levels, but what we characterize as a 'perfect storm' of technologies.

Algorithms and AI

For context, algorithms cover three broad domains: Computational Statistics (e.g., Monte Carlo methods), Complex Systems (e.g., Agent-Based systems), and Artificial Intelligence (e.g., Artificial Neural Networks). See Figure 5.

- **Computational Statistics** - computationally intensive statistical methods.
- **Complex Systems** - system featuring a large number of interacting components, where the collective dynamics are non-linear and often give rise to emergent properties not predictable from the individual elements' interactions.
- **AI Algorithms** - mimicking a new form of human learning, reasoning, knowledge, and decision-making.
  - Knowledge-based systems – a system that utilizes a database of knowledge or facts about a particular domain to reason, make inferences, and provide solutions or recommendations. An example being Rule-based systems that operates on a set of predefined rules or logical statements represented as IF-THEN rules
  - Evolutionary algorithms - algorithms for global optimization inspired by biological evolution (e.g., Genetic Algorithms).
  - Machine learning – algorithms with the ability to learn and improve from data without being explicitly programmed. These algorithms adapt and adjust their behavior as they are exposed to new information, enabling them to identify patterns, make predictions, and solve complex tasks more accurately over time.

Figure 5: Algorithm taxonomy (Koshiyama et al, 2020)

At a simple level, machine learning (ML) algorithms cover:

- **Traditional AI** - ML models to identify patterns within a training data set and make predictions.
- **Generative AI** - a broad label that's used to describe any type of AI used to dynamically create new 'human-like' texts, images, speech, video, programs, or synthetic data (Lawson, 2023).

And for the future, still topic of speculation and ongoing research:

- **Algorithmic General Intelligence (AGI)** - solving problems as well as humans; faced with an unfamiliar task and unpredictable inputs, the AGI system could find a solution.
- **Algorithmic Superintelligence (ASI)** – solving all problems better than people (ASI, 2023) across a comprehensive range of categories and fields of endeavor.

Key terms are:

- **Transformers** - a new class of disruptive ML model, that adopts the mechanism of self-attention, differentially weighting the significance of each part of the input data (Amatriain et al., 2023).
- **Generative Pre-trained Transformers (GPT)** - that 'dynamically' creates new human-like content.
- **Large Language Models (LLM)** - LLMs are a subset of AI trained on a vast quantity of (online) data to produce human-like responses to dialogue or other natural language inputs (Riedl, 2023).

ChatGPT and its growing number of competitors, including Microsoft Copilot, Google's Bard, Anthropic, Character.ai, Cohere and others have proven capability of holding human-level conversations, but also subject to generating inaccurate, unethical, and misinformation (MIT, 2023). Notable is *AI hallucination*: a confident response that is biased, too specialized, even totally wrong. These AI hallucinations can occur due to factors like limited training data or the absence of an uncertainty acknowledgment mechanism. Instead of admitting a lack of knowledge –"I don't know that answer"--, the model may fabricate a response that appears plausible but lacks factual accuracy.

However, it is more accurate to view these errors as *paralogisms*— fallacious arguments or illogical conclusions induced by the limitations of the AI language model. Recognizing this, it becomes crucial to critically evaluate and always verify AI-generated information (facts checking). It is essential to approach their outputs with caution and careful consideration, acknowledging that AI language models are fallible and capable of producing misleading responses.

Generative AI has massive implications for business, education, employment, but also law enforcement and crime. As commented by the UK Sunday Times newspaper (Fortson, 2023) "the ability to entwine a chatty, randy, bot with the image or video of a [real] person made to order to meet a user's preferences is [already] here".

User Interfaces (UI)

Another major area of emerging technologies are user interfaces (UIs): the intermingling of chatbots, natural language processing (NLP) and the metaverse. Arguably, the metaverse is likely to be hugely popular because it will allow humans to interact through their surrogate (fantasy) digital twin. As illustrated by OpenAI's ChatGTP and the technology stack in Figure 4, user interfaces are increasingly an amalgam of virtual environments, human-centric interaction using natural language text, images, speech, and video: generated dynamically by increasing powerful AI algorithms etc.:

- **Natural language** – interacting using natural language processing for text, images, speech, and video.
- **Conversational AI** – enabling machines to engage in human-like conversations to build intelligent systems that can understand and respond to natural language input, simulating human-like conversations with users.
- **Generative AI** – a broader concept that involves machines generating new content or output, such as text, images, music, or videos, that is not directly based on pre-existing data. Its primary purpose is to generate novel and creative outputs using technologies such as GTP, and increasingly AGI and ASI for human-level interaction.
- **Brain–computer interface (BCI)** – for the future: Elon Musk's Neuralink (https://neuralink.com/), an invasive direct communication pathway between the brain's electrical activity and an external device, smart phone, computer, or robot but for human applications non-invasive interfaces will be preferable (Waldert, 2016).

Conversational AI underpins applications such as chatbots, virtual assistants, customer support systems, voice-activated devices, and other interactive platforms where natural language processing (NLP) and natural language understanding (NLU), and natural language generation (NLG) are required to facilitate human-machine conversations. On the other hand, generative AI is employed in various creative fields, such as content creation, art, music, and storytelling to generate realistic images, write articles, compose music, produce video content, and more. Conversational AI primarily aims to facilitate human-machine conversations and understand user queries, while generative AI focuses on creating new and unique content. Both fields utilize different techniques and have distinct applications, but they can also intersect in certain areas where generative models are used within conversational AI systems to generate more creative and personalized responses.

Blockchain Technologies

Blockchain technologies are often equated with the negative aspects of cryptocurrencies, and hence often dismissed. However, blockchain, tokenization and smart contracts are infrastructure technologies used increasingly for automation.

A blockchain is a distributed (database) ledger that is an immutable 'chain' of transactions across many computers. (AWS, 2023). In Figure 6, the *timestamp* is the time or date of block creation. The *hash* is a unique digital identifier (cf. fingerprint) of the transaction and used to secure the block information. Lastly, cryptographic hash algorithms and authentication protocols frequently employ *nonces*, a value or a number that can only be used once.

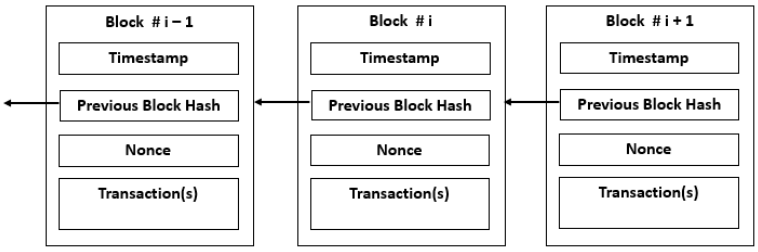

Figure 6: Blockchain architecture

The key technologies are:

- **Distributed ledger** - an 'audit trail' of cryptographically encoded transactions: a record of consensus maintained and validated by nodes. Not all distributed ledgers employ blockchains. For example, Hedera Hashgraph (https://hedera.com) uses a directed acyclic graph (DAG) structure, where transactions are linked through a graph instead of being organized in a linear chain.
- **Blockchain** - a distributed database that maintains a continuously growing list of ordered records, called blocks, linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.
- **Cryptography** - a method of securing information and communications through the use of codes: mathematical concepts and rule-based algorithms, that transform information in ways that are hard to decipher.
- **Cryptocurrencies** - a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank.
- **Tokenization** - the process of assigning a unique digital identifier and properties to an asset that's usable on a blockchain application.
- **Smart contract** – a program, representing an agreement, stored on a blockchain that runs when predetermined conditions are met, and used to automate the execution.

Pivotal in blockchain are cryptography techniques and protocols to maintain integrity, confidentiality, authentication, privacy and non-repudiation. Cryptography can broadly be broken down into three different types: a) Secret Key Cryptography; b) Public Key Cryptography; and c) Hash Functions. Common techniques include the use of asymmetric cryptography for authenticating transactions (e.g., through Elliptic Curve Cryptography) and Zero-Knowledge Proofs for maintaining the privacy of transactions.

Decentralized Infrastructures

Another major trend in technology is greater decentralization: a move from centralized cloud computing (and arguably vulnerable), to what may be characterized euphemistically as *Federated* computing:

- **Cloud computing** – the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer. To support collaboration, organizations need to transfer their data to centralized and potentially vulnerable servers.

- **Federated computing** – addresses peer-to-peer collaboration, distributed (and privacy-preserving) datasets, federated learning algorithms, decentralized applications (i.e., Dapps), privacy-preserving infrastructures, and integrated autonomous devices.

The two core (software and hardware) technologies are:

- **Web 3.0** – the third generation of the World Wide Web based on distributed ledger technology (DLT). Web 3.0 features open, decentralized, and interconnected protocols to provide peer-to-peer automated, collaborative services. Examples include: DData, DeFi and GameFi (Treleaven et al, 2022a).
- **IoT Infrastructures** - – internet of physical objects - 'things' - that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet (IoT, 2033).

Web 3.0 uses distributed datasets, decentralized federated learning, blockchain technologies, and edge computing to provide peer-to-peer automated services. Significant increases in transactions per second and interoperability between different 'Layer 1' blockchains encourage the development of 'ecosytems'. Decentralized finance (DeFi) is one important class of Web 3.0 services, using tokenization to manage assets and provide financial services, in the Data Economy (DataEcon, 2021).

Of particular importance for Web 3.0 verification is Decentralized identifiers (DID) an emerging W3C open-standard based identity framework that uses digital identifiers and verifiable credentials that are self-owned, independent, and enable trusted data exchange (DID, 2023).

IoT Infrastructures – traditionally when discussing cybercrime and information security (IST), we largely focus on individual smartphones, computers, and the Internet. However, the Internet of things (IoT) describes physical objects (or groups of such objects) with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks (IoT, 2023). This is the convergence of multiple technologies, including ubiquitous computing, commodity sensors, increasingly powerful embedded systems, as well as machine learning.

