

The Impact of Organized Crime in the Digital Age on American and British Societies

Matěj Mlýnek

Bachelor's Thesis
2025



Tomas Bata University in Zlín
Faculty of Humanities

Univerzita Tomáše Bati ve Zlíně

Fakulta humanitních studií

Ústav moderních jazyků a literatur

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Matěj Mlýnek
Osobní číslo:	H22563
Studijní program:	B0231P090005 Anglický jazyk pro manažerskou praxi
Forma studia:	Prezenční
Téma práce:	Dopady organizovaného zločinu v digitální době na americkou a britskou společnost

Zásady pro vypracování

Shromáždění odborných materiálů k tématu práce
Studium odborné literatury
Analýza současného stavu
Porovnání Spojených států amerických a Spojeného království
Vyvození a formulace závěru práce

Forma zpracování bakalářské práce: **tištěná/elektronická**
Jazyk zpracování: **Angličtina**

Seznam doporučené literatury:

Albanese, Jay S. 2015. *Organized Crime in Our Times*. 6th ed. Oxon: Routledge.
Bartlett, Jamie. 2014. *The Dark Net: Inside the Digital Underworld*. Brooklyn: Melville House
Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. 2022. *Cybercrime and Digital Forensics: An Introduction*. 3rd ed. Oxon: Routledge.
Marsh, Ian, and Gaynor Melville. 2019. *Crime, Justice and the Media*. 3rd ed. New York: Routledge.
Shelley, Louise. 2018. *Dark Commerce: How a New Illicit Economy Is Threatening Our Future*. Princeton, NJ: Princeton University Press.

Vedoucí bakalářské práce: **Ing. Martin Horák, Ph.D.**
Ústav regionálního rozvoje, veřejné správy a práva

Datum zadání bakalářské práce: **2. ledna 2025**
Termín odevzdání bakalářské práce: **6. května 2025**

L.S.

Mgr. Libor Marek, Ph.D.
děkan

doc. Mgr. Roman Trušník, Ph.D.
ředitel ústavu

Ve Zlíně dne 24. února 2025

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Tato bakalářská práce se zabývá proměnou organizovaného zločinu v souvislosti s nástupem digitalizace a rychlým vývojem technologií a analyzuje jejich vliv na společnost a bezpečnostní sféru. V teoretické části je rozebrán historický kontext tradičních mafiánských organizací a popsána jejich adaptace na digitální prostředí, včetně forem kriminality, jako jsou kybernetické útoky, ransomwarové vydírání, využívání kryptoměn či působení na dark webu. Praktická část práce provádí komparativní analýzu Spojených států amerických a Velké Británie z hlediska jejich strategií v boji proti digitálnímu organizovanému zločinu, přičemž reflektuje legislativní opatření, preventivní mechanismy a technologické nástroje pro detekci a prevenci hrozeb. Důraz je kladen rovněž na etické a bezpečnostní otázky spojené s rostoucím zapojením umělé inteligence v rámci páchání i potírání trestné činnosti.

Klíčová slova: organizovaný zločin, kyberkriminalita, hacking, darknet, bezpečnost, legislativa, Spojené státy, Spojené království

ABSTRACT

This bachelor thesis deals with the transformation of organized crime in the context of the advent of digitalisation and the rapid development of technology and analyses its impact on society and the security sphere. The theoretical part discusses the historical context of traditional mafia organisations and describes their adaptation to the digital environment, including forms of criminality such as cyber-attacks, ransomware extortion, the use of cryptocurrencies and operating on the dark web. The practical part of the thesis conducts a comparative analysis of the United States and the United Kingdom in terms of their strategies to combat digital organised crime, reflecting on legislative measures, prevention mechanisms and technological tools for threat detection and prevention. Emphasis is also placed on the ethical and security issues associated with the increasing involvement of artificial intelligence in both the perpetration and the suppression of crime.

Keywords: organized crime, cybercrime, hacking, dark web, security, legislation, United States, United Kingdom

Touto cestou bych rád poděkoval všem, kteří mě podporovali během psaní této práce i během mého studia. Děkuji svému vedoucímu práce, panu doktoru Horákovi za cenné rady a vedení, rodině za trpělivost a podporu a přátelům za to, že mi připomínali, proč má smysl jít dál.

„Ne to, co se ti děje, ale jak to přijímáš, určuje tvůj osud.“ – tato slova Marka Aurelia mi byla připomínkou, že překážky jsou jen zkouškou cesty, nikoli jejím koncem. Skrze úsilí a překonávání nesnází člověk roste, a proto věřím, že i tato práce je jen dalším krokem na cestě ke hvězdám – Per aspera ad astra.

