ORGANISED CRIME – THE CYBER DIMENSION

Dr Dionysios Demetis
Hull University Business School
Centre for Systems Studies
d.demetis@hull.ac.uk
ORCID: https://orcid.org/0000-0002-3411-0609

Abstract

This chapter reviews a few critical technological developments and reflects both on their trajectory as well as on the opportunities that they create for novel forms of cyber-enabled criminality. While the future of organised crime remains forever out of grasp, primarily due to the uncertainties created by the introduction of any new technology and the radical innovation that criminals exhibit, there are sensible aspects that we can consider and learn from. By taking examples from the dark web, blockchain technology and artificial intelligence, this chapter puts forward several new research directions that reflect on the intersection between technology and organised crime. These must prompt researchers to design new studies, new scholarly explorations, and consider the ways in which a deeper understanding of organised crime can emerge from how it adopts new technologies.

Keywords: cybercrime, cyber-enabled criminality, information systems, dark web, blockchain, artificial intelligence

Introduction

The fast pace of technological change makes it always challenging to delineate what we should be focusing on in terms of research. In this chapter, I will explore three major developments as examples of how we should be thinking critically about the cross-section between digitalisation and the future of organised crime. I shall explore these novel technological developments in brief and discuss how they pave the way for new forms of criminality. I will also reflect on what are some foundational research questions that can be proposed against this evolving backdrop. These three areas are: the *dark web,* developments in *mutual distributed ledgers* (a.k.a. *blockchain* technology) and *artificial intelligence.* I will also use these three areas as examples to put forth some more fundamental questions for a future research agenda.

First, it is important to recognise that the (digitalised) information landscape has changed radically through technology and that this has enabled new forms of organised crime[1]. Such organised crime is both exhibiting a continuity and a connection to previous criminality, but it also exhibits a discontinuity[2]: new forms of brokering (cyber-) criminal activity become possible as technology develops[3]. From the massive computers behind closed doors, we have now got wireless connections, tablets, smartphones, transactional websites, cryptocurrencies, and so on. An ecosystem of (digitally enabled) openness has allowed for the development of far more complex networks of networks that vandalize the information society[4]. Criminal networks are not only becoming technology-enabled[5]; technology allows for the launch of novel digitalised criminal networks. Also, new modes of operating criminally, given the complexity of technological innovations, allow criminals to find 'radical innovation pathways'. For instance, human traffickers have been found to implant their victims with unique Radio Frequency Identification microchips[6] (RFID), giving rise to the possibility of having a digital register of human slaves for trafficking, brokering human slavery digitally, as well as

[1] Dionysios Demetis, *Breaking bad online: A synthesis of the darker sides of social networking sites*, 38 EUROPEAN MANAGEMENT JOURNAL (2020)
[2] Ross Anderson et al., *Measuring the Cost of Cybercrime*, *in* THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY 265–300 (2013),
[3] Wingyan Chung et al., *Fighting cybercrime: a review and the Taiwan experience*, 41 DECISION SUPPORT SYSTEMS 669–682 (2006)
[4] Steven Furnell, *Cybercrime: Vandalizing the information society*, WEB ENGINEERING, PROCEEDINGS (2003)
[5] Hind Benbya et al., *Complexity and Information Systems Research in the emerging digital world*, 44 MIS QUARTERLY 1–17 (2020); Jannis Kallinikos, *The order of technology: Complexity and control in a connected world*, 15 INFORMATION & ORGANIZATION 185–202 (2005).
[6] Jeffrey Voas & Nir Kshetri, *Human Tagging*, 50 IEEE COMPUTER 78–85 (2017)

augmenting human trafficking with other technology-enabled exchanges, like crypto-assets[7] or digital contracts. Such developments open the door to cyber-auctions of human victims, with this potential being just one out of many futures of cyber-enabled criminal activity. In this example, the technology-enabled facilitation of human trafficking, changes the phenomenon itself; it also creates new pathways through which victims can be trafficked. Overall, it remains a stark reminder that whatever the technological innovation might be, criminals will tend to be the first adopters. But given the interoperability between different technologies, and the sheer variety of criminal activities, more fundamental questions arise: what technology-oriented permutations will lead to productive criminal innovations[8]? What are the features of different technologies that – given the right circumstances – can allow criminals to adopt them? What is the spectrum of digitally enabled criminality?

Indeed, technology allows criminals to onboard, exploit, and operationalise a large number of digitalised elements. Research so far has been concentrating mostly on the criminal phenomena and the use of technology in them but has not dug more deeply into the structural changes that technology brings forth. The combinatory possibilities allowed for by new technological innovations means that we need new ways to study these phenomena. This is an issue that raises theoretical, methodological, as well as practical concerns. Both scholars and law enforcement tend to play catch-up with new ways of conducting crime through technology, but working at a meta-level, we can develop frameworks, theories even, that can offer deeper insights into the cyber-enabled organising of criminal activities.