Digital identity and authentication

A key infrastructure technology is decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. Digital identity refers to the information utilized by computer systems to authenticate external entities, including a person, algorithms, organization, application (W3C, 2022). DIDs are designed to be decentralized, providing individuals and entities with control over their digital identities without relying on a central authority. They are globally unique, ensuring reliable identification across systems and domains. DIDs are resolvable, allowing for the retrieval of associated information and highly available for seamless access to data and services. Additionally, DIDs enable cryptographic verifiability, ensuring the integrity and trustworthiness of digital identity claims. Building on this W3C specification, the European Commission's identification, authentication and trust regulation EIDAS 2.0 seeks to create a transnational standard (EU EIDAS, 2023).

Appendix 1 gives definitions of various AI and emerging technologies.

3. Cybercrime Innovation (CrimeTech)

Given the expanding nature of cyber 'crime' the section addresses awareness: a) illegal activities (e.g., malware, denial-of-service); b) jurisdictional arbitrage that are likely to become illegal (e.g., misinformation, deviant content); and c) dark or sludge practices, unscrupulous candidates for future regulation (e.g., utility companies, digital addiction).

Using (Maskun et al, 2020) as a classification, traditional cybercrimes subdivide into:

- **Devices-as-targets** – where cybercrime targets data, computers and IoT devices, includes denial-of-service, hacking, malware, ransomware, spyware, worms and zombies etc.:
    - *Unauthorized access* – using hacking to access and modify information.
    - *Malicious code* – harmful computer code or web script designed to create system vulnerabilities leading to back doors, security breaches.
    - *Interruption of service* – designed to render a service inaccessible (e.g., DOS and DDOS attacks).
    - *Theft or misuse of service* - improper use of computers and communications.
- **Devices-as-tools** – where cybercrime utilizing smartphones, computers and IoT devices, definitions include clickjacking, cyberbullying, data breaches, hoax emails, phishing, pump-and-dump, romance scams and scareware etc.:
    - *Content violation* – unauthorized entry into or transmission corrupting of harmful software code into the target computer system.
    - *Unauthorized modification* – modification of data with intent to cause impairment.
    - *Improper use of communications* – broadly, malicious communications is sending indecent or grossly offensive, threatening, or information which is false or believed to be false.

Next, we speculate on future cybercrimes, powered by dark content information, increasingly realistic deepfakes, plus rogue criminal algorithms and avatars, either deliberately created or evolving 'feral' algorithms.

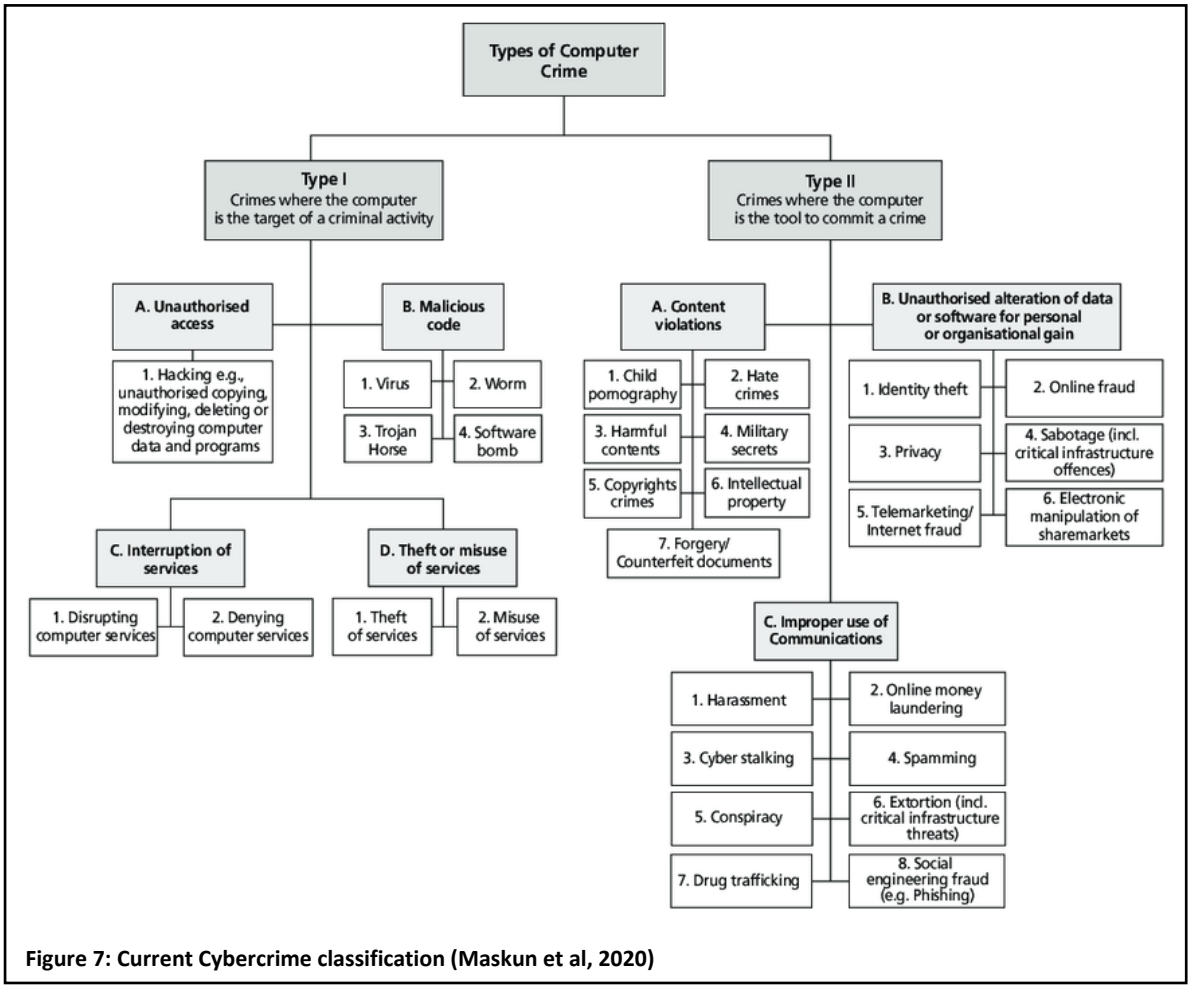

Figure 7: Current Cybercrime classification (Maskun et al, 2020)

Algorithms and AI

Two emergent areas for cybercrime are firstly generative AI with the increasing quality of deepfakes, and AI generated 'crimeware' tools, for planning crimes and writing crimeware programs etc.; and secondly the potential of sophisticated 'criminal' algorithm.

Generative AI is a powerful impersonation tool for fraudsters to commit scams, by creating highly convincing and realistic scams that can be difficult to detect. For example, ChatGPT can be used to create phishing emails that appear to be from legitimate sources, such as banks, tricking individuals into providing personal information or transferring money. ChatGPT can also be used to generate phone scripts, which can be used by fraudsters to impersonate customer service representatives. Additionally, ChatGPT is already being used by criminals to program cybercrime apps.

Generative AI and GPT supercharge traditional cyber scams include hacking, impersonation, malware, and reputational attacks. This includes data mining to identify potential victims, pump-and-dump, ransomware targeting deviant dark web 'trap' sites to ensnare victims, and romance scams where criminals create a fake online identity, supported by compelling Chatbots and avatars to gain a victim's affection and trust. Examples include:

- **Deepfakes** – already generative AI can produce convincing bogus content and fakes. Applications range from influencers, financial ramping, reputational attacks, to cyber extortion.
- **Dark patterns** – legitimate companies will increasingly 'trick' online customers, while trying to avoid reputational damage.
- **Digital addition** – highly successful online games, betting sites and social media platforms are encouraging excessive and harmful behaviors, using technologies such as recommender systems in retail and tokenization in 'play-to-earn' gaming. This will escalate until regulated.
- **Dark content** – combining deepfakes and anonymous agents will see an escalation of illegal deviant content. Opening users to cyber extortion. Also, we should include for the future misinformation and fake training data to intentionally corrupt algorithms.

Criminal Algorithms covers increasingly sophisticated malicious software designed to carry out or facilitate illegal online activity. Old-school malware written for 'fun' has already given way to a new era of AI-powered crimeware designed for spamming, data theft, or extortion:

- **Crimeware** – using GPT to create cybercrime software.
- **Cyber espionage** – expect a major expansion of spying by corporations, governments, and criminal organizations (e.g., North Korea); and increasing collaboration of these players, both for financial gain and economic disruption.
- **Cyber extortion** - the use of various tactics, such as phishing, malware injection, and DDoS attacks to hold a victim's data or systems hostage until a (cryptocurrency) ransom is paid.
- **Victim profiling** – using data analytics to identify potential cybercrime victims.

User Interfaces

User interfaces are increasingly an amalgam of virtual environments, and human-centric interaction using natural language text, images, speech, and video etc.

Human-centric Interaction - interacting using Chatbots and natural language processing for text, images, speech, and video. Examples of cybercrime include promotions using fake influencers:

- **Impersonation** – creating fake content of individuals and celebrities, and even fake avatars, such as avatar influencers to distribute misinformation.

Virtual Environments – humans, algorithms and avatar interacting in virtual environments, such as the metaverse allowing humans to interact through their surrogate (fantasy) digital twin.

- **Dark content** – information and algorithmic content, including on the dark web, that is either inaccurate, disapproved of by public opinion, deviant or illegal. Allowing users and website operators to remain anonymous.
- **Cyber extorsion** – users accessing deviant content are vulnerable to cyber ransom, facilitated using cryptocurrencies.
- **Romance scams** – one example is the increasing sophistication of romance scams using data analytics to profile victims and compelling avatars.