CONTENTS

INTRODUCTION	11
I THEORETICAL PART	12
1 THE BEGINNINGS OF ORGANIZED CRIME.....	13
1.1 HISTORICAL ROOTS OF THE MAFIA.....	13
1.2 EVOLUTION OF TRADITIONAL MAFIA STRUCTURES.....	14
1.3 THE SHIFT TO MODERN FORMS OF CRIME	16
2 DIGITALISATION OF ORGANISED CRIME	18
2.1 THE IMPACT OF THE INTERNET AND TECHNOLOGY	19
2.2 THE SHIFT FROM PHYSICAL TO DIGITAL CRIME.....	21
2.2.1 Crime as a Service: a new business model	22
2.3 THE GROWING INFLUENCE OF ARTIFICIAL INTELLIGENCE.....	23
2.3.1 The future of AI and its impact on the security environment	24
2.4 THE DARK WEB AS A SPACE FOR ILLEGAL ACTIVITIES	25
2.5 CRYPTOCURRENCIES AND FINANCIAL TRANSACTIONS IN THE UNDERWORLD	27
3 IMPACT OF ORGANISED CRIME ON SOCIETIES AND THEIR SECURITY.....	30
3.1 CYBERSECURITY THREATS.....	30
3.2 THE MISUSE OF AI BY ORGANISED CRIME	31
3.3 MISUSE OF AI BY THE PUBLIC AND INDIVIDUALS.....	32
3.4 IMPACT ON BUSINESSES AND THE ECONOMY	33
3.5 SOCIAL STRUCTURES AND CRIME	33
3.6 PREDICTIVE ANALYTICS AND CRIME PREVENTION	34
4 LEGAL AND TECHNOLOGICAL RESPONSES TO ORGANISED CRIME	36
4.1 LEGAL FRAMEWORK AND INTERNATIONAL COOPERATION	36
4.2 COMBATING AND PREVENTING CYBERCRIME	37
4.3 ETHICAL AND SOCIAL CHALLENGES OF AI IN CRIME	37
4.4 AI AS A TOOL IN THE DEFENCE AGAINST DIGITAL CRIME.....	38
II PRACTICAL PART	40
5 THE HISTORICAL DEVELOPMENT AND SHIFT TO DIGITAL FORMS OF CRIME IN THE U.S. AND THE UK.....	41
5.1 THE ECONOMIC IMPACT OF DIGITAL CRIME	41
5.2 THE IMPACT OF DIGITAL CRIME ON THE PUBLIC AND EVERYDAY LIFE	43
6 CURRENT CHALLENGES AND CONSEQUENCES OF DIGITAL CRIME FOR SOCIETY AND SECURITY IN THE US AND THE UK.....	45

6.1.1	Overview of the most significant attacks and their impact	46
6.2	THE US AND UK APPROACH TO DIGITAL CHANGES	49
6.3	POLITICAL AND SECURITY CONSEQUENCES.....	53
6.4	THE DARK WEB AND ANONYMOUS FINANCE, IMPACTS ON SOCIETY.....	55
6.4.1	Case studies (Silk Road in the US vs. UK cryptocurrency scams)	56
6.5	LEGAL AND ETHICAL IMPLICATIONS OF THE FIGHT AGAINST DIGITAL CRIME	58
6.5.1	Future developments and predictions	60
7	SUMMARY OF THE COMPARATIVE ANALYSIS OF THE UNITED STATES AND THE UNITED KINGDOM.....	63
	CONCLUSION	66
	BIBLIOGRAPHY	67
	LIST OF FIGURES	71
	LIST OF TABLES	72
	LIST OF ABBREVIATIONS	73
	APPENDICES.....	74

INTRODUCTION

Organised crime, which in the past focused mainly on physical control and trafficking in drugs, weapons or illegal human trafficking, is now experiencing revolutionary changes. With the advent of the digital era and the development of technology, particularly the internet, many traditional criminal practices have moved into the virtual world. This development has led not only to new ways of committing crime, but also to unexpected impacts on social structures and security. Organised crime today is increasingly focusing on cybercrime, including hacking, online fraud, extortion and the abuse of internet platforms such as the dark web.

The aim of this thesis is to analyse how digitalisation and the advent of artificial intelligence have affected organised crime in Anglo-Saxon countries, specifically the United States and the United Kingdom. The focus will be on the specific effects that this crime has had on the social structures of these countries, on the security and legal aspects, and on the possibilities of prevention and response by state institutions. This analysis will also look at the role of artificial intelligence and its potential impact on organised crime in the future. The thesis will provide examples of how organized crime and cybercrime affect not only individuals, but also companies and entire communities, contributing to long-term changes in the security environment.

The practical part will focus on a comparison between the two selected countries, United States and the United Kingdom and an analysis of their approaches to fighting these new forms of crime. It will focus on how the different legislative and security systems in these countries are coping with the challenges posed by the digital age.

I THEORETICAL PART

1 THE BEGINNINGS OF ORGANIZED CRIME

Organized crime has a long and interesting history that dates to ancient civilizations, but in the context of the modern mafia it is of interest to trace its origins and development in diverse cultural settings. In Japan, the origins of the mafia can be traced back to the Edo period (1603-1868), when organisations began to form within the local society, which gradually became the basis for what we now call the yakuza. Known for their tightly structured hierarchies and specific codes, yakuza initially originated as groups of merchants and businessmen who conducted various illegal activities on the fringes of the law, mainly in the form of money lending and protecting business interests.¹

This initial form was distinctly different from traditional notions of the mafia, which is often associated with violence and illegal trade. Many members of the yakuza were originally merchants who used their business skills and contacts to create illicit networks, often being seen as protectors and guarantors of trade. This character gradually transformed into the organised crime as we know it today - involved in activities such as drug trafficking, extortion, smuggling and corruption.²

A significant shift in this development occurred during the Meiji period (years 1868-1912), when the Industrial Revolution and the urbanization of Japan occurred, creating favourable conditions for the emergence of more powerful and informal organizations that began to dominate various sectors of the economy, including gambling, prostitution, and drug trafficking.³

This transition shows how mafia structures gradually evolved from initially "legitimate" business organisations to illegal criminal clans, a process that can be observed in various forms in other countries, including those of the Anglo-Saxon world.⁴

1.1 Historical roots of the Mafia

Criminal organisations are not just a modern phenomenon but have deep historical roots going back to the time when state power was not strong enough to maintain order. It was in these conditions that the first groups began to form, providing protection, settling disputes and at the same time exploiting the weakness of the state apparatus for their own benefit.