Dark web-based organised crime[9]: new platforms for criminals

One example where we can study some of the frontiers of how cyber-enabled criminality occurs is the dark web where latest research and insights can help us point to issues that require further research. At a moment in time where publicly available data on the internet has increased at an incredible pace (known as the *surface web*) and where proprietary databases of companies and institutions (known as the *deep web*) have deepened, cyber-enabled crime has found a relative refuge in the darkest corners of the dark web. While criminally-oriented forums

[7] Dionysios Demetis, *Breaking bad online: A synthesis of the darker sides of social networking sites*, 38 EUROPEAN MANAGEMENT JOURNAL (2020)
[8] Can we systematise the study of combinations of technological elements and scope out future criminality?
[9] I am grateful to agents from both the Federal Bureau of Investigation and the United States Secret Service for our discussions on the dark-web, which have helped me reflect on this section

go back a long way in the history of the internet[10], the architecture of the dark web that is accessible through (largely open-source) software such as TOR, offers a higher degree of protection as it ping-pongs network connections around the world and creates several layers between the information accessed and its recipient[11]. This has allowed several vibrant criminal communities to flourish and strengthen their networked ties.

Through the dark web, we see cybercriminals exchanging an incredible level of detailed data-elements between them, including full online identities[12] that include anything from first and last names, social security/national insurance numbers, dates of birth, car license plates, home addresses, e-mail addresses, usernames and passwords, even preferred contact hours (of potential victims). Full online identities are sold for a few dollars (usually between $3 to $5) and are used for conducting fraud, applying for loans, credit cards, etc. Hijacked bank-accounts and e-banking credentials are readily available. Cyber-criminals can be rented for a daily rate (a rent-a-cybercriminal service), allowing anyone to tap into underground skillsets. Money launderers can be hired and cyber-money laundering services that are automated (e.g. through shuffling/mixing cryptocurrencies) can be procured. Even assassins can be hired on the dark web. The dark web has become a playground for criminality offerings and a repository of personal data resulting from data breaches[13]. It covers a wide spectrum of activities and yet, because of that variation, we do not have a very clear idea of the sheer variety of activities conducted in it and the momentum of each one. While there are some services on the dark web that catalogue these activities (e.g. a dark-web wiki-style register), our understanding of the characteristics of each activity, its intensity, volume, side-effects, and position in the broader cyber-enabled criminality is frail. This raises a number of questions: 1) How does the dark-web allow cyber-enabled criminality to express itself, 2) With what intensity, volume, socio-economic, and other attributes, is each criminal activity expressed? 3) Given the volume of data, the complexity of its forums, etc., how can we study the dark-web to give us insights into the frontiers of cyber-enabled criminality? 4) Can we work on delineating behaviours, schemes, trends and observe what criminality spikes are emerging before law enforcement experiences

[10] See for example, SHADOWCREW as one of the precursors to the dark web
[11] Eric Nunes et al., *Darknet and deepnet mining for proactive cybersecurity threat intelligence*, *in* IEEE INTERNATIONAL CONFERENCE ON INTELLIGENCE AND SECURITY INFORMATICS: CYBERSECURITY AND BIG DATA, ISI 2016 (2016)
[12] Also known as Fullz
[13] HANNAH BARTON, THE DARK SIDE OF THE INTERNET (2016), Taylor and Francis

their impact[14]?, 5) Are there ways in which we can *de-silo* dark web forums and search across multiple fields of data and across such forums (e.g. usernames/Bitcoin wallets, searching within keywords against captured forums, etc)? 6) Can we capture the greater movements and activity-trends in the dark web and create meaningful 'information dashboards' for intelligence agencies and law enforcement[15]?

While the activity-oriented deconstruction(s) of the dark-web (e.g., focusing on a single phenomenon like cyber-money laundering) would open significant research insights about that activity, there is another fruitful pathway of research for the dark-web: *probing the self-organisation of cyber-criminals themselves*. Very little research has been done towards that end. How do cyber-criminals support one another in the dark web? What are the services that they offer *to each other* so that they can amplify the successful outcomes through their efforts? We do know from both previous research[16] as well as dark-web oriented studies that cybercriminals form tight groups and collaborate feverishly. For example, cybercriminals offer training courses for other aspiring cybercriminals[17]; they are pioneers in dark-web based e-learning and take the time to compile detailed learning materials that guide new cyber-criminals on how they should protect themselves against law enforcement when conducting crime. They share know-how in forums and can also tap into similar risk management techniques as those used by financial institutions when they are attempting to shield the clients for fraud. Only in the case of cyber-enabled crime, this occurs in reverse. For instance, in stolen credit card numbers that can be bought on the dark net, some novel services have surfaced where the 'customer' (i.e. the person seeking to use the stolen credit card) can opt to pay an extra amount for 'enhanced protection' (typically only a few extra US dollars). Through this service, the credit card number will be risk-scored for the probability of being rejected by popular anti-fraud solutions during use by the 'customer'. Let that sink in for a moment: cybercriminals offer risk management services to other aspiring cyber-criminals. Given such self-referential innovation, we can ask: how do cyber-criminals engage in risk-management practices? What are the ways in which they support each other and propagate trust in underground communities