Blockchain Technologies

Although generative AI (e.g., ChatGPT) receives most publicity, blockchain and cryptocurrencies illustrate cybercrime 'opportunities' generated by a hyped emerging technology. Blockchain scammers took a record $14 billion in 2021 (CNBC, 2022). This involved fake coins and non-fungible tokens (NFT); hacked wallets; investment scams involving ICOs, and bogus companies; and most

recently exploiting smart contract vulnerabilities, etc. These scams involve a mixture of crypto, and AI deepfakes making them a challenge to classify.

Many cryptocurrency scams discussed below, are already commonplace, but are increasing in sophistication: a) Bitcoin investment schemes, b) rug pull scams, c) man-in-the-middle attack, d) social media cryptocurrency giveaway scams, e) crypto-Ponzi schemes, f) fake cryptocurrency exchanges, g) employment offers and fraudulent employees, h) flash loan attack.

Cryptocurrencies – the currency of choice for cybercriminals: anonymous payments, money laundering, hyped valuations and investments, bogus crypto coins and NFTs, ransomware etc.

- **Bogus coins** – take advantage of the anonymous and decentralized nature of the crypto space to mint tokens solely designed to drain ignorant investors of their funds and enrich them instead.
- **NFT Giveaways** - also known as airdrop scams, occur when fraudsters ask you to promote an NFT and sign up on their website in exchange for a free NFT. Once agreed, the scammer sends a link requiring the victim to enter your wallet details to receive the prize, thereby compromising access.
- **Fake Crypto Exchanges/Wallets** - fake cryptocurrency trading platforms or fake versions of official crypto wallets to trick unsuspecting victims. These fake websites usually have similar but slightly different domain names from the sites they attempt to mimic.

Anonymity - taking advantage of the anonymous and global nature of blockchain technologies.

- **Money laundering** - to move funds to addresses where its original criminal source can't be detected, and eventually to a service that allows cryptocurrency to be exchanged for cash.
- **Employment offers and fraudulent employees** - scammers impersonate recruiters or job seekers to get access to (cryptocurrency) accounts. With this ploy, they offer an interesting job but require cryptocurrency as payment for job training. Another example is (North Korean) IT freelancers trying to capitalize on remote job opportunities by presenting impressive resumes and claiming to be US-based.
- **Counterfeit NFTs** - NFTs are about creating unique digital tokens. However, counterfeiting is rampant on many NFT platforms, resulting in victims buying a stolen copy of a real-world artist's work.
- **Promotions** - marketing phantom cryptocurrencies, NFTs, APPs, and investments.
- **Celebrity endorsements** - this involves selling cryptocurrencies or tokens using endorsements from celebrities, businesspeople, or influencers; some fake some real.
- **Bitcoin investment schemes** - fraudulent crypto investment managers, claiming to have made millions, promise their victims they will make huge profits with investments.
- **Initial coin offerings (ICOs)** – fraudulent and sophisticated ICOs are notorious for offering customers discounts on new crypto coins in exchange for established cryptocurrencies, or the latest variant is Initial token offerings (ITOs), similar to fraudulent ICOs but involving tokens.
- **NFT bidding scams** – with NFT bidding in secondary markets, scammers place the highest bid but then change the cryptocurrency used for the bidding without the vendor's knowledge.

Technology scams – sophisticated manipulation of blockchain infrastructure technologies.

- **Cloud mining scams** – bogus cloud mining companies offer rentable mining hardware in exchange for a fixed fee or a share of the revenue. However, victims end up losing money or earning less than was implied.

- **Cryptojacking** - is the act of hijacking a computer to mine cryptocurrencies against the user's will, through websites, or while the user is unaware.
- **Smart contract vulnerabilities** – exploiting vulnerabilities in smart contracts used to automate the execution of an agreement between different parties.

A growing area is smart contract attacks include: a) reentrancy attack – causes the vulnerable contract to submit an external call.; b) front-running - allows malicious actors to see the intended outcome of a smart contract before it's confirmed; c) integer overflow and underflow - forces the smart contract's balance to cycle back to the maximum value; d) logic errors – simple logic errors in the smart contract code; e) block gas limit vulnerability – a DOS attack can cause a block to exceed storage and generate a 'refund'; f) default visibility - an attacker had an opportunity to call public functions and change ownership.; and g) timestamp dependence - a malicious miner can manipulate the timestamp so that it is in their favor. (Pixelplex, 2023). Other potential vulnerabilities that are regularly spotted by smart contract auditors include: irrelevant code, improper initialization, incorrectly handled exceptions, Incorrect work with ERC-20 tokens (Pixelplex, 2023).

Decentralized Infrastructures

The two growing areas for cybercrime are firstly decentralized web3 infrastructures supporting anonymous agents; and secondly attacks on critical IoT infrastructures due to their vulnerability and the nascent nature of IoT IST technologies.

Web 3.0 are ecosystems supporting distributed datasets, federated machine learning algorithms and interconnected protocols to provide peer-to-peer automated, collaborative services. In these decentralized ecosystems the challenge is to authenticate possibly anonymous participants: humans, algorithms, and organizations.

- **Bad actors** – criminals creating anonymous participants (e.g., humans, algorithms, avatars) and tokenized assets that pass identity and trust verification procedures. Hence web3 technologies such as self-sovereign identity (SSI), pseudonymity and anonymity present vulnerabilities.
- **Data authenticity** – providing disinformation and misinformation, including algorithm training data.
- **Data vulnerability** - unauthorized access to data (especially by DApps, which are a vital component of the web3 landscape).

One example of a recent and prominent web3 security attack is 'ice phishing'. The use of deceptive techniques for duping users into digitally signing malicious blockchain transactions, which grant permissions to the attackers to utilize the user's tokens.

IoT scams attacking infrastructure are a daily occurrence. Figure 8 classifies the various IoT attacks into:

- **Physical** – concerned with the hardware elements, such as attacking the sensor nodes.

- **Software** – attacking weaknesses in the system implementation and communication interfaces, using phishing, viruses, and spyware for DoS attacks.
- **Network** – exploiting the interconnections and the transfer of data between IoT devices.
- **Encryption** - focusses on breaching the encryption mechanisms used to protect IoT systems.

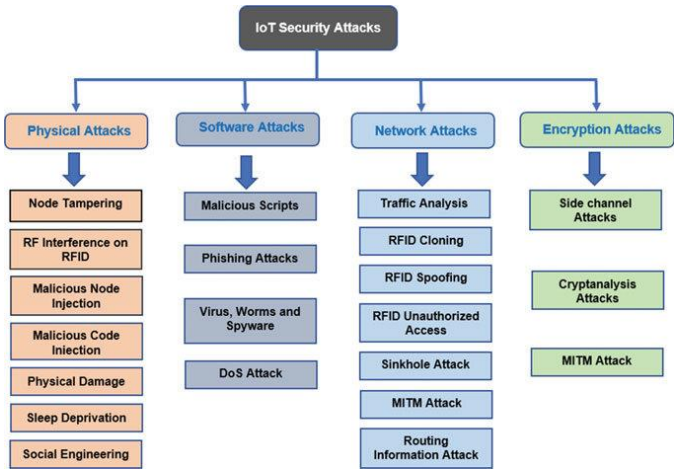

Figure 8: IoT Security Attacks (Atlam & Wills, 2019)

Current IoT scams include cyber espionage, cyber extortion, denial-of-service, and ransomware. Future IoT scams are likely to involve cyberterrorism and cyber warfare.

In summary, Figure 9 illustrates possible future cybercrimes, with Appendix 2 giving definitions of current activities.

	Crypto coins & Token scams	Generative AI scams	Superintelligence scams
Crimeware	▪ Schemes offering bogus coins and tokens	▪ ChatGPT Investment scams	▪ Data mining for victims
Criminal algorithms	▪ Crypto investment scams	▪ Deepfake content ▪ ChatGPT created criminal apps	▪ 'Feral' AGI and ASI algorithms
Cyber espionage	▪ Payments in cryptocurrencies	▪ Subversive economic and social content	▪ 'Cyberspy' algorithms
Cyber extortion	▪ Ransomware using cryptocurrencies	▪ Ransomware in the deviant Metaverse	▪ Criminal algorithms
Cyberfakes	▪ NFTs, exchanges	▪ Text, images, speech. video	▪ Criminal avatars
Dark patterns	▪ Play-to-earn computer games	▪ Reputational attacks ▪ Revenge port	▪ Biased algorithms
Dark content	▪ Misleading crypto promotions by influencers	▪ Incorrect information ▪ Subversive training data ▪ Nefarious material	▪ Romance scam avatars
Dark web	▪ Payments for dark web content	▪ Tools for cybercrime ▪ Nefarious metaverses	▪ Deviant and illegal metaverses
Deepfakes	▪ Fake ICO, cryptocurrencies and tokens	▪ Text, images, speech, video	▪ Avatars
Digital addiction	▪ Play-to-earn computer gaming	▪ Romance avatars	▪ Addictive algorithms

Figure 9: Current Crypto scams versus Future AI scams

Next, we will review the future of information security technologies.

4. Information Security Technology (InfoSec)

Traditionally, InfoSec has focused largely on individual smartphones and computers. In comparison, InfoSec for decentralized infrastructures (e.g., Web 3.0 and IoT) are immature, and hacking will clearly escalate. With new emerging technologies and their opportunistic exploitation by criminals. The challenge for InfoSec is to verify new agents and identify previously unseen anomalies and to do so in real-time. In particular, 'trust' in information and in participants operating in digital environments.

For context, traditional InfoSec software a) *monitors* access and report behaviour including diagnostic programs, intrusion detection (IDS) and prevention (IPS), log and record management; b) *regulates* access to data or systems, while still allowing interaction, examples being access controls, firewalls, sandboxes and VPNs; c) *prevents* or restricting access to data and systems, using techniques such as cryptography/encryption and steganography; and d) *removes* access of malicious or harmful software that may compromise security of a system, including keyloggers, malware, spyware, and virus software. (CSS, 2023).