¹ Kaplan, 2012, 16-27

² Kaplan, 2012, 16-20

³ Kaplan, 2012, 20-27

⁴ Kaplan, 2012, Xvii-xxiv

One of the earliest known examples of organised crime was the Chinese Triads, which emerged in the 17th century as secret associations fighting against imperial rule. These groups had their own code of honour, a complex hierarchy, and over time focused on illegal trade, gambling, and extortion. The Japanese Yakuza operated in a similar fashion, with roots going back to Edo-era merchants and vagabonds who created their own underworld.⁵

In Europe, the first mafia structures began to appear, particularly in Sicily, where the local population could not rely on a weak and corrupt government. Instead, family clans emerged to provide protection and justice in exchange for loyalty and financial contributions. This principle later gave rise to the Cosa Nostra, one of the world's most notorious mafias.⁶

Similar criminal organizations developed in the United States, where immigrant gangs began to form in the second half of the 19th century. In particular, Italian, Irish and Jewish communities formed their own underworlds that focused on alcohol smuggling, gambling, and extortion. These groups played a key role in the Prohibition era, where the illegal alcohol trade brought huge profits to the mafias and consolidated their power.⁷

Thus, the mafias were always formed in an environment lacking strong state authority and built their structure on the principles of family loyalty, respect, and violence. Although historical conditions have changed, the basic principles of organised crime have in many ways remained the same to the present day.⁸

1.2 Evolution of traditional mafia structures

With the development of organised crime, mafia groups began to build stronger internal structures that allowed them to manage their activities more effectively and minimise the risk of internal conflict or interference from the authorities. Traditional mafias gradually transformed into complex hierarchical organisations with clearly defined rules, roles and a strict code of ethics that ensured their cohesion and stability.⁹

One of the basic features of mafia organisations was the family or clan structure. In the case of the Sicilian Cosa Nostra (translated as "My Cause" or "Our Cause"), the mafia operated on the principle of "famiglia", i.e. families that had a don, a leader with absolute authority. Below him were caporegime (captains) who controlled groups of soldiers (soldati)

⁵ Kaplan, 2012, 257-263

⁶ Kaplan, 2012, 123-126

⁷ Kaplan, 2012, 315-318

⁸ Kaplan, 2012, 132-135

⁹ Dickie, 2004, 21-26

and conducted the orders of the dons. This model was firmly rooted in ancient Sicilian traditions, where loyalty to the family was of higher value than any state authority.¹⁰

A similar system existed in the Italian 'Ndrangheta that developed in Calabria. Here, mafia families were linked by blood relations, which made infiltration and the disintegration of the organisation even more difficult. In Naples, on the other hand, the Camorra developed, which did not have as strict a family structure as the Cosa Nostra but functioned as a looser network of smaller gangs competing for power.¹¹

An essential part of the traditional mafias was the so-called omertà, a strict law of silence. Mafia members were never allowed to cooperate with the authorities, and those who violated this principle faced severe punishment - often in the form of death. This code served as a protection against infiltration and also ensured that even when individual members were arrested, the wider structure of the organisation was not revealed.¹²

As Mafia organizations grew, so did their criminal activities. While initially focused on extortion and protecting businessmen, the mafias gradually expanded into gambling, smuggling, drug trafficking, and money laundering. In the United States, during Prohibition (year 1920-1933), the mafias became enormously rich from the illegal production and distribution of alcohol, thus securing influence in political and business circles.¹³

After the Second World War, mafia organisations increasingly used legal businesses as a cover for their illegal activities. This created interconnected networks between the mafia, politics and business that survived massive state intervention. Some families have even invested in real estate, banking, or construction, extending their influence far beyond the traditional underworld.¹⁴

While traditional mafia structures have been extremely resilient for decades, modern times have brought new challenges. With the development of technology and the strengthening of security forces, it has become increasingly difficult to sustain the old models of organised crime. This has led to a gradual transformation of mafias into more flexible and decentralised groups that are better adapted to the digital age.¹⁵

¹⁰ Dickie, 2004, 13-20

¹¹ Dickie, 2004, 21-26

¹² Dickie, 2004, 48-54

¹³ Critchley, 2009, 12-22

¹⁴ Dickie, 2004, 188-189

¹⁵ Albanese, 2015, 181-203

1.3 The shift to modern forms of crime

As the world has changed with the advent of modern technology and globalisation, organised crime groups have had to adapt their methods to maintain their power and influence. Traditional mafia models, which were based on physical presence, direct control of territory and maintaining fear in communities, have gradually given way to more modern, decentralised, and technologically sophisticated forms of organised crime. This shift has not been sudden but has occurred gradually in response to changes in society, the economy, and the legal environment.¹⁶

With the development of international trade and the free movement of capital, mafia organisations began to expand beyond the borders of their home countries. As a result, their activities became linked to transnational criminal networks, leading to the emergence of global organised crime. The Italian 'Ndrangheta, for example, has become a major player in the international drug trade, with operations ranging from South America to Europe to Asia.¹⁷

This trend was also reflected in the Russian mafia, also known commonly as the Bratva, which after the collapse of the Soviet Union spread its influence to Western countries and began to engage in sophisticated forms of economic crime such as money laundering, tax evasion and stock market manipulation. While traditional mafia groups rely on physical violence and intimidation, modern criminals often choose less visible forms of coercion. Thanks to the boom in the financial sector, mafias have begun to focus on economic crime, corruption, and abuse of state subsidies.¹⁸

Another major shift has been the move towards cybercrime, which allows criminals to operate anonymously and remotely. Whereas bank robberies used to be a physical affair, today most financial fraud takes place online, through hacking, phishing, and ransomware. One of the biggest changes in organised crime is the way illegal commodities are traded. Drugs, guns and forged documents are now available on the dark web, where transactions take place anonymously using cryptocurrencies such as Bitcoin or Monero.¹⁹

This new model of trade allows criminal organisations to bypass traditional distribution networks and reduce the risk of getting caught. In the past, mobsters had to organise complex

¹⁶ Albanese, 2015, 181-207

¹⁷ Dickie, 2004, 21-26

¹⁸ Albanese, 2015, 211-241

¹⁹ Bartlett, 2014, 8-12

smuggling operations, whereas today they can order goods directly from a supplier on the other side of the world and have them delivered via anonymous shipping services.²⁰