[14] This would give LEAs more time to prepare and consider investigative options, law enforcement approaches, and financial institution actions
[15] A design science approach here would be most useful to delineate requirements
[16] Abeer ElBahrawy et al., *Collective dynamics of dark web marketplaces*, 10 SCI REP 18827 (2020)
[17] Dionysios Demetis, How the 'Original Internet Godfather' walked away from his cybercrime past – interview, The Conversation (2018), https://theconversation.com/how-the-original-internet-godfather-walked-away-from-his-cybercrime-past-interview-88822.

of interest? How do they engage in self-organisation[18] and what are the broader systemic properties of their criminal system? In what ways do they exploit standardised business-practices (like risk-management, risk-reward options, tools, processes, procedures) and appropriate them for their own means? A wide variety of research approaches could enable the exploration of such research questions and inform their research design (e.g., cyber-ethnographic research, case-based research designs, mixed methods and a variety of epistemological traditions).

Beyond the phenomena-driven dark-web based aspects and even beyond the self-organisation aspects that cyber-enabled criminality exhibits, there is another wider research agenda for the dark-web that we also need to be working towards. For example, it has been shown that online cyber-criminal communities from Silk Road to Alpha Bay, are either taken down by law-enforcement, or opt for a voluntary dissolution while new dark-web markets emerge[19]. There are also dark-web marketplaces that are designed to defraud other cybercriminals and see shorter lifespans of online activity and swifter exit-cycles. Despite serious pressure to take down online marketplaces from the dark-web, there are always current and reliable dark-web markets through which cyber-criminal activities are conducted. On balance, and over the past decade, the entire dark-web market ecosystem is demonstrating significant resilience despite a few considerable successes from Law Enforcement. Why? Where can we attribute the broader resilience of the dark-web market ecosystem and what novel approaches can we consider to disrupt it? At this higher-level of considering the dark web, researchers[17] have also noticed a mobility of users once a disruptive event occurs (like shutting down a marketplace). Dark web users of illegal marketplaces simply shift their activities to one of the various alternatives. While this demonstrates the grander and much higher-level movements of dark-web users once a market is disrupted, we can gain considerable insights by studying activities and discussions in a more granular level. What is the micro-level and macro-level activity on the dark web that

[18] Steve Alter, Work System Theory: Overview of Core Concepts, Extensions, and Challenges for the Future, 14 Journal of the Association for Information Systems 72–121 (2013); Kenneth E Boulding, General systems theory - the skeleton of science, 2 Management science 197–208 (1956); Dionysios Demetis, Technology and Anti-Money Laundering: a systems theory and risk-based approach (2010), http://www.elgaronline.com/view/9781848445567.xml; Heinz von Foerster, On self-organizing systems and their environments, in Observing Systems 1–23 (1981); Ludwig Von Bertalanffy, An outline of general system theory, 1 British Journal for the Philosophy of Science 134–165 (1950); Niklas Luhmann, System as difference, Organization (2006); Niklas Luhmann, Introduction to Systems Theory (2012); Niklas Luhmann, Social systems lii, 627 (1995).

[19] Abeer ElBahrawy et al., Collective dynamics of dark web marketplaces, 10 Sci Rep 18827 (2020).

contributes towards an escalation of cyber-enabled crime? How and where do cyber-criminals collaborate with ordinary criminals? What kind of pre-emptive interventions can we consider so that we may disrupt illegal activities or identify and suppress them before they materialise into more substantial cybercriminal actions?

Within a context like that, we need to recognise that the dark web is just one widespread instance. There are many other channels of communication that are used by both cyber-criminals and ordinary criminals. Smaller, encrypted channels and platforms like Telegram, Wicker, Jabber, etc., remain part of modern-day communication tools. While there is nothing intrinsically criminal in any of them (including the dark web[20]), the broader appropriation of digital tools by criminals, casts further research questions into the spotlight. In this context, one of the most significant questions to re-consider is this: what is the balance between privacy and security in a digitally framed world of communication and criminality? How much of our privacy are we willing to 'give up' for security and what are the contextual elements that influence the privacy/security spectrum? There are of course deeper surveillance-oriented questions here that push ethical concerns in the monitoring of criminality.

From the broader challenges considered in the context of the dark-web, I would like to move into reflecting on a series of research questions that can be posed in the context of Mutual Distributed Ledgers (a.k.a. Blockchain Technologies). This will allow us to bring to the surface a different set of questions, of a different kind.

Blockchain-based distributed crime

Admittedly, a body of scholarly work has already emerged and is starting to deal with various facets of blockchain-based applications[21]. For example, in the context of cryptocurrencies, it has already been pointed out that cybercriminal groups benefit from the relative anonymity that cryptocurrencies offer. While some strides have been made in tracing the chain of transactions through blockchain-analysis techniques in some cryptocurrencies (e.g. Bitcoin) and reflecting on the potential to use blockchain for financial crime investigations[22], more privacy-friendly

[20] For instance, the utility of the dark web for supporting access to news around the world where nation states become oppressive and restrict access to information has led the BBC (and other news organisations) to set up mirror websites in the dark web

[21] Yuanfeng Cai & Dan Zhu, Fraud detections for online businesses: a perspective from blockchain technology, 2 Financial Innovation (2016).