Broadly security software covers two areas:

- **Authentication technologies** – the process or action of proving or showing something to be true, genuine, or valid; covering actors, information, and behaviour. The three basic types of authentication a) knowledge-based such as a password or PIN code that only the identified user would know; b) property-based meaning the user possesses an access card, key, key fob or authorized device unique to them; c) biometrics refers to physical attributes, such as fingerprints, facial recognition, and voice patterns. (Gabar et al, 2014) review classifies techniques into traditional (e.g., knowledge-based, object-based) and biometrics (e.g., physiological, behavioral).
- **Anomaly detection** - the general term for detection and prevention, identifying patterns in data that do not conform to a well-defined notion of normal behavior: fraud detection, intrusion detection, abusive user behaviour, or illegality (Garg, 2020). Covering everything from unintentional behaviour to online abuse, illegal activities, and crime.

Defining a clear boundary between 'normal' and 'abnormal' is not always straightforward, as anomalies can be contextual and dynamic. For example, consider a) *Contextual nature of anomalies* - what may be considered normal in one context or situation could be abnormal in another; b) *Evolving and dynamic anomalies* - new patterns emerge or circumstances change, what was previously considered normal might become abnormal, and vice versa; c) *Subjectivity and varying perspectives* - different stakeholders may have different perspectives on what should be considered normal or abnormal.

AI language models, like ChatGPT, can play a role in detecting anomalies in various ways, but they can potentially be exploited by bad actors to craft anomalies or malicious content to target information systems in cyberattacks, making penetration testing more intricate and challenging. It's important to be aware of such risks and take appropriate measures to mitigate them. Collaboration between AI developers and cybersecurity experts is crucial to defend against these sophisticated attacks that utilize AI technologies. The biggest issue being multidisciplinary awareness. Here are some strategies for tighter collaboration:

- **Cross-disciplinary collaboration** - fostering collaboration between AI developers and cybersecurity experts to share knowledge and address challenges from multiple domains.
- **Threat modeling and risk assessment** - identifying and assess potential threats and vulnerabilities specific to AI systems to develop targeted mitigation strategies.
- **Adversarial testing and evaluation** - conducting rigorous testing to identify weaknesses and vulnerabilities in AI models, simulating real-world attack scenarios.
- **Secure development practices** - implementing secure coding guidelines and practices to ensure the development of AI systems with security in mind.
- **Continuous monitoring and incident response** - establishing robust monitoring systems and incident response plans to detect and respond to security breaches or attacks in real-time.

- **Ethical and legal considerations** - addressing ethical and legal implications of AI technologies, ensuring compliance with regulations and ethical guidelines.
- **Community engagement and information sharing** - engaging with the InfoSec community to share knowledge, discuss emerging threats, and collaborate on best practices.

Algorithms and AI

Traditional IST software for individual smart phones and computers typically works on known intrusions, both retrospectively (e.g., scanning memory for viruses) and real-time (e.g., unauthorized access). As discussed, for the future the challenge is detecting previously unseen patterns and in real-time:

- **Anomaly detection** - (Garg, 2020) provides a review of different machine learning models used for anomaly detection, divided into distance based, statistical, classification, and angle techniques.
- **Real-time intervention** - with emergent technologies unforeseen abuses and scams by anonymous participants and algorithms in global environments, requiring near real-time verification and prevention.
- **Predictive detection** – for the future it may be possible to apply proactive 'policing', defined as using data science to be actively involved in predicting, detecting and preventing intrusions. Possibly using algorithmic superintelligence.

User Interfaces

As noted, user interfaces are increasingly an amalgam of virtual environments, and human-centric interaction. Challenges include:

- **Authentication** – authenticating global anonymous humans, algorithms, avatars. and organizations.
- **Anomaly detection** – detecting when participants exhibit illegal or unacceptable behavior, and in real-time.
- **Trust** – an area of growing importance is authenticated whether information is correct or agents can be 'trusted'; a challenge in global environments.

Blockchain Technologies

Previously we discussed algorithm authentication. Given the extent of cybercrime attacks on blockchain technologies, blockchain anomaly detection IST is equally important.

- **Blockchain audit** – auditing blockchain technologies from checking governance processes, to testing a blockchain's operation, to inspecting its inner workings (e.g., smart contract vulnerabilities).
- **Blockchain authentication** – the process of verifying the identity and trust of algorithms interacting with blockchains.
- **Blockchain security** – need for a new class of highly secure blockchain technologies (e.g., encryption).

Decentralized Infrastructures

Organizations are moving from centralized cloud computing to decentralized infrastructures (cf. crowd computing) to retain control over their (valuable) datasets and manage access whether by humans or algorithms. A challenge for InfoSec is developing a new generation of IST for verification. Examples include:

- **Identity verification** - a service used to verify the credentials of a unique (decentralized) identity that an agent (e.g., human, algorithm, avatar) claims to have with the supporting data they possess.
    - *Agent profile* – a collection of information and settings, including identity, personal details, preferences, characteristics, and behavior associated with a user.
    - *Hyper-personalization* – highly personalized profiling is increasingly important, with machine learning and psychology providing insights into a user's behavior, objectives, values, or incentives, and used for monitoring behavior.
    - *Multi-factor authentication* - an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.
- **Web3 infrastructure** – a web3 data architecture that seeks to integrate decentralized and privacy-preserving datasets across an organization or group of collaborating organizations.
    - *Blockchain DLT* - using distributed ledger, cryptocurrencies, tokenization, and smart contracts for secure distributed databases.
    - *Federated learning* – a machine learning technique that trains models utilizing distributed datasets. It is often used with privacy enhancing technologies, such as differential privacy. It combines the power of decentralized machine learning analytics with privacy-preserving data infrastructure for data security.
- **Trust detection** – the new 'fraud detection': trust in Agents, information, and algorithms: a) *truthfulness* in information generated, b) *blockable* content deemed inappropriate due to social norms or the law; c) *integrity* in systems of the anonymous Agents (e.g., humans, algorithms, avatars, androids, and organizations); d) *conduct* where (AGI) algorithms and Agents understands bias, ethics, risk and legality.
- **Open IST** – a possible approach is Open IST (cf. Open Banking) intended as IT services that use open APIs enabling third-party developers to build applications and services supporting information security and law enforcement. The goal is greater security transparency options for account holders, ranging from private data, Agents profiles, to emerging cybercrimes.

In summary, simplistically, traditional IST addresses, standalone centralized systems of individual smart phones and computers, under attack from mostly identifiable intrusions, some of which can even be addressed retrospectively. In contrast, future information security technology (cf. IST 3.0) increasingly involves decentralized ecosystems, anonymous agents (e.g., humans and algorithms), global jurisdictions and the requirement of real-time intervention, as illustrated by Figure 10.

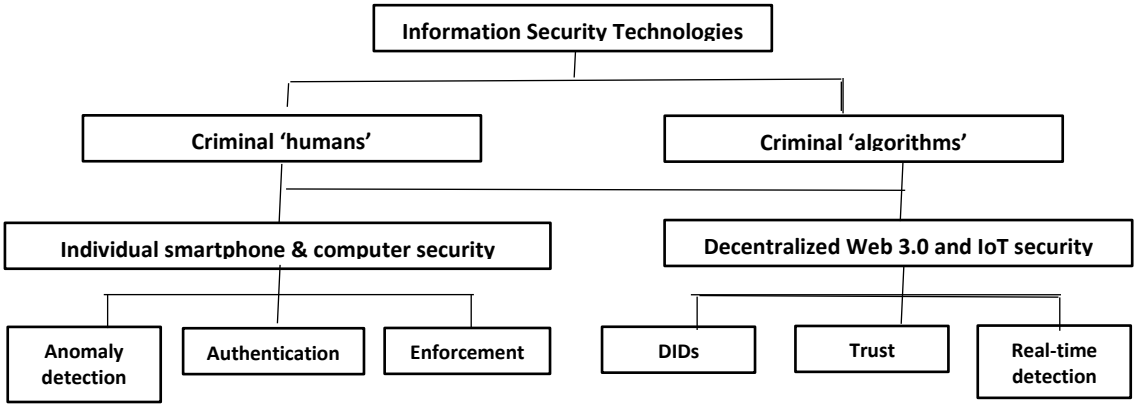

Figure 10: Information Security Technologies (InfoSec)

Whereas information security technology (InfoSec) is concerned basically with cybercrime detection and prevention, law enforcement (LawTech) is concerned with detection and prosecution.

5. Law Enforcement (LawTech)

The key challenge for law enforcement is **awareness**: since cybercrime increasingly operates in a 'dark' criminal ecosystem.

As a definition, increasingly **LawTech** is used for all aspects of (DeepTech) technologies for delivering law enforcement services: *PoliceTech* the wide range of scientific and technological methods, techniques, and analytics used in policing; *SupTech* supporting 'supervisors' (e.g., regulators, police, prosecutors, probationers, judiciary); *RegTech* regulatory monitoring, reporting, and compliance. Whereas *LegalTech* supports legal services firms.

For law enforcement cyberspace is the proverbial hidden 'parallel universe'. At a basic level, stakeholders (e.g., law enforcement, regulators, policy makers, politicians) need: a) LawTech knowledge-transfer 'awareness' training; b) a radical rethinking of their operational models; and c) a programme to leverage emerging DeepTech innovations. As we have argued, with cybercrime: firstly, the dynamic nature of emerging technologies requires real-time intervention to possibly unseen inappropriate and criminal activities; secondly, participants are increasingly anonymous humans, algorithms, and avatars; and thirdly, innovations and abuses frequently occur in cyberspace domains unfamiliar to law enforcement.

Europol (Europol, 2023) recently conducted a series of workshops involving subject matter experts from various areas. The objective was to examine the potential misuse of Large Language Models (LLMs) like ChatGPT by criminals and to explore how these models could assist investigators in their daily work. The workshops aimed to observe the response of LLMs when exposed to criminal and law enforcement scenarios, enabling law enforcement agencies to comprehend the challenges posed by both derivative and generative AI models. ChatGPT is already able to facilitate a significant number of criminal activities, ranging from helping criminals to stay anonymous to specific crimes including terrorism and child exploitation. As the technology advances and new models emerge, it is crucial for law enforcement to remain proactive in understanding these developments to effectively counteract abuse and leverage potential benefits.