Thanks to advanced encryption technologies, modern criminal groups are able to communicate without fear of eavesdropping. Applications such as EncroChat or Sky ECC, which were developed for encrypted communication, became common tools for organised gangs before they were compromised by international security forces in 2020 and 2021. These developments show that mafias are no longer just local organisations controlling certain territories, but global networks using modern technologies to expand their influence

21

²⁰ Holt, 2022, 462-465

²¹ J.J. Oerlemans, 2022, 309-315

2 DIGITALISATION OF ORGANISED CRIME

The development of digital technologies, especially the internet, mobile devices and advanced encryption methods, has enabled organised crime to adapt to new challenges and opportunities. The digitalisation of crime has brought about fundamental changes in the way organised crime groups operate and are able to conduct their activities. While in the past, criminal organisations focused on traditional forms of illegal activities such as drugs, weapons, prostitution or extortion, digitalisation has enabled the emergence of new forms of organised crime that are completely connected to the internet and digital technologies.²²

One of the biggest benefits for organised crime has been the ability to communicate and conduct transactions anonymously on the Internet. Criminal organisations have begun to move to the dark web, the hidden part of the Internet where most illegal activities take place, including drug trafficking, arms trafficking and stolen identities. The dark web provides an environment that is difficult to monitor and regulate, thereby allowing criminals to hide their identities and operations from the law.²³

With the digitalisation of organised crime, the nature of the crime itself has changed. In many cases, there is no longer a need for physical contact between perpetrators and victims. Crime is moving into cyberspace, where criminals can operate remotely, without personal involvement. This means that organised crime groups can operate internationally, and their operations can involve hundreds to thousands of people from various parts of the world.²⁴

This shift from traditional "physical" organised crime to its digital forms also brings new challenges for law enforcement agencies. It is difficult to prosecute criminals who use digital methods and technological tools to conduct crimes, as many of them operate from extremely protected, geographically dispersed locations. With the emergence of new digital crime methods, such as money laundering through cryptocurrencies and the use of anonymous payment methods, it has become more difficult not only to identify them but also to secure sufficient evidence.²⁵

It is becoming advantageous for organised crime to use cryptocurrencies as a tool for conducting financial transactions. Thanks to cryptocurrencies, criminal organisations can

²² Bartlett, 2014, 12-16

²³ Bartlett, 2014, 12-16

²⁴ Holt, 2022, 452-453

²⁵ Albanese, 2015, 69-81

move large sums of money between different countries without being easily traced. Due to the anonymity of cryptocurrencies such as Bitcoin or Monero, which ensure that transactions are not publicly visible, they have become a popular choice for financing illegal activities.²⁶

The growth of digitalisation of organised crime is also linked to the increased use of customised technology, for example for attacks on government and corporate infrastructures. Cyber-attacks such as ransomware attacks (where data is "hijacked" and a ransom is demanded for its return) have become frequent practice among organised groups that use sophisticated tools to infiltrate targeted systems. This new form of cybercrime shows how far organised crime groups have come in adapting to technological advances.²⁷

In addition, digital spying and cyberbullying are increasingly emerging as methods by which criminals manipulate victims. New forms of surveillance and collection of personal data through malware, spyware and other malicious tools allow organised crime to access sensitive information that can then be used for fraud or extortion.²⁸

This move into the digital space not only makes criminal operations much more accessible and dynamic but also requires law enforcement agencies to continuously adapt to the new technological challenges that are emerging with the development of the internet and digital tools. It also points to contemporary trends in the way organised crime is highly globalised and adapted to the new challenges posed by the digital age.²⁹

2.1 The impact of the Internet and technology

The Internet has provided the Mafia and other criminal organisations with a space where they can operate without geographical restrictions. While it used to be necessary to physically control territory, control is now shifting to the realm of cyberspace – instead of the streets, criminals move in anonymous discussion forums, encrypted networks and specialised platforms where drugs, weapons, fake documents, or stolen data are traded.³⁰

The main advantages of the internet for organised crime include:

- Anonymity – the use of VPNs, encrypted communications and anonymous transactions makes it difficult to detect perpetrators.

²⁶ Bartlett, 2014, 78-83

²⁷ Holt, 2022, 143-145

²⁸ Holt, 2022, 334-336

²⁹ Marsh, 2019, 193-227

³⁰ Shelley, 2018, 241-244

- Global reach – the mafia is no longer limited to a specific country or region but can operate internationally with minimal physical contact.
- Automation of crime – sophisticated cyber-attacks can be carried out automatically using malware, allowing crimes to be committed on a large scale.
- Encrypted communication and its importance to the underworld

³¹

Modern criminal groups rely on encrypted communication platforms that allow them to organise operations without the risk of eavesdropping. An example is EncroChat, a network designed for secure communication that has been used by drug dealers, mafia groups and other criminal organisations around the world. After it was breached in 2020, security forces uncovered thousands of criminal operations, showing how important these tools are to the underworld.^{32, 33}

After the closure of EncroChat and similar platforms, organized crime has moved to even more sophisticated methods of communication, including custom encrypted applications and darknet forums with strict input authentication. In parallel, mafia groups have increasingly begun to focus on automated cyberattacks and fraud, using advanced algorithms and artificial intelligence to maximise their reach and effectiveness.³⁴

One of the most prevalent methods is phishing and social engineering, where attackers fraudulently obtain personal information or passwords to bank accounts. Another significant threat is ransomware attacks, in which malware encrypts victims' data and perpetrators then demand a ransom in cryptocurrency to recover it. Botnets, which are large networks of compromised computers that are used to launch massive cyber-attacks, steal funds or spread disinformation, also play a significant role.³⁵

This shift towards digital crime methods clearly shows that organised crime is no longer limited to physical activities, but is increasingly moving into the digital cyberspace, where it is gaining new opportunities for operations with minimal risk of detection.³⁶