[22] Lamprini Zarpala & Fran Casino, A blockchain-based forensic model for financial crime investigation: the embezzlement scenario, 3 Digit Finance 301–332 (2021)

cryptocurrencies are becoming an instrument of choice. At the same time, cyber-tools that facilitate cyber-money laundering and digitalise the traditional 3-stages of money laundering (placement, layering, integration), become more and more sophisticated. For example, tools like mixers and tumblers rely on a repository of stored cryptocurrencies through which a shuffling process is executed, and the cyber-laundered cryptocurrencies are forwarded to novel addresses[23]. Options like cold storage of maintaining cryptocurrencies offline (or off chain in common parlour) and blockchain-based developments like smart contracts can amplify the potential criminal pathways.

A key general question that needs to be recognised here and that could create a stream of research could be articulated as follows: How can blockchain technology (e.g. through cryptocurrencies, smart contracts, and other distributed forms of digitalized organising) enable criminals[24]? How can law enforcement use blockchain technology to better detect, prevent, and pursue organised crime? The latter question involves further questions of organising for Law Enforcement Agencies (LEAs), for example: how can cross-border collaboration in pursuing organised crime be enabled through blockchain technologies?

I will indicate some options for the importance of tackling the first part of the question on how blockchain can enable organised crime and argue that we need to place a significant effort in understanding novel cyber-organised strands of crime. This is because the broader developmental trajectory of mutual distributed ledgers (MDLs) – a.k.a. blockchain technology – changes the very fabric of information organisation and reconfigures the dynamics of (online) trust[25]. While there is nothing intrinsically criminal in blockchain, a key set of developments could turn out being every (cyber)criminal's dream come true and launch novel digitalised organised crime options.

---

[23] Rolf van Wegberg, Jan-Jaap Oerlemans & Oskar van Deventer, Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin, Journal of Financial Crime (2018); Satoshi Nakamoto, Bitcoin: a Peer-to-Peer Electronic Cash System, (2009).

[24] The theory of affordances could help organise some of these aspects in *enabling, constraining* or other categories like *misperceived*:
Olga Volkoff & Diane M. Strong, Critical realism and affordances: Theorizing IT-associated organizational change processes, 37 MIS Quarterly: Management Information Systems (2013); James J. Gibson, Gibson, James J. "The Theory of Affordances" The Ecological Approach to Visual Perception. Boston: Houghton Mifflin, 1979. Print., The Ecological Approach to Visual Perception (1979); Paul Leonardi, A comparative study of feature use and shared affordances, 37 MIS Quarterly 749–755 (2013).

[25] Michael Mainelli & Mike Smith, Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology), 3 Journal of Financial Perspectives 38–58.

Understanding the radical shift in information organising can help us interpret this important change, launch novel research questions about organised crime and digitalisation, and adjust our research agendas for the future.

Blockchain essentially demarcates a key shift in organising information. We are moving away from both the centralised model and away from the cluster-based networking model wherein we can place conceptually the structure of traditional organised crime (i.e. as *clusters* of different organised crime groups that either compete or collaborate). Blockchain offers a way of organising entities in a *distributed manner* where everyone can be connected to everyone else in a particular network. The development of cryptocurrencies and smart contracts are just two expressions of a much deeper informational shift.

In fact, what MDLs have started signalling to the criminal world is that there needs to be a stronger cooperation between cybercriminals and criminals. From this point of view, the very transition from centralised forms of networking, to decentralised and then to distributed, sees parallels in the coexistence of criminality from lone wolf attacks, to organised crime groups to what I would label as *fluid hyperconnected criminality.* Fluid in the sense that organised crime will become far more dispersed and dynamic through digital technologies so the more 'static and stable' organised crime groups will give way to novel formations. Hyperconnected in the sense that these groups will come together to conduct a crime, profit from it, disperse, and re-link in different ways, to execute another crime, and so on. Each reconfiguration will link different criminal nodes in the distributed network based on the 'specialisations' required. Such hyperconnected criminality becomes both more dangerous and more pervasive. Blockchain technology has the features needed to power at least some of its organising needs. What will be the defining trends of such a digitalized transition for organised crime?

Such a cyber-enabled, pulsating, dynamic and novel criminal network will be like an electricity grid for crime. Anyone will be able to 'plug in' or 'tap in' and receive a (cyber or traditional) criminal service. Digitalized distributed criminal services will be scored by those procuring them; these will become the user-friendly (cyber)criminal services of the future: think of a Tripadvisor and Uber-like kind of service for criminality where criminal activities can be bought, delivered, and evaluated seamlessly between masked identities. A dashboard can update those procuring criminal services. Notifications like: 'Your criminal is on his way', 'Your criminal has successfully stolen the target's data and assassinated the target', 'Review

(encrypted) stolen sample, proof of crime, and pay in digital tokens', 'Score the criminal service you have received' will modernize the digitalization of cyber-enabled contemporary criminality. Digitally enabled crime-auctions can allow different criminals to bid for getting hired for a specific crime. How will these new e-Bay-like services for crime function? Unlike the dark-web that is predominantly cyber-crime oriented, the potential for a truly blockchain-based distributed crime evolution can unify all criminality.