An interesting illustration of stakeholders needing LawTech awareness is the case of a US radio presenter suing OpenAI for libel after ChatGPT comprehensively fabricated legal accusations, including inventing entire legal documents alleging embezzlement of funds (Nolan, 2023). While this incident raises concerns, it also highlights the critical need for a better understanding of AI generative models and their capabilities, particularly among end-users. It underscores the importance of educating individuals on the limitations and potential risks associated with these models to make informed judgments when interacting with AI-generated content.

Context

Conceptually LawTech spans the set of rules individuals, organizations and now algorithms, must follow to conform to society, a specification, policy, standard or law:

- **Social norms** - informal, mostly unwritten, rules that define acceptable and appropriate actions of individuals, groups, organizations, and societies, thus guiding human behaviour.
- **Regulatory Compliance** – is the state of being in accordance with established guidelines or specifications, or the process of becoming so. An example being the regulation and enforcement of the laws and rules that exist within the financial services sector and capital markets.

- **Laws/Statutes** – the system of rules which a particular country or community recognizes as regulating the actions of its members and which it may enforce by the imposition of penalties, passed by a legislative body.

Social norms are the informal rules that govern behavior in groups, organizations, and societies. Notably, social norms vary widely from country-to-country, region, and religion. The four types of social norms are: a) *folkways* - are behaviors that are learned and shared by a social group that we often refer to as "customs"; b) *mores* - re culturally-specific expectations that are set to determine how someone is expected to behave in specific society; c) *taboos* - a strict prohibition of behavior that society holds so strongly that violating it results in extreme disgust or expulsion from the group or society; and d) *laws* - rules that define acceptable and appropriate actions. within a given group or community, thus guiding human. behaviour. Here recommender systems and generative AI could be used to filter content that would be considered offensive by a specific community (e.g., Muslims).

Enforcement ranges from: peer pressure, to cyber abuse (cf. Woke), even online threats of violence.

Regulatory Compliance - the traditional regulatory model involves setting applicable regulations for registered individuals and institutions in defined jurisdictions under national laws. Reports and data are collected retrospectively and analyzed to investigate and where necessary to prosecute activities. However, the pace of innovation and the amount of data that is being produced whether for crimes or compliance purposes pose insurmountable challenges to command-and-control type regulation (Sinclair, 1997). The scale of the challenge facing regulators is illustrated by the UK Bank of England Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA) current data reporting figures. PRA-regulated firms must sort through Exabytes of data to fulfil reporting requirements. These firms pay £4.5Bn/$5.17Bn pa to do so yet only 2% of received data is reviewed by regulators globally. That said, (financial) regulators have responded quickly to cryptocurrencies (e.g., classifying them as regulated securities) and influencers (e.g., teenage TikTok financial 'influencers'), but still retrospectively.

Future law enforcement needs to address the dynamic nature of emerging technologies, and the societal need to balance *innovation* and *regulation*, against a background of opportunism: entrepreneurial and criminal (cf. LawTech 3.0):

- **Real-time regulation** – leveraging decentralized web3 technologies and AI for real-time and on-demand reporting of compliance.
- **Regulatory coordination** – establishing secure regulatory networks and standards to support national and international collaboration to reduce overregulation/cost.
- **RegTech Innovation** – supporting RegTech innovation, while monitoring innovations in a safe sandbox environment, as pioneered by the UK Financial Services Authority Innovation Hub (FCA, 2023)

Law/Statutes – the traditional law enforcement and regulatory models are essentially similar. Laws are based on identifiable individuals and organizations in defined jurisdictions. However, authorities can take years to introduce legislation: conducting consultations, establishing committees, producing whitepapers, responding to lobbying, drafting legislation, forming a political consensus, and voting. As examples of the changing SupTech models:

- **Judicial guidance** – in Singapore victims can use AI to find out if they are likely to win in court.
- **Algorithmic dispute resolution** - the automation of professional dispute resolution using AI and Blockchain technologies (Barnett & Treleaven, 2018).

- **Online filing** - online case filing and management system for claims in small claims courts and tribunals. Discovery of electronic documents is now widespread. (Lederer 1997).
- **Virtual courts** – a remote court where some or all of the participants involved in legal proceedings such as a trial or hearing takes part remotely instead of meeting in-person.
- **Recidivism algorithms** - used to assess a criminal defendant's likelihood of committing a future crime.

Digitalization is now a key pillar of legal system transformation, especially addressing issues such as inequality and access to Justice. However, with controversial automated algorithmic sentencing, SupTech continues to keep 'the human (judge) in the loop'.

To address an 'explosion' of cybercrime, law enforcement arguably needs to utilize the very same web3, AI and emerging technologies that are providing criminals with a wealth of opportunities.

- **Real-time enforcement** – leveraging decentralized web3 technologies and AI for real-time and on-demand reporting of (potential) criminal activities.
    - *Data* – obtaining data in real-time or on-demand.
    - *Analytics* – employing real-time anomaly and intrusion detection.
    - *Resilience* – promoting decentralized environments that support privacy, federated analytics, and resilient IoT infrastructures.
- **Coordination** – establishing secure law enforcement networks and standards to support national and international collaboration to address globalization.
    - *LawTech awareness* - stakeholders (e.g., law enforcement, regulators, policy makers, politicians) need DeepTech, CrimeTech and LawTech 'knowledge' training.
    - *Law enforcement standards* – to support automation open standards are needed for reporting, and for interrogation of national laws and regulator's handbooks.
    - *Law enforcement coordination* – to support coordination, agencies require secure infrastructures, since an agent is frequently subject to multiple national legislation and by laws in multiple international jurisdictions.

Courts and Tribunals (JudicialTech)

Regarding law enforcement, the rapid adoption of emerging technology in courts has transformed criminal and civil trials. For example, prosecutions in the UK now rely increasingly on digital evidence, such as Body Worn footage, CCTV, Cell Site and mobile data, and messaging (EncroChat).

In a broader context, the use of judicial algorithms raises existential issues around the future of the legal system. Susskind distinguishes between the use of predictive systems such as LexMachina (LexMachina, 2023) which predict the outcome of legal cases and generative systems such as LegalFly (LegalFly, 2023) for contract review (Susskind, 2023). D'Amato asked the question, 'Can/Should Computers replace Judges? His conclusion was that there are aspects of human judgment that should not be reduced to algorithms. (D'Amato 1977).

In the UK Sir Geoffrey Vos, Head of Civil Justice, recommended that judicial support using emerging technologies should be encouraged:

- **Document review and 'triable issues' –** huge datasets create delay, so automation of pretrial investigation and discovery is widely beneficial.
- **Legal analytics** – tools such as LexMachina use AI data science to analyze millions of pages of docket entries and documents to provide litigation insights on courts, judges, lawyers, law firms, and parties.
- **Judicial guidance** –victims can use AI in Singapore to find out if they are likely to win in court.

In considering the extent to which AI technologies can render the legal system unfair, it is important to distinguish use by Lawyers (LegalTech) and by the Judiciary (JudicialTech). Addressing concerns around machines making sentencing decisions, Vos recommended appeal to a human Judge as an 'escape valve' (Vos 2023). Lederer warns of the dangers of bias in the design of the algorithm and large amounts of inaccurate and unverified data (Lederer 2022). Controversial examples include:

- **Facial recognition** – facial recognition algorithms while promoted as speeding the identification and apprehension of suspects, have mistakenly identified Afro American and Asian men (Clearview 2020).
- **Recidivism tools** – machine learning technology intended to predict the likelihood of future criminal conduct, was challenged in the 2017 Wisconsin State Supreme Court when used for sentencing State v Loomis. (Loomis 2016).

Lastly, Wachter and colleagues (Wachter 2020) called for consistent assessment procedures to define common standards for the assessment and detection of prima facie automated discrimination. Kerrigan contends that this approach is flawed and argues that AI should not replace Judges (Kerrigan 2022).

Algorithms and AI

In this section we focus on AI technologies for the future detection and prosecution of crimes and inappropriate behaviour: from misinformation to rogue algorithms. The challenge of algorithms and AI is ensuring benign moral alignment with human beings. Data science examples include:

- **Criminal information** – this covers incitement and discrimination, deepfake impersonation, and crimeware software, but necessarily misinformation or copyright infringement which are civil law matters.
- **Proactive enforcement** – for example, predictive policing involves using algorithms to analyze massive amounts of information in order to predict and prevent potential future crimes, such as terrorism and even civil disorder. Related is proactive policing, usually defined as the predisposition of law enforcement to be actively involved in preventing and investigating crime.
- **Judicial algorithms** –algorithms that use statistical probabilities based on factors such as age, employment history, and prior criminal record to predict a defendant's likelihood of recidivism, and controversially recommend sentencing.

User Interfaces

User interfaces (UIs) will increasingly deploy totally convincing deepfakes, dark content and criminal algorithms/avatars. This may require a modification of existing laws to encompass not just physical humans but increasing 'digital' algorithms generating content and activities.

- **Dark content** – the detection and prosecution of creators of deviant and illegal content. Notably deviant (avatar) content may not be covered by existing laws.
- **Criminal algorithms** – law enforcement may detect criminal algorithms, but it may be impossible to identify the instigator (cf. traditional computer viruses).

Blockchain Technologies

The challenge of blockchain is bringing technologies within the scope of existing laws.

- **Cryptocurrencies** – governments are increasingly tackling cryptocurrencies by classifying them as (financial) securities, subject to existing laws, and rigorously prosecuting crypto

exchanges for illegal operation. This is likely to encourage crypto companies to engage in jurisdictional arbitrage.

- **Smart contracts** – a smart contract does not typically constitute a valid binding agreement in law, although a smart legal contract is intended to be both executable by a machine and legally enforceable. Hence changes to the Law may be required to cover all aspects.