³¹ Holt, 2022, 182-185

³² Holt, 2022, 177-183

³³ J.J. Oerlemans, 2022, 309-315

³⁴ Holt, 2022, 209-231

³⁵ Holt, 2022, 431-433

³⁶ Holt, 2022, 139-145

2.2 The shift from physical to digital crime

With the development of technology, organised crime is gradually moving away from traditional methods and into the digital space. This transition brings many benefits – it allows for greater anonymity, reduced physical risk and the expansion of operations to a global level. While traditional mafia practices such as extortion, drug trafficking and the physical elimination of enemies still exist, more and more criminal groups are turning to cybercrime, which is less risky and often more profitable.³⁷

In the past, organised crime groups have dominated in areas such as illegal gambling, alcohol, drug and gun trafficking, and protection rackets. These practices often required violence and physical control over a territory. But the advent of digitalisation has significantly changed the form of these activities:

Table 1 Forms of crime

Traditional crime	Digital crime
Ransom and extortion	Ransomware attacks, threats of sensitive data breaches
Drug smuggling	Online marketplaces on the dark web
Money laundering	Cryptocurrency transactions, mixers and anonymous wallets
Fraud and financial crime	Online phishing, identity theft, ATM skimming
Illegal gambling	Online casinos and betting platforms on the dark web

(source: own elaboration based on Albanese, 2015, 181-203)

This shift does not mean that traditional methods of organised crime have completely vanished, but rather that they have adapted to the new possibilities offered by the digital

³⁷ Marsh, 2019, 193-200

environment. Many forms of crime have been moved online, giving criminal groups not only greater flexibility but also global reach and anonymity.³⁸

One notable change is cyber extortion, which has replaced earlier physical intimidation with more sophisticated methods such as DDoS (which stands for "distributed denial of service") attacks on companies, which are then forced to pay ransoms in order to restore their services. Another widespread tactic is blackmail by threatening to publish sensitive data or manipulated deepfake videos that can damage the reputation of individuals and companies.^{39, 40}

Traditional money laundering has also undergone a fundamental change - whereas previously illicit financial flows were hidden through complex networks of bank accounts and fake companies, today cryptocurrencies, anonymous wallets and sophisticated mixing services have taken over this role, allowing the origin of illicit income to be effectively disguised.⁴¹

Similar developments can be observed in the drug and arms trade. While previously it was necessary to arrange transactions in person and rely on physical smuggling, today it is possible to order illegal goods anonymously via the dark web and have them delivered directly by mail, thus significantly reducing the risk for sellers and buyers.⁴²

2.2.1 Crime as a Service: a new business model

Modern digital crime is increasingly professionalised and has gradually transformed into a Crime-as-a-Service (CaaS for short) model, where criminals offer their illegal services on demand. This system allows even less tech-savvy individuals to enter the world of cybercrime without the need for advanced IT skills. The most commonly offered services include hiring hackers for targeted cyber-attacks, selling stolen databases containing sensitive personal information, or offering ransomware kits that even inexperienced cybercriminals can purchase to carry out their own attacks. In addition, the trade in fake documents and identities, which allow anonymous transactions and facilitate the circumvention of security measures, is becoming increasingly common.⁴³

³⁸ Albanese, 2015, 181-193

³⁹ Holt, 2022, 23-24

⁴⁰ Westerlund, 2019

⁴¹ Bartlett, 2014, 64-66

⁴² Bartlett, 2014, 114-120

⁴³ Prithwish, 2024, 1-9

This development means that it is no longer necessary to be a professional hacker to commit digital crime – simply ordering the desired service on a darknet marketplace and paying in cryptocurrency reduces the risk of detection while expanding the opportunities for various criminal activities.⁴⁴

2.3 The Growing Influence of Artificial Intelligence

Technological advances in Artificial Intelligence (AI) over the past decades have caused major changes in many sectors, from industry and healthcare to cybersecurity and crime. While AI offers immense benefits - from automating complex processes to rapidly analysing large volumes of data - it is also creating new challenges that are fundamentally affecting the security and stability of society.⁴⁵

AI has become not only a tool in the fight against crime, but also a weapon in the hands of criminal organisations. Organised crime, which has historically adapted to the changing conditions of society, is now increasingly using advanced AI technologies to strengthen its activities. From sophisticated cyber-attacks to spreading disinformation and fraud to automating illicit financial transactions, AI is enabling criminals to operate more efficiently and covertly than ever before.⁴⁶

One of the key characteristics of AI is its ability to learn from vast amounts of data and adapt to new conditions. However, this means that traditional methods of fighting crime can quickly become obsolete. Security and state institutions must therefore constantly adapt to keep up with technological innovations that can be exploited for criminal purposes.⁴⁷

Another important aspect of AI is its ability to influence human behaviour. For example, generative AI tools can create realistic deepfake videos that distort reality and can be used to blackmail, spread propaganda or manipulate public opinion. In turn, AI-driven social networking algorithms can purposefully spread misinformation and radicalise users. All this contributes to a new form of hybrid threat, where digital crime is intertwined with political and social conflicts.⁴⁸

At the same time, however, AI is also being used to defend against these threats. Predictive analytics, machine learning and advanced algorithms are helping security forces

⁴⁴ Bartlett, 2014, 114-120

⁴⁵ Prithwish, 2024, 37-39

⁴⁶ Prithwish, 2024, 19-22,36-37

⁴⁷ Prithwish, 2024, 36-37

⁴⁸ Westerlund, 2019

identify suspicious activity, monitor financial transactions and prevent cyber-attacks. AI is also becoming a key component of cybersecurity systems that can detect threats in real time and automatically respond to attempted breaches of digital infrastructure.⁴⁹