This potential for a radical displacement from organised crime to distributed crime is akin to developing a *cyber-enabled crime-grid* that would allow anyone to tap into it and procure all kinds of (cyber)criminal services. Cyber-crime as a service (CCaaS) and Crime as a Service (CaaS) are already becoming an established reality that need to be dealt with. But a cyber-enabled crime-grid will also require novel cyber-money laundering approaches, for which little research has been done[26]. While we know that cyber-mixers and shufflers rely on a repository of bitcoins (or other cryptocurrencies) and reconfigure the classic placement-layering-integration triad by shuffling digital value, we do not have a vibrant research community that concentrates around cyber-money laundering alone[27]. Even basic and persistent problems like advanced and dynamic cross-border information sharing between banks, LEAs, investigators and prosecutors remain under-researched. Also, cyber-money laundering is inextricably bound to digital identity, digital value, new technological innovations and will ultimately adapt to new digital frontiers (e.g. defrauding avatars in the metaverse and stealing their digital assets).

These developments raise several questions: What novel modes of organising will support criminals as they reorganise themselves via the use of blockchain technology? How will a cyber-enabled global crime-grid look like and what will be the foundations that sustain it? At what significant 'anchor-points' can blockchain power this new crime-grid? What is the variety of cyber-money laundering techniques available and how will these evolve or augment traditional ML approaches? As scholars, we need to tap into a wide variety of experts and specialisations to get a handle on these developments. More importantly, we need to build on research approaches that cut across strict disciplinary silos (e.g. systems theory/systems thinking).

---

[26] R Stokes, *Virtual money laundering: the case of Bitcoin and the Linden dollar*, 21 INFORMATION AND COMMUNICATIONS TECHNOLOGY LAW 221–236 (2012)

[27] Even though cyber-money laundering was identified early on as a theme: He Ping, *New Trends in Money Laundering - From the Real World to Cyberspace*, 8 JOURNAL OF MONEY LAUNDERING CONTROL 48–55 (2004

Another important trail of research at the intersection between blockchain and criminality would need to focus around *trust.* One of the biggest problems that criminals are faced with, particularly those engaged in organised crime is the level of trust (or mistrust) between them and splitting loot fairly. The many variants of both *trust* and *communicative structures* between criminals have been well documented[28]. As gangster Jackson said: "I have no way of checking your (implied criminal) credit rating or anything else, so I judge you by whom you associate with." In addition, the distribution of trust in criminal enterprises is *deeper,* with participants being both trustors and trustees**.** In that context, the top problems that criminals face (and are looking for answers to) are: trusting each other, communicating safely, minimising opportunist behaviour, establishing alibi, making loot jointly available and splitting it fairly, and then laundering the proceeds of crime (either via traditional money laundering techniques and/or cyber-money laundering). Trust problems hold back large-scale expansions of organised crime. Blockchain can unlock their potential. How is (online) trust brokered at the intersection between cyber-criminals and criminals? How will the adoption of MDLs (a.k.a. blockchain) enable new trust-mechanisms between criminals and how will that construct new forms of criminal activity?

Enter all the different types of blockchain-based "solutions" that will surface to assist criminality. The stage where ransomware cyber-attacks are cashed out in bitcoins, is Phase 1. Gone are the days where years of robberies, murders, loan sharking, etc., would be required to become the 'confidant' of the Godfather. Such criminal activities will be supported by a variety of anonymity-oriented distributed criminal ledgers where each criminal is associated with a secure crypto-record. Smart "criminal contracts" will be executed online and when proof of fraud, murder, rape, kidnap, etc., is securely transmitted, it will unlock a fixed amount of trust tokens (e.g. in cryptocurrencies or in other proprietary digital assets). More complex crimes can be 'crime/crowd-sourced' from within the distributed criminal network. Proprietary digital assets can be rewarded to its participants.

A cyber-organised criminal activity can be enabled by the many available cryptocurrencies and these will compete in the marketplace of online trust and criminal safety. Alternatively, new, criminally-designed cryptocurrencies, can become new vehicles of criminal exploration. The closest that an underground market has come to this is online child exploitation[29]. A case in

[28] DIEGO GAMBETTA, CODES OF THE UNDERWORLD: HOW CRIMINALS COMMUNICATE, PRINCETON UNIVERSITY PRESS (2011)

[29] Dionysios Demetis & Jan Kietzmann, *Online Child Sexual Exploitation: A New MIS Challenge*, 22 JAIS 5–40 (2021).

point here is Richard Huckle, who, in 2016, was given 22 life sentences for 71 counts of serious sexual assaults against children. Huckle set up a dark-net forum called "The Love Zone" where he had 'gamified' child sexual exploitation online. He awarded himself and others 'pedopoints' (a digital token) with abused children being the value tokens. He maintained a ledger/scorecard for recording the crimes and registering point-rewards[30]. Huckle had effectively created a cyber-enabled organised crime out of online child sexual exploitation, with an added dimension of gamification.