Decentralized Infrastructures

We have argued that due to the fluid and opportunistic nature of cybercrime, law enforcement needs to adopt a new decentralized and automated operational model. Including LawTech awareness training, law enforcement secure infrastructures, and encouragement of LawTech innovation.

- **Horizon scanning** – detecting early signs of potentially important developments through a systematic examination of potential threats and opportunities, with emphasis on new technologies.
- **Knowledge-transfer** – raising awareness amongst stakeholders of CrimeTech and LawTech emerging technologies.
- **LawTech infrastructure** - to support secure networks for national and law enforcement collaboration together with (e.g., XML) information standards for coordination.
- **Predictive analytics** – pioneering the use of AI algorithms to analyze massive amounts of information in order to (even) predict and help prevent potential future cybercrimes.
- **Rapid-start laws** – to engage with Justice Ministries and politicians to provide legal provisions for rapid response to cybercrime 'innovations' (cf. Financial Regulators).
- **Sandboxes** – provide a LawTech testing environment where new or untested technologies and software can be run securely.
- **Self-reporting** – to engage with AI and emerging technologies' communities to encourage self-regulation and self-reporting of emerging cybercrime trends.
- **Tech sprints** – essentially hackathons, coding events that bring LawTech programmers and other interested people drive innovations.

In summary, the major cybercrime challenge for law enforcement is **awareness** for individuals, organizations, and law enforcement. *Streetwise* is the colloquial term for individuals having the experience and knowledge necessary to deal with the potential difficulties or dangers of life in an urban environment. We probably need a new term *Cyberwise* to cover experience and knowledge of existing and emerging cyber threats:

- **LawTech** – LawTech and CrimeTech awareness training for all stakeholders (e.g., law enforcement, regulators, policy makers, politicians).
- **PoliceTech** – a) *proactive policing* involves using algorithms to analyze massive amounts of information in order to predict and help prevent potential future; b) *proactive enforcement* is usually defined as the predisposition of a police officer to be actively involved in preventing and investigating crime; predictive enforcement; and futuristically c) *predictive policing* systems dedicated to apprehending and detaining people before they have the opportunity to commit a crime.
- **SupTech** – supervisory technology, includes automation of justice including a) *delegation of enforcement* means police officers can apply penalties for minor crimes, opening the possibility of real-time justice; b) *recidivism algorithms* used to assess a criminal defendant's likelihood of committing a crime; c) *algorithmic dispute resolution* uses AI to automate professional arbitration and dispute resolution.

- **RegTech** – web3 decentralized technology, plus on-demand and near real-time report for automating compliance and regulation.

Besides LawTech training for stakeholders, the Police and Judiciary will benefit form their own highly secure decentralized infrastructure for coordination, but given the pervasive global nature of cybercrime, a specialist international law enforcement agency may even be required, or an expansion of Interpol.

6. Conclusions

Finally, it is generally agreed that society is on the threshold of an 'explosion' of cybercrime. Law enforcement, InfoSec providers and arguably the Judiciary need new operating models and to embrace AI and emerging technologies to address the inevitable rise of cybercrime. Disruptors include **agents** moving from the realm of humans to 'Superintelligence' algorithms; **devices** moving from single smartphones and computers to autonomous networks of IoT devices; **deepfakes** moving from inaccurate data to totally convincing 'fake' text, images, audio, and video; and **globalization** – moving from identifiable humans and organizations in legal jurisdictions, to digital agents operating anonymously in global virtual environments.

This paper shows how AI and emerging technologies are closely tied to digital, physical, and political security. AI can be used to both launch and defend against cyberattacks. Its introduction into society changes the attack surface that bad actors can target. As AI systems' capabilities grow, they will surpass humans in many areas. Care must be taken to ensure that the trial process retains judicial independence so as to retain public confidence in the legal system. Preparing for the potential malicious uses of AI is an urgent task. Social engineering attacks will become more sophisticated, and companies are increasingly pursuing actions to defend against massive hacking by automating cyber-defense systems. However, AI-based defense can only be a complete solution with help, especially when we look beyond the digital domain. More work should be done to understand the balance of openness in AI, verify system robustness, and adopt policy frameworks for the new decentralized digital world that is coming. Advanced AIs may cause unprecedented damage to our societies, so we must prepare today before these more potent misuse potentials are realizable. Researchers and policymakers should learn from other domains with more extended experience in preventing and mitigating malicious use to develop tools, policies, and norms appropriate to AI applications (Brundage, 2018).

To conclude, we are truly experiencing a 'tsunami' of emerging technologies. In the futuristic film Minority Report a predictive policing system dedicated to apprehending and detaining people before they have the opportunity to commit a crime. This is no longer pure fantasy for law enforcement but needs updating to address Superintelligence algorithms and avatars. However, the applicability and acceptance of such a predictive policing system would break the principle of presumption of innocence and vary across jurisdictions, influenced by the unique legal, cultural, and societal factors at play. It would require careful consideration of the balance between crime prevention, individual rights, and the principles of the legal system in each country to which any AI agency shall conform.

7. Acknowledgements

We especially wish to thank Dr Enzo Fenoglio and Dr Martin Schoernig who undertook comprehensive reviews of this paper.

8. Further Reading

(AGI, 2023) Algorithmic General Intelligence, Wikipedia, https://en.wikipedia.org/wiki/Artificial_general_intelligence

(Amatriain et al, 2023) Amatriain, X., et al, Transformer models: an introduction and catalog, https://arxiv.org/pdf/2302.07730.pdf

(Anomaly, 2023) Anomaly Detection, Wikipedia, https://en.wikipedia.org/wiki/Anomaly_detection

(ASI, 2023) Artificial Superintelligence, TechTarget., www.techtarget.com/searchenterpriseai/definition/artificial-superintelligence-ASI

(Atlam & Wills, 2019) Atlam, H., Wills, G., IoT Security, Privacy, Safety and Ethics, www.researchgate.net/publication/332859761_IoT_Security_Privacy_Safety_and_Ethics

(AWS, 2023) What is Blockchain technology?, AWS, https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc (Fortson, 2023) Fortson, D., Ways AI will change all our lives, Sunday Times Tech Talk, 12th February 2023.

(Barnett & Treleaven, 2018) Barnett, J., Treleaven, P., Algorithmic Dispute Resolution—The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies, The Computer Journal, Volume 61, Issue 3, March 2018, Pages 399–408, https://doi.org/10.1093/comjnl/bxx103

(Bellasio et al., 2020) Jacopo Bellasio, Erik Silfversten, Eireann Leverett, Anna Knack, Fiona Quimbre, Emma Louise Blondes, Marina Favaro, Giacomo Persi Paoli, How could technological developments influence the future of cybercrime?, www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA137-1/RAND_RRA137-1.pdf

(Big Bang, 2021) Big Bang financial market (regulation). Wikipedia, https://en.wikipedia.org/wiki/Big_Bang_(financial_markets)

(Bloomberg, 2023) Introducing BloombergGPT, https://www.bloomberg.com/company/press/bloomberggpt-50-billion-parameter-llm-tuned-finance/

(Boreham, 2022) Boreham, J., An In-Depth Guide on Metaverse Avatars & How to Create One, https://metaverseinsider.tech/2022/07/16/metaverse-avatars/

(Brozek, 2023) B. Brożek, M. Furman, M. Jakubiec, B. Kucharzyk, The black box problem revisited. Real and imaginary challenges for automated legal decision making, Artificial Intelligence and Law (2023) 1–14. doi:10.1007/s10506-023-09356-9.

(Brundage, 2018) Brundage, Miles et.al., The malicious use of artificial intelligence : forecasting, prevention, and mitigation, http://arks.princeton.edu/ark:/88435/dsp01th83m203g

(Carmiel, 2022) Carmiel, D., 5 Trends Shaping The Future Of Cybercrime Threat Intelligence, Forbes, https://www.forbes.com/sites/forbestechcouncil/2022/12/19/5-trends-shaping-the-future-of-cybercrime-threat-intelligence/?sh=47a1e7d530a6

(Chessen, 2017) Chessen, Matt, The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, And Threaten Democracy… And What Can Be Done About It. https://www.jstor.org/stable/resrep03728

(ChinaSCS, 2023) China Social Credit System, Wikipedia, https://en.wikipedia.org/wiki/Social_Credit_System

(Clearview 2020 The New York Times January 24 2020. New Jersey bars police from using Clearview Facial Recognition App, https://www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html

(CNBC, 2022) Crypto scammers took a record $14 billion in 2021, CNBC, https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html#:~:text=Scammers%20around%20the%20world%20took,%243.2%20billion%20worth%20of%20cryptocurrency

(D'Amato, 1977) D'Amato, A., Can/should computers replace judges?. Georgia Law Review, 11,11-36, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781304

(Dargan et al., 2022) Shaveta Dargan, Shally Bansal, Munish Kumar, Ajay Mittal & Krishan Kumar Augmented Reality: A Comprehensive Review, https://link.springer.com/article/10.1007/s11831-022-09831-7

(DID, 2023) Decentralized identifiers (DID) v1.0, W3C, https://www.w3.org/TR/did-core/

(Edwards, 2023) Edwards, B., Microsoft's new AI can simulate anyone's voice with 3 seconds of audio, https://arstechnica.com/information-technology/2023/01/microsofts-new-ai-can-simulate-anyones-voice-with-3-seconds-of-audio/

(Europol, 2023), ChatGPT - The impact of Large Language Models on Law Enforcement, a Tech Watch Flash Report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg.