In addition to the decentralisation of cybercrime, artificial intelligence is becoming an increasing threat, which criminal organisations are using to automate fraud and further streamline their operations. AI is not only enabling the creation of deepfake videos used to blackmail and discredit public figures, but also optimising phishing campaigns, which are becoming increasingly convincing and harder to detect thanks to machine learning.⁵⁰

Another dangerous aspect is the ability of AI to generate fake identities that can be almost indistinguishable from real people. These identities are used not only for financial fraud, but also to manipulate public opinion or infiltrate security systems. Thanks to these technologies, organised crime is becoming increasingly professionalised and expanding its capabilities, posing a growing challenge to legal and security forces around the world.⁵¹

2.3.1 The future of AI and its impact on the security environment

The future of AI in security and crime promises to bring innovative technologies and challenges that will have a major impact on the overall security environment. With the rapid development of AI and machine learning, the technologies we know today are expected to become more sophisticated, allowing security forces to not only protect the population more effectively, but also to counter new and unexpected threats.⁵²

The future of security could see the emergence of advanced cybercrime detection and prevention tools that can automatically respond to cyber-attacks in real time. Another area that is likely to develop is the use of autonomous systems that will be able to conduct investigations or protect specific areas without the need for human intervention. This could include drones and robots that would monitor critical infrastructure assets or conduct area inspections.⁵³

As AI continues to evolve, it is likely that new forms of crime will emerge that use AI. For example, cybercriminals may use AI to create increasingly sophisticated attacks that will

⁴⁹ Eckerson, 2007, 2-3

⁵⁰ Westerlund, 2019

⁵¹ Westerlund, 2019

⁵² Prithwish, 2024, 41-44

⁵³ Prithwish, 2024, 42-43

be harder to detect. In contrast, as technologies for creating deepfake content develop, new forms of fraud and manipulation of public opinion may emerge.^{54, 55}

Security authorities and regulators will need to respond to these dynamic developments. This includes the development of new legal frameworks capable of coping with the rapid advances in technology. Regulatory agencies will need to set new standards for privacy and data protection in the context of the expanding use of AI. Collaboration between governments, technology companies and non-profit organisations will also be a key step in creating global rules for the safe and ethical use of AI.⁵⁶

Ultimately, striking a balance between protecting society from threats and preserving fundamental human rights and freedoms will be essential. In the future, not only technological innovation will be key, but also the ability of organisations and government agencies to adapt to rapid change and respond to the new challenges that AI will bring.⁵⁷

2.4 The Dark Web as a space for illegal activities

With the increasing digitalisation of organised crime, the dark web has become one of the main venues for illegal activities. This hidden part of the Internet, accessible only through special anonymising tools such as the anonymous web browser Tor (which stands for "The Onion Router"), allows anonymous communication, trading and financial transactions, providing an ideal environment for various forms of criminality.⁵⁸

The dark web is a specific part of the internet that is part of the wider deep web - a space that is not indexed by mainstream search engines such as Google. While the deep web includes, for example, corporate databases, academic archives or internal government systems, the dark web represents its darker side, where criminal organisations, hackers and illegal traders are concentrated. This hidden ecosystem offers anonymity and relative safety from surveillance, making it an ideal platform for a range of illegal activities.⁵⁹

One of the main ways organised crime uses the dark web is through black markets, also known as darknet marketplaces. Drugs, weapons, fake documents, hacking tools and other prohibited products are traded on these illegal marketplaces. Trading here works similarly

⁵⁴ Prithwish, 2024, 41-42

⁵⁵ Westerlund, 2019

⁵⁶ Prithwish, 2024, 12-13, 15-16

⁵⁷ Prithwish, 2024, 37, 42-47

⁵⁸ Bartlett, 2014, 8-12

⁵⁹ Bartlett, 2014, 9

to regular e-commerce platforms - buyers can rate sellers and provide feedback, which helps build trust among anonymous users. This system greatly facilitates access to illegal services and goods without the need for a physical meeting between merchants and customers.⁶⁰

In addition to marketplaces, the dark web also serves as a communication hub for criminal organisations using encrypted forums and chat services. These platforms enable the secure coordination of illegal activities, information sharing and trading of sensitive data. They are often only accessible through a rigorous authentication process, which ensures that unwanted individuals, including police investigators, do not gain access to the network.⁶¹

Another important function of the dark web is the provision of criminal services on demand, which is referred to as Crime-as-a-Service (CaaS). This business model allows even less experienced individuals to use sophisticated cyber-attacks without the need for technical expertise. On the dark web, for example, hackers can be hired to target companies or individuals, purchase stolen databases containing personal information, or gain access to ransomware kits that allow for the extortion of victims. In some cases, criminals even offer the services of assassins, although these are often just defrauds to extort money from gullible clients.⁶²

A very widespread industry on the dark web is the trade of personal data and identities. Stolen databases containing passwords, payment details, passports and ID cards can be found on specialised forums. This information is then used for financial fraud, identity theft or other criminal activities. Moreover, as deepfake technologies and artificial intelligence grow in quality, it is becoming increasingly difficult to detect fake identities, allowing criminals to operate with even greater anonymity.⁶³

Among the most serious and heinous crimes enabled by the dark web is the distribution of child pornography and abuse-related material. This type of illegal content is one of the main targets of police investigations targeting the dark web. However, despite repeated crackdowns by law enforcement agencies, such activities are constantly moving to new platforms, making it exceedingly difficult to suppress them definitively.⁶⁴

⁶⁰ Bartlett, 2014, 66-70

⁶¹ Bartlett, 2014, 83-87

⁶² Prithwish, 2024, 1-9

⁶³ Westerlund, 2019

⁶⁴ Bartlett, 2014, 117-122

In the past, several large darknet marketplaces have emerged and played a key role in online crime. The first major marketplace was Silk Road, which operated between the years 2011 and 2013 and allowed anonymous trading of drugs and other illegal products. After its closure by the FBI and the arrest of its founder, Ross Ulbricht, a number of new marketplaces emerged to fill the vacuum. Among the most prominent of these was AlphaBay, which operated between 2014 and 2017 and was one of the largest dark web marketplaces of its time. The same fate befell Hansa Market, which was secretly taken over by European security forces in 2017, who used it to monitor user transactions before shutting it down for good.^{65, 66, 67}