While the internet has allowed paedophiles to find each other and the dark web has allowed them to communicate and exchange photos at a (relatively) safer place, a privacy-friendly blockchain-powered system of trust would be a novel challenge.

Similar to legitimate uses of blockchain, criminal uses will experience a variety of similar 'innovations'. A few blockchain-based use cases for criminality could be: a) verifying the quality and purity of illegal substances by combining both digital and physical anti-tampering mechanisms, creating a combined digital and physical leap in drug trafficking, b) assisting criminals in human trafficking by tagging humans with RFID microchips (i.e. we have a blend of digital and physical human slavery that can construct a secure and effective slave-index and transfer can be maintained between human traffickers, facilitating slave cyber-auctions and distributing the loot online), c) terrorist financing where there is already evidence that terrorist websites are accepting donations in Bitcoins but they could evolve to facilitate their broader blockchain-based organisation, etc. These are all examples that require further exploration. What are the domain-specific (e.g. in terrorist financing) blockchain-oriented criminal innovations that can occur? To address these issues and their implications, we need a vibrant research community at the cross-section of cybercrime, information systems, anti-money laundering, and information security that will explore MDLs in their proper context and unlock the potential that it can carry for criminality. This will help us realise the ways in which blockchain can have an impact in the cyber-dimensions of organised crime and also probe the following question with more precision: how can law enforcement re-organise globally, share information and intelligence and create new ways of countering crime through blockchain technology?

[30] It was an accidental discovery and then a tip-off that led the Australian Police to alert the National Crime Agency to a full investigation before Huckle was arrested at Heathrow. Before Police managed to get to Huckle, an estimated 200 children were abused.

Artificial Intelligence and the future of crime

While digital developments like those explored above can reshape criminality itself, there are other equally exciting developments that can underscore even more challenging changes for the future of crime. Artificial Intelligence (AI) certainly has such a potential, even when true AI[31] is still very much work in progress. While we do need to recognise that there is significant hype surrounding developments in AI, there are already interesting implementations and appropriations of AI-applications by criminals. For example, in a rather unusual cybercrime and financial fraud case, criminals synthesized the voice of a CEO of a UK energy company[32]. The criminal(s) created an AI-based synthetic voice that replicated the voice of the CEO with a high-degree of accuracy (also known as a deep fake). To train the AI system, they used real samples that were harvested from public interviews that the person had given in the past. Then they used the synthetic voice to conduct a conversation with the CFO of the company who authorised a payment of about £250,000. A complex mix of social engineering techniques, information on company processes and the AI approach to a synthetic voice was the winning approach for criminals. But as interesting as this case is, it only scratches the surface on the real potential for the AI-oriented enablement of criminality.

The first aspect to consider here is that AI is really an umbrella term for several computational innovations[33]. Their broader categories involve *machine learning* (which has different forms of its own like deep learning, supervised and unsupervised learning), *natural language processing* (that can enable classifications, question answering, text generation, content extraction, etc), *computer vision* (where image recognition and machine vision recognise objects in the world), *speech* (with text-to-speech and speech-to-text) and other branches that include robotics and so on.

[31] By 'true AI', I refer here to the possibility for the emergence of "Strong AI", a non-biological but sentient/self-conscious being that is autonomous and exhibits self-organisation, while it relies on variable forms of spontaneously constructed automated decision making. This raises the question though if the nature of intelligence itself and how that can be considered:
Ian Angell, *Intelligence: logical or biological*, 36 COMMUNICATIONS OF THE ACM 15–16 & 119 (1993)

[32] Catherine Stupp, *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*, THE WALL STREET JOURNAL, 2019

[33] RAJENDRA AKERKAR, ARTIFICIAL INTELLIGENCE FOR BUSINESS, SPRINGER (1st. edition ed. 2018)

Even though some fledgling aspects on AI-oriented criminality are starting to receive some attention like in the context of deep fakes[34], there is indeed a pressing need to understand how the technological innovations across the multiple branches of AI can reshape the future of organised crime and the different modes in which new interconnections and networks can emerge. This requires a research programme at the cross-section between AI, financial crime and information systems alongside cyber-enabled crime and management. As a scholarly community that is interested in this space, we cannot afford to carry on treating AI as a semantic umbrella without exploring its consequences for various forms of cyber-enabled organised crime. We do need to tackle the implications of AI with a more incisive approach and that means exploring the consequences of each AI-branch by asking its corresponding foundational questions. For example, and in reference to the case used at the start of this section on the CEO's speech replication, we could ask: how will the AI-oriented ability to synthesize human speech be useful to criminals in conducting fraud, impersonation, and a wide variety of crimes? What are the enabling/constraining factors of that particular AI-innovation and of tackling it? Similarly, if one considers the development of deep-learning, one could ask: how can advances in deep learning lead to an increase in organised crime, and similarly, how can they be appropriated by law enforcement or private institutions to detect criminal activity? Taking an incremental approach in tackling the implications of AI in organised crime is important as the interconnections are likely to be as complex as their domains of application. Then we can start to take more synthetic research questions and try to study them in a context.