(EU AI, 2022) Artificial intelligence: threats and opportunities, European Parliament, www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities

(EU EIDAS, 2023) Shaping Europe's digital future, European Commission, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

(FCA, 2023) UK Financial Conduct Authority Innovation Hub, https://www.fca.org.uk/firms/innovation

(Forbes, 2021) Napoletano, E., Schmidt, J., Decentralized Finance Is Building a New Financial System, www.forbes.com/advisor/investing/defi-decentralized-finance/

(Gaber et al, 2014) Tarek Gaber, T et al, Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues, https://www.researchgate.net/publication/268388162

(Garg, 2020) Sahil Garg, Algorithm selection for Anomaly Detection, Medium, https://medium.com/analytics-vidhya/algorithm-selection-for-anomaly-detection-ef193fd0d6d1

(GenAI, 2023) Golden, Generative AI, https://golden.com/wiki/Generative_AI-DZDYKZP

(GTP, 2023) Generative Pre-Trained Transformers, Wikipedia, https://en.wikipedia.org/wiki/Generative_pre-trained_transformer

(GPT 4, 2023) GPT-4 is OpenAI's most advanced system, producing safer and more useful responses, OpenAI, https://openai.com/product/gpt-4 (Hyper Personalization, ?) Hyper personalization, https://cdn2.hubspot.net/hubfs/2389934/eBooks/Hyper-Personalization-whitepaper-dotCMS.pdf

(InfoSec, 2023) Computer Security, Wikipedia, https://en.wikipedia.org/wiki/Computer_security

(IoT, 2023) Internet of Things, Wikipedia, https://en.wikipedia.org/wiki/Internet_of_things

(Itsekson, 2023) Itsekson, A, What Are the 7 Layers of IoT Architecture?, Jelvix, https://jelvix.com/blog/iot-architecture-layers

(Kaspersky, 2023) What Are Scam Websites and How To Avoid Scam Websites, https://www.kaspersky.com/resource-center/preemptive-safety/scam-websites

(Kerrigan, 2022) Artificial Intelligence – Law and Regulation, www.e-elgar.com/shop/gbp/artificial-intelligence-9781800371712.html

(Koshiyama et al, 2020) Koshiyama, A., Firoozye, N., Treleaven, P., Algorithms in Future Capital Markets, SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3527511

(Koshiyama et al, 2021) Koshiyama, A., et al, Towards Algorithm Auditing, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3778998

(Lawson, 2023) Lawson, G., What is generative AI? Everything you need to know, https://www.techtarget.com/searchenterpriseai/definition/generative-AI

(Lederer, 2022) Lederer, F., Problematic AI When Should we use it? https://scholarship.law.wm.edu/popular_media/571/

(LegalFly, 2023) Supercharging Legal with AI, LegalFly, https://www.legalfly.ai/

(Loomis 2016) State of Wisconsin v Loomis, No 2015AP157-CR, https://scholar.google.com/scholar_case?case=3222116451721963278&hl=en&as_sdt=6&as_vis=1&oi=scholarr

(LexMachina, 2023) Predict the behavior of courts, judges, lawyers and parties with Legal Analytics, LexMachina, https://lexmachina.com/

(Maskun et al, 2020) Maskun, M., et al., Qualifying Cyber Crime as a Crime of Aggression in International Law, Journal of East Asia and International Law, www.researchgate.net/publication/347143188_Qualifying_Cyber_Crime_as_a_Crime_of_Aggression_in_International_Law

(MIT, 2023) ML Confidence Predictions, MIT,., www.marktechpost.com/2023/02/18/mit-researchers-have-developed-a-new-technique-that-can-enable-a-machine-learning-model-to-quantify-how-confident-it-is-in-its-predictions/?utm_source=substack&utm_medium=email

(Mihov et al, 2022) Mihov, A-H, Firoozye, N., Treleaven, P., Towards Augmented Financial Intelligence, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4148057

(Moy & Gadgil, 2022) Moy, C., Gadgil, A., Opportunities in the Metaverse , www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf

(Nolan, 2023) Nolan, B., Radio Hosts sues OpenAI, https://www.businessinsider.com/openai-chatgpt-fake-legal-case-ai-georgia-2023-6?r=US&IR=T

(Pixelplex, 2023) Smart contract vulnerabilities, https://pixelplex.io/blog/smart-contract-vulnerabilities/

(PlayDapp, 2022) Play to earn games, https://playdapp.io/document/P2E_NFT_Game_Analysis_Playdapp_Report_en.pdf

(Rand, 2013) Predictive Policing - Forecasting Crime for Law Enforcement, www.rand.org/content/dam/rand/pubs/research_briefs/RB9700/RB9735/RAND_RB9735.pdf

(Riedl, 2023) Riedl, M., A Very Gentle Introduction to Large Language Models without the Hype, https://mark-riedl.medium.com/a-very-gentle-introduction-to-large-language-models-without-the-hype-5f67941fa59e

(Resnick & Varian, 1997) Resnick, P., Varian, H., Recommender systems, Commun. ACM, March 1997, https://dl.acm.org/doi/pdf/10.1145/245108.245121

(Rude-Jensen et al, 2021) Rude Jensen, J., von Wachter, V., Ross, O., An Introduction to Decentralized Finance (DeFi), www.researchgate.net/publication/351405518_An_Introduction_to_Decentralized_Finance_DeFi

(Sirimanne, 2022) Sirimanne, S., What is 'Industry 4.0' and what will it mean for developing countries?, United Nations UNCTAD, https://unctad.org/news/blog-what-industry-40-and-what-will-it-mean-developing-countries#:~:text=Industry%204.0%20refers%20to%20the,%2C%20energy%20efficiency%2C%20and%20sustainability.

(Susskind, 2023) Susskind, R., Tomorrow's Lawyers, https://global.oup.com/academic/product/tomorrows-lawyers-9780192864727

(Treleaven et al, 2019) Treleaven, P., Barnett, J., Koshiyama, A., Algorithms: Law and Regulations, IEEE COMPUTER, https://ieeexplore.ieee.org/document/8672418

(Treleaven et al, 2022a) Treleaven, P., Greenwood, A., Pithadia, H., Xu, J., Web 3.0 Tokenization and Decentralized Finance (DeFi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4037471

(Treleaven et al, 2022b) Treleaven, P., Smietanka, M., Pithadia, H., Federated Learning, IEEE COMPUTER, https://ieeexplore.ieee.org/document/9755189

(Treleaven et al, 2023) Treleaven, P., et al, Decentralized Financial Regulation (DeReg): using Web 3.0, machine learning, blockchain and data science technologies to 'rethink' Regulation.

(Tyler et al, 2018) Tyler, P. et al, Internet of Things realising the potential of a trusted smart world, Royal Academy of Engineering, www.researchgate.net/publication/363923496_Internet_of_Things_realising_the_potential_of_a_trusted_smart_world

(UKAI, 2023) UK Government ai-regulation-a-pro-innovation-approach, https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

(Vos, 2023) Vos, G., The future of London as a pre-eminent dispute resolution centre: opportunities and challenges, https://www.judiciary.uk/speech-by-the-master-of-the-rolls-the-future-of-london-as-a-pre-eminent-dispute-resolution-centre-opportunities-and-challenges/

(W3C, 2022) W3C Decentralized Digital Identifiers (DID), https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers

(Wachter 2020) Wachter et al, Why Fairness Cannot Be Automated, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547922

(Waldert, 2016) Waldert, S; (2016) Invasive vs. Non-Invasive Neuronal Signals for Brain-Machine Interfaces: Will One Prevail? Frontiers in Neuroscience , 10 , Article 295. 10.3389/fnins.2016.00295.

(Yan, Wilson, 2020) Yan, LK., Wilson, C., Developing AI for Law Enforcement in Singapore and Australia, Communications of the ACM, April 2020, Vol. 63 No. 4, Page 62, 10.1145/3378418.

9. Appendix 1 – Emerging Technologies

This section lists key components of these emerging technologies:

- **Agents** - moving from the realm of humans to algorithms, avatars, androids in global environments.
  - *Algorithm* - a procedure used (by a device) for performing a computation or executing a task.
  - *Avatar* - is a graphical representation of a user or the user's character or person in a virtual environment.
  - *Android* - a functional and realistic humanoid robot or other artificial being, often made from a flesh-like material.
- **Algorithms** – comprising computational statistics (e.g., Monte Carlo methods), complex systems (e.g., Agent-Based systems), and AI (e.g., Artificial Neural Networks). AI covers:
  - *Traditional ML* - using machine learning (ML) for automation such as data scraping, analytics, and transacting (e.g., trading).
  - *Generative AI* - – large language model algorithms (such as ChatGPT) that can be used to create 'human-like' content, including audio, images, text, videos, even code and simulations. These generative pre-trained transformers (GPT) use large language models (LLMs) based on deep learning neural networks with billions of machine learning parameters (GTP, 2023).
  - *Artificial General Intelligence* - AGI is machine intelligence that can solve problems as well as a human. The concern is losing control of the algorithms.
  - *Artificial Superintelligence* - ASI is machine intelligence that can solve all problems better than people, and will be a watershed for humanity and tech.
- **User Interfaces (UI)** – increasingly users interacting using natural language and through virtual environments, such as the metaverse.
  - *Natural language processing* – NLP is the application of computational techniques to the analysis and synthesis of text, images, speech, and video.
  - *Chatbots* - at the most basic level, a computer program that simulates and processes human conversation (either written or spoken), allowing humans to interact as if they were communicating with a real person.
  - *Virtual and Augmented reality* - an immersive virtual environment in which users can interact with a computer-generated environment and other users. Avatars in the Metaverse are digital representations of people (Boreham, 2022).
- **Blockchain DLT**- – a distributed database that maintains a continuously growing audit trail of ordered records, called blocks, linked using cryptography (AWS, 2023).
  - *Distributed ledger* - a distributed database that is consensually shared and synchronized across multiple sites, institutions, or geographies, accessible by multiple people.
  - *Cryptocurrencies* - a digital currency, which is an alternative form of payment created using encryption algorithms.
  - *Tokenization* - tokenization is the process of allocating a unique identifier to something of value and hence a digital token that's usable on a blockchain application (Treleaven et al, 2022a).
  - *Smart contracts* - a computer program or a transaction protocol that automatically executes, according to the terms of a contract or an agreement.
  - *Layer 1* – the name given to a base bockchain such as Bitcoin, Ethereum or Polkadot. It is the first level of the ecosystem and corresponds to the main chain of the network. Layer 2 solutions and sidechains can be built on top.