Despite police crackdowns and closures of darknet marketplaces, the dark web remains a dynamic and adaptable environment. Each time a major marketplace is suppressed, new ones emerge, often with improved security measures and more sophisticated anonymisation methods. This constant progress shows that the fight against organised crime on the dark web is a long-term one and requires constant innovation by both security forces and cybersecurity regulators.⁶⁸

While marketplaces are regularly shut down, new ones are quickly emerging, often with more sophisticated security features that make them harder to track down and shut down. Most transactions on the dark web are conducted through cryptocurrencies, which allow for relative anonymity. Bitcoin has long been the main currency on the dark web, but because of its traceability, Monero, Zcash, and other anonymous cryptocurrencies that are designed to obscure transaction history are now increasingly used.⁶⁹

The use of cryptocurrencies not only enables trading, but also money laundering and the financing of other criminal activities. The use of "mixers" and "tumblers" can hide the origin of funds and make them difficult to trace.⁷⁰

2.5 Cryptocurrencies and Financial Transactions in the Underworld

Cryptocurrencies have become a key tool in digital organised crime, mainly due to their anonymity, decentralisation and lack of strict regulation. These factors make them an ideal

⁶⁵ Prithwish, 2024, 7-9

⁶⁶ Afilipoaie, 2018, 1-5

⁶⁷ Holt, 2022, 462-465

⁶⁸ Bartlett, 2014, 68-74

⁶⁹ Bartlett, 2014, 78-83

⁷⁰ Bartlett, 2014, 132-134

medium for financing illicit activities, as they enable fast and almost untraceable transactions across the globe. Although some governments and financial institutions are introducing increasingly stringent measures to monitor and regulate crypto-transactions, criminal organisations are constantly looking for new ways to circumvent these restrictions and maintain the anonymity of their operations.⁷¹

One of the most common ways criminals abuse cryptocurrencies is by using them to pay for illegal goods and services. Most transactions on the dark web are conducted entirely in cryptocurrency, which facilitates anonymous transactions between buyers and sellers. Thus, cryptocurrencies eliminate the need for traditional financial institutions and allow bypassing banking controls and tracking financial flows.⁷²

Another key aspect is money laundering, where criminals use sophisticated techniques to hide the origin of illegally obtained funds. Mixers and tumbler services are often used for this purpose, breaking transactions into smaller amounts and routing them through various cryptocurrency wallets. This process makes it significantly more difficult to track the movement of funds and their links to specific individuals or organisations. In addition, criminals use decentralised exchanges (DEX), which, unlike centralised platforms such as Coinbase or Binance, do not require registration and allow anonymous exchanges of cryptocurrencies without identity verification.⁷³

One of the most serious misuses of cryptocurrencies is their use in extortion attacks (ransomware). In these cases, hackers attack victims' systems, encrypt their data and then demand a ransom, which must be paid in cryptocurrency. This model has become extremely profitable, as victims will often pay rather than risk losing important files or disclosing sensitive information.⁷⁴

In addition to ordinary crime, cryptocurrencies are also used to fund terrorism and other criminal operations. Due to their decentralised nature, they enable anonymous money transfers without the oversight of state institutions, making them an attractive tool for terrorist organisations and mafias operating on a global scale.⁷⁵

⁷¹ Holt, 2022, 460-468

⁷² Holt, 2022, 460-468

⁷³ Prithwish, 2024, 12-15

⁷⁴ Holt, 2022, 143-145

⁷⁵ Prithwish, 2024, 12-15

In response to these risks, regulators around the world are seeking to curb the abuse of cryptocurrencies through stricter rules. Many countries are implementing Know Your Customer (KYC) and Anti-Money Laundering (AML) policies that force crypto exchanges to identify their users and monitor suspicious transactions. Some governments are even considering bans on anonymous cryptocurrencies such as Monero (abbreviated XMR), which hide not only the identity of the sender and recipient, but also the amount of the transaction.⁷⁶

Despite these efforts, however, completely stopping illegal crypto transactions remains extremely difficult because blockchain technology is decentralized and globally distributed. Cryptocurrencies are constantly evolving, and criminal organisations are finding new ways to circumvent regulations, which poses one of the biggest challenges in digital security and financial crime.⁷⁷

⁷⁶ Prithwish, 2024, 13

⁷⁷ Bartlett, 2022, 9-12

3 IMPACT OF ORGANISED CRIME ON SOCIETIES AND THEIR SECURITY

Organised crime, whatever its specific form, represents one of the most serious security risks to society in modern times. Historically, its impact has been primarily associated with physical crime, smuggling, extortion, corruption and violence. Today, however, with the advent of digitalisation and the rapid development of information technology, this threat has been transformed and greatly expanded. Criminal groups are now taking advantage of the new opportunities offered by the digital environment to move their activities into a sphere that is less visible, more anonymous and often much more profitable than traditional forms of crime.⁷⁸

The impact of cyber organised crime on society and security is now so extensive that it affects not only the economy and the daily lives of citizens, but also the very foundations of trust in state institutions, the rule of law and the functioning of society as a whole. Digital crime brings new forms of attacks, such as ransomware campaigns, attacks on critical infrastructure, massive data leaks, but also fraud, affecting the daily lives of millions of people. The impact of these phenomena is not limited to large multinational companies or governments but affects a wide range of victims - from small businesses to individual citizens whose identity, finances or privacy may be at risk.⁷⁹