Naturally, on each 'instance' of an AI-application, we have the development of further innovations that operationalise both structured and unstructured data for training the AI-systems. For instance, in the context of deep learning, we have practical applications like the creation of *virtual assistants, face recognition, money laundering detection approaches, etc.* Each of these has the potential to be adapted by both criminals and law enforcement. This allows us to take a separate line of exploration here as an example of possible scenario-planning; this in turn can lead to further research agendas and questions. Let us conduct a thought experiment and hypothesize the development of an *automated money laundering AI-agent that different organised crime groups can use.* This could be an AI-agent that could partner with criminals and facilitate automated money laundering (it would find its own optimal

[34] Jan Kietzmann et al., *Deepfakes: Trick or treat?*, 63 BUSINESS HORIZONS 135–146 (2020)

route for laundering money and calculate the less risky pathway – for the criminals – to conduct the money laundering operation with the smallest chance of detection). How would it work?

The criminal of the future should be able to give a simple text instruction to an AI system like: "Create 25 synthetic human identities, construct photorealistic identity documentation in passport form for each one, negotiate bribes of up to £y if there are friction points, open bank accounts online or buy bank accounts from the dark web, and engage in the automated cyber-money laundering of the £4m deposited in account X by rendering the complexity of the layering stage to z-degrees of depth". Then they could let AI take over and support the money laundering operation. There is no doubt that already existing developments (for example in the context of semi-autonomous algorithmic trading) are readily facilitating the automated execution of mammoth amounts of money annually and are already setting the stage where millisecond-transacting from automated systems is the norm[35]. Thus, conducting an automated set of transactions is not the problem. But an AI-empowered money laundering operation would go further. Relying on deep fakes, constructing synthetic identities, and conversing in a form that would be indistinguishable from humans[36], it would take us closer to *unsupervised and autonomous/digitalised money laundering.* Organised crime could and would bestow more and more complex decision making into the 'hands' of algorithms. This would increase the demand for the necessary autonomy needed for AI to act as a digital money launderer broker.

As synthetic identities and synthetic humans are already practically indistinguishable from 'real' humans, AI-enabled identity construction could throw all online Know Your Customer (KYC) processes into chaos[37]. Future AI-synthetic humans could converse freely with the customer support agents of digital banks during video onboarding and answer all the necessary background questions required (though chances are that AI itself will be conducting such interviews in an AI vs AI scenario). Digitalised organised crime groups will compete based on who has more effective AI 'solutions'. AI itself can be deployed to look out for new

[35] Alain Chaboud et al., *Rise of the Machines: Algorithmic Trading in the Foreign Exchange Market*, 980 INTERNATIONAL FINANCE DISCUSSION PAPERS 1–44 (2009); P Treleaven, M Galas & V Lalchand, *Algorithmic trading review*, 56 COMMUNICATIONS OF THE ACM 76–85 (2013); Simson Garfinkel et al., *Toward algorithmic transparency and accountability*, 60 COMMUNICATIONS OF THE ACM (2017).

[36] See for example developments in Conversational AI

[37] In an upcoming era of synthetic humans and digital identities that can be indistinguishable from 'real' humans, could physical bank branches or specialised authentication centres be making a comeback? How we will be authenticating humans in a future where AI can create synthetic human identities that are indistinguishable from reality and where both video/audio deep fakes can be convincingly representing and engaging in human-to-human interaction?

opportunities for conducting criminal activities and make recommendations. It could seek out real-world vulnerabilities, consider local law enforcement challenges and inefficiencies (after all, freely available annual performance reports and statistics can inform such algorithmic decisions), and suggest new targets for the various crimes that organised crime groups are interested in. How can AI seek out new opportunities for organised (or distributed) crime groups?

Overall, the possibilities opened up by AI are a step change in re-inventing organised crime groups though technological failures and unintended consequences of AI need to be factored into these dynamics too[38]. At present, the balance between human agency and computer agency might be in favour of humans, albeit with some cyber-enabled actions. In the future, the balance will shift[39] towards automated, AI-enabled, organised crime. Taking this to its extreme, we could even see autonomous AI-organised crime groups emerging without any human involvement at all. This would pit AI vs AI further[40]. This begs the question: what forms of fully-autonomous cyber-enabled organised crime can we expect? How can organisations start preparing for them? We are already starting to see some traction in the latter. For example, in information systems management, we have studies preparing organisations for adopting management practices and frameworks in order to deter, detect, and respond to deep fakes that may target either single employees or the company as a whole, and incur a number of reputational and financial risks[41]. What information systems and management practices will need to be adopted to counter AI-enabled attacks and exploitation?