- **Decentralized Infrastructures** – integrated systems comprising Web 3.0 decentralized application (Dapps) that can operate autonomously (using Blockchain technology) and IoT infrastructures of smart devices.
    - *Web 3.0* – the new decentralized iteration of the WWW.
    - *Digital identifiers* – unique information used by computer systems to identify and interact with an external Agent – a person, organization, or smart device.
    - *Smart devices* – smartphones, computers, Bluetooth devices using short-range wireless, and sensors embedded in vehicles, machines, and the built environment.
    - *IoT infrastructures* – internet of physical objects - 'things' - that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.

10. Appendix 2 – Cybercrime definitions

This section lists definitions of current cybercrimes:

- **Botnet** - a network of private computers infected with malicious software and controlled as a group without the owners' knowledge.
- **Clickjacking** - the malicious practice of manipulating a website user's activity by concealing hyperlinks beneath legitimate clickable content, thereby causing the user to perform actions of which they are unaware.
- **Crimeware** - a range of malicious software designed to carry out or facilitate illegal online activity. Old-school malware written for 'fun' has given way to a new era of AI-powered 'crimeware' designed for spamming, data theft, or extortion.
- **Criminal algorithms** – as algorithms become increasingly intelligent through AGI and ASI, criminal algorithms will be deliberately created, but also have propensity to evolve (cf. feral) into nefarious algorithms.
- **Cyberbullying** - sending, posting, or sharing negative, harmful, false, or malicious content about someone (e.g., revenge porn).
- **Cyber espionage** – spying by corporations, governments, and criminal gangs for: economic espionage, extortion, state-sponsored cybercrime, military espionage, cyber warfare targeting national infrastructure, and terrorism.
- **Cyber extortion** - the use of various tactics, such as phishing, malware, and DoS attacks, to threaten reputational damage, or hold a victim's data or systems hostage until a ransom is paid.
- **Cyberfakes** – a term describing fake companies, platforms and investment scams, especially prevalent involving cryptocurrencies, including Initial Coin Offerings (ICO) and fake exchanges.
- **Dark patterns** – a dark pattern is a user interface that has been carefully crafted to 'trick' users into doing things, such as renewing contracts at an inflated price, signing up for recurring bills, or buying overpriced insurance with their purchase.
- **Dark content** – information and algorithmic content, including on the dark web, that is either inaccurate, disapproved of by public opinion, deviant or illegal.
- **Dark web** – the part of the Web only accessible by means of special software, such as the TOR browser, allowing users and website operators to remain anonymous or untraceable.
- **Data breaches** - an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.
- **Deepfakes** - creating convincing text, images, speech and video hoaxes, resulting in bogus information, malicious content, and fakes used for criminal activities.
- **Denial-of-service** - DoS describes a class of cyber-attacks designed to render a service inaccessible. A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.
- **Digital addiction** – digital engagement resulting in impulse control disorders (ICDs) characterized by excessive and harmful behaviors. Such as obsessive use of social media, mobile devices, the Internet, betting sites, or video games.
- **Hacking** - the gaining of unauthorized access to data in a system or computer (cf. black hat, white hat, and grey hat hackers).
- **Hoax emails** – a scam that is distributed in email form, designed to deceive, and defraud email recipients, often for monetary gain.

- **Identity theft** - a crime in which an attacker uses personal information, and increasingly deepfakes of a victim and misuses it to act in the victim's name.
- **Malware** - software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. An example being a 'wiper'; a class of malware intended to erase (hence the name) the hard drive of the computer it infects, maliciously deleting.
- **Man-in-the-middle attack** - An attack where the adversary positions themself in between the user and the system so that they can intercept and alter data traveling between systems (e.g., WIFI pineapple).
- **Phishing** - using emails, phone calls or other messages purporting to be from reputable individuals and companies to induce victims to reveal personal information, such as passwords, credit card numbers, or crypto wallet.
- **Pump and dump** - a type of scam known as a "rug pull." These scams involve market manipulators who spread false information about a crypto project and eventually sell their tokens (or "pull the rug") after enough retail investors buy into the currency.
- **Ransomware** - a type of malicious software designed to block access to a computer system until a sum of (cryptocurrencies) money is paid.
- **Reputational attacks** – for example revenge porn is the sharing of private, personal materials, either photos or videos, of another person, without their consent and with the purpose reputational damage.
- **Romance scams** - occur when a criminal adopts a fake online identity to gain a victim's affection and trust.
- **Scareware** - malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection, or fake ChatGPT apps.
- **Spyware** - any software that installs itself on a victim's computer and starts covertly monitoring online behavior without their knowledge or permission; increasingly used by governments to monitor opponents or industrial espionage.
- **Stalkerware** - monitoring smartphone apps, blue tooth tracking devices or spyware that are used for cyberstalking.
- **Trojan horse** - a type of malware that disguises itself as legitimate code or software.
- **Viruses** - a type of malware that attaches to another program (like a document), which can replicate and spread after a victim first runs it on their system.
- **Worms** - a type of malware whose primary function is to self-replicate and infect other computers while remaining active on infected systems.
- **Zero-Day Attack** - when security teams are unaware of their software vulnerability, and they've had "0" days to work on a security patch or an update to fix the issue.
- **Zombie** - a computer connected to a network that has been compromised by a hacker, a virus or a Trojan; and can be used remotely for malicious tasks.

11. Appendix 3 – Information Security Technologies (IST)

This section lists key definitions of these emerging IST:

- **Antivirus** – is a computer program used to prevent, detect, and remove malware. viruses and other kinds of malicious software from your computer or laptop. also known as anti-malware.
- **Bring Your Own Device (BYOD)** - is the set of policies in a business that allows employees to use their own devices – phone, laptop, tablet or whatever – to access business applications and data.
- **Cybersecurity -** focuses on protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible.
- **Digital identity** - a unique persistent identifier associated with a body of information about an individual, organization, device, algorithm, or avatar that exists online.
- **Encryption & keys** – a way to conceal information by altering it so that it appears to be random data. An encryption key is a random string of bits created explicitly for scrambling and unscrambling data.
- **Ethical hacking** – involves an authorized attempt to gain unauthorized access to a computer system, application, or data.
- **Firewalls** – a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.
- **Fraud detection** – software that protects customer and enterprise information, assets, accounts and transactions through analysis of activities by users and other defined entities.
- **Internet & network security** – overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection. protects your network and data from breaches, intrusions, and other threats.
- **Intrusion Detection System (IDS)** – is to ascertain attack or malicious activities in standalone system or in networked systems, by continuously monitoring the audit trail of traffic.
- **Multi-factor authentication (MFA)** – an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.
- **Passwords** – for completeness, a string of characters that allows access to a computer system or service.
- **Penetration testing (pen test)** – a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.
- **Predictive enforcement** - commonly known as predictive policing, involves using algorithms to analyze massive amounts of information in order to predict and help prevent potential future crimes. Related is proactive policing, usually defined as the predisposition of law enforcement to be actively involved in preventing and investigating crime.
- **User authentication** - verifies the identity of a user attempting to gain access to a network or computing resource Authentication can be classified into three groups: something you know - a password or personal identification number (PIN); something you have - a token, such as bank card; something we are - biometrics, such as fingerprints and voice recognition.
- **VPN** – an arrangement whereby a secure, apparently private network is achieved using encryption over a public network, typically the internet.

12. Appendix 4 – Law Enforcement (LawTech)

This section lists key definitions of Law Enforcement and Regulation:

- **Judicial algorithms** –algorithms that use statistical probabilities based on factors such as age, employment history, and prior criminal record to predict a defendant's likelihood of recidivism, and controversially recommend sentencing.
- **JudicialTech** - AI and emerging technology systems to support the courts and judicial system.
- **Jurisdictional arbitrage** - the practice of taking advantage of differences and discrepancies between competing legal jurisdictions.
- **JusticeTech** - the creation of technological tools that allow people with legal issues to navigate the legal system without a lawyer.
- **LegalTech** – AI and emerging technology systems to support Legal Services firms.
- **Offender profiling** - also known as criminal profiling, is an investigative strategy used by law enforcement agencies to identify likely suspects and has been used by investigators to link cases that may have been committed by the same perpetrator.
- **PoliceTech** – AI and emerging technology for automating policing.
    - *Proactive policing* involves using predictive analytics to analyze massive amounts of information in order to predict and help prevent potential future.
    - *Proactive enforcement* is usually defined as the predisposition of a police officer to be actively involved in preventing and investigating crime; predictive enforcement.
    - *Predictive policing* systems dedicated to apprehending and detaining people before they have the opportunity to commit a crime (cf. .
- **RegTech** – technology for automating compliance and regulation.
- **Regulatory compliance** – an organization's adherence to laws, regulations, guidelines and specifications relevant to its business processes.
- **Sandboxes** – provide a LawTech testing environment where new or untested technologies and software can be run securely.
- **Self-reporting** – to engage with AI and emerging technologies' communities to encourage self-regulation and self-reporting of emerging cybercrime trends.
- **Social norms** - the informal rules that govern behavior in groups, organizations, and societies.
- **SupTech** – the use of technologically enabled innovation by supervisory authorities. With regard to law enforcement:
    - *Delegation of enforcement* means police officers can apply penalties for minor crimes, opening the possibility of real-time justice.
    - *Recidivism algorithms* to assess a criminal defendant's likelihood of committing a crime.
    - *Algorithmic dispute resolution* uses AI to automate professional arbitration and dispute resolution.
- **Tech sprints** – essentially hackathons, coding events that bring LawTech programmers and other interested people drive innovations.
- **Virtual Courts** - are court hearings conducted by audio-visual means, where cases are progressed without the need for participants to attend the Court in person.