3.1 Cybersecurity threats

One of the biggest and most pressing risks posed by organised crime is the threat to cybersecurity. Traditional forms of crime, such as drug trafficking, extortion or trafficking, are now increasingly moving into the digital space, allowing criminals to operate globally and bypass local legal systems.⁸⁰

Cybercrime covers a wide range of illegal activities, including phishing, ransomware, identity theft, DDoS attacks and other forms of online fraud. This crime has rapidly evolved and become highly sophisticated. Mafia organizations that used to focus primarily on physical crimes are now using modern technology to infiltrate systems, steal sensitive data, and destabilize economic and government institutions.⁸¹

⁷⁸ Albanese, 2015, 220-236

⁷⁹ Bartlett, 2014, 8-12

⁸⁰ Holt, 2022, 144-145

⁸¹ Prithwish, 2024, 6-7

At the same time, cybercrime is becoming a tool for traditional forms of crime, for example, through illegal drug or arms trafficking, which often takes place through dark web marketplaces. Hacker groups linked to organised crime can have access to vast amounts of sensitive information and funds, threatening the security of individuals and companies. The consequences of these attacks can be devastating - from loss of trust in financial institutions to widespread financial damage. Combating these new forms of crime requires innovative approaches to cyber security and international cooperation, as organised crime in the digital era crosses national borders.⁸²

3.2 The misuse of AI by organised crime

The use of artificial intelligence (AI) in organised crime is a dangerous and highly effective form of cybercrime. With the development of AI, criminal organisations are increasingly focusing on its automation, analysis and prediction capabilities, allowing them to plan and execute illegal activities more effectively. AI provides criminals with tools that can not only speed up and simplify their operations but also make them harder to detect and defend against.⁸³

One of the most significant ways organized crime is using AI is to automate cyberattacks. Using machine learning and algorithms, criminals can create complex attacks that are able to learn and adapt to the security measures of targeted systems. This makes them increasingly effective at attacking corporate infrastructures, banking systems, and even individuals. For example, ransomware attacks that demand a ransom for decrypting victims' data can now be much more extensive and target multiple vulnerabilities simultaneously.⁸⁴

Another important aspect is the ability to generate deepfake content, a technique that organised crime can use for fraud and extortion. With the help of AI, realistic fake videos and audio recordings can be created that can harm individuals or companies, either for financial gain or to damage their reputation.⁸⁵

In addition, organized crime is focusing on using AI to predict behaviour. With the ability to analyse vast amounts of data, AI can estimate weaknesses in security systems and predict the behaviour of individuals or organisations, allowing criminals to target specific

⁸² Holt, 2022, 23-26

⁸³ Prithwish, 2024, 41-44

⁸⁴ Bartlett, 2014, 8-12

⁸⁵ Westerlund, 2019

vulnerable targets. This technology also helps to automate and streamline the logistics of illegal operations such as drug or arms trafficking.^{86, 87}

3.3 Misuse of AI by the Public and Individuals

The use and misuse of AI is undoubtedly not limited to organised crime. With the increasing availability of AI tools, it is also becoming more widespread among ordinary users and individuals who can use them for illegal or malicious activities. These abuses can have far-reaching consequences for individuals, societies, and even democratic institutions.⁸⁸

One of the most widespread abuses of AI is the generation of deepfake videos and voices. These technologically advanced tools enable the creation of realistic fake images and audio recordings that can harm the privacy of individuals, damage the reputation of public figures, and even influence the political process. Such fake material can be used to create false accusations, spread disinformation or manipulate public opinion. This phenomenon has become particularly dangerous during election campaigns, where deepfake technologies can be used to spread false claims and destabilise political systems.⁸⁹

Another form of AI misuse is the manipulation of public opinion. Using sophisticated algorithms that can analyse and predict individuals' behaviour based on their online activities, targeted advertising campaigns can be created that not only sell products but also influence opinions and political choices. Algorithms can tailor content to resonate with users' specific emotions, making them a powerful tool for manipulating voters and public opinion.⁹⁰

In the area of cyberbullying and online stalking, the misuse of AI is another major concern. People can use technology to create false or fake identities, spread rumours or target individuals for harassment. Thanks to the anonymity of the internet and the power of AI, abusive individuals can create realistic but fake images and audio to destroy the lives and reputations of their victims, making it increasingly difficult for victims to defend themselves or reveal the real culprit.⁹¹

⁸⁶ Eckerson, 2007, 2-3

⁸⁷ Prithwish, 2024, 3

⁸⁸ Prithwish, 2024, 4-7

⁸⁹ Westerlund, 2019

⁹⁰ Eckerson, 2007, 2-3

⁹¹ Holt, 2022, 334-336

3.4 Impact on businesses and the economy

Organised crime also has a significant impact on the economy and the functioning of businesses. Traditional methods of extortion, bribery or blackmail have been commonly used in the recent past to keep mafia groups in control of a particular area or industry. Today, this model has changed in response to globalisation and technological advances, but the principles of extortion and illegal activities remain relevant.⁹²

Companies that do not protect their cyber security become easy targets for hacking attacks or for threats and extortion that can lead to huge financial losses. Ransomware attacks, where criminals lock up company data and demand ransom, are now frequent practice. In addition to direct financial losses, organised crime also causes reputational damage, which can have long-term consequences for businesses and their client relationships.⁹³

Another economic impact occurs when criminal organisations control certain legal industries such as construction, alcohol, tobacco or gambling. Illegal activities such as money laundering or fraud affect market dynamics because illegal money can distort prices and competition. This can lead to inefficient allocation of resources, loss of investment and destabilisation of corporate structures. At the same time, as criminal organisations increasingly engage in "digital entrepreneurship", there is a proliferation of activity that is directly linked to technology. Attacks on financial systems, banking institutions or even global financial markets have the potential to affect the global economy, demonstrating how dangerous cybercrime organisations can be.⁹⁴

3.5 Social structures and crime

Criminal organisations also have a profound effect on the social structures and everyday