Meta-questions about digitally-enabled crime & conclusions

The three domains I have explored above are only sample domains to highlight the different developments that could take place and the kinds of questions that we should be asking. However, it is equally important to point out that no technology exists in isolation. The way in which technology interferes with the social reality around us is complex[42] and creates the

[38] For example, when Microsoft released its AI chatbot on Twitter, it turned into an automated Nazi in the space of 24 hours and a misinformation engine – after all, it was learning from those

[39] Dionysios Demetis & Allen Lee, *When Humans Using the IT Artifact Becomes IT Using the Human Artifact*, 19 JOURNAL OF THE ASSOCIATION FOR INFORMATION SYSTEMS 929–952 (2018)

[40] In a limited manner, this is already taking place where AI-deployments within companies are trying to detect sophisticated cyber-attacks or deep fakes.

[41] Jan Kietzmann et al., *Deepfakes: Trick or treat?*, 63 BUSINESS HORIZONS 135–146 (2020)

[42] DON IHDE, TECHNOLOGY AND THE LIFEWORLD: FROM GARDEN TO EARTH, A MIDLAND BOOK (1990)

equivalent of a digital cocoon[43], a cyber-blanket that is starting to cover more and more territory; technology shapes the fundamental ways in which social interactions are expressed and creates both new opportunities for organised crime and *new forms* of organised crime (e.g. distributed crime, or (cyber)-crime as a service). The fact that no technology exists in a silo and technical interoperability allows for combinations, means that there are synthetic opportunities from the different ways in which technologies can be combined. This creates an important question: how can we systematize and explore the potential developments of organised crime based on combined technological elements? That is a hard question as even standalone technological artifacts can be exploited by organised crime appropriately. For example, even before the infamous 'wall' that former President Donald Trump set out to fund and build in the Mexican border to "stop drugs flowing", drug traffickers used drones to fly cocaine over the wall[44] (one was discovered accidentally after it crashed as it was rather 'overloaded' with drug parcels). Such technology-inspired human innovations from organised crime are easier to predict but when multiple technologies are used to accomplish a goal then human ingenuity is harder to pin down for predictive planning and other purposes. Worse, when the logic behind criminal activity or actions is embedded into algorithms (like in the case of cyber-money laundering) it can be masked and it becomes harder to detect given the sheer volume of data exchanged.

Thus, at a meta-level, we need to ask a more foundational question: what are the basic pillars of digitalisation and how can these alter the course of organised crime? What are the key constructs, functions, and foundations of technology and how do these support organised crime? In the section above, through the examples of the dark web, blockchain, and AI, we saw how technology constructs new modes of underground electronic marketplaces (e.g. dark-web marketplaces), how blockchain technology changes the very nature of information organisation and can restructure digitalised and distributed value (like in the case of cryptocurrencies), and how AI can shift the balance between human/algorithmic agency while creating radical innovations. A research programme that would focus on exploring these research questions would take a sociotechnical perspective on organised crime and attempt to deconstruct the development of organised criminal activities based on a handful of premises. These would be the primary functions of how digitalisation reconstructs organised crime. Automation is one

[43] Jannis Kallinikos, *The order of technology: Complexity and control in a connected world*, 15 INFORMATION AND ORGANIZATION 185–202 (2005)
[44] Nick Valencia & Michael Martinez, *Drone carrying drugs crashes south of U.S. border*, CNN, 2015

such trait. Algorithmic execution and algorithmic decision making is another. Speed and communication is a third. Digital identity would be another central pillar. What are the key technological foundations of the future of organised crime?

If we hypothesize enough technological advances (e.g. like an advanced form of AI), then we can conceive of the trajectory of other novel forms of criminality (like *automated cyber-criminality* where AI-agents would be attacking businesses autonomously, collecting Bitcoins and cyber-laundering these through mixers before depositing them into the digital wallets of their masters). Such an approach is a prerequisite in making some advances and in understanding part of the future that is – to some degree – already being designed.

Naturally, criminality is not devoid of social, economic, technical, and political developments and conditions. While I have concentrated on some of the technological aspects in this chapter, it is equally important to recognise that technology carves out new realities *across* domains. Technology affects political, legal, economic and social developments variably. Consequently, each unique configuration of these domains within a nation state or between different countries will continue to remain a fertile ground for organised crime and/or broader criminal exploration. Academic disciplines in between technology-law (also known as technolegal studies), technology-economics, technology-society continue to develop. As an example, each cyber-enabled crime either emerges from a unique configuration of socio-economic, socio-technical and political developments, or exploits specific conditions. Any given significant event (e.g. the covid pandemic) can become a significant factor that spawns waves of cyber-enabled criminality, fraud, and exploitation. Whether it is recessions, inequality, pandemics, transitions into new ways of organising, new norms or standards or laws, each change will bring about additional opportunities for criminals and challenges for law enforcement. These will have their own technological interferences.

Our research community needs to engage with this complexity to better understand the complexity facing us. We need to find meaningful ways to probe, deconstruct, and interpret this complexity so that we can help our Law Enforcement agencies dent the explosive waves of cyber-enabled criminality that are on the horizon. It is both a scholarly and societal responsibility to think through such implications and test novel research designs, exploratory research ideas and push the frontiers of how we engage with research at a sociotechnical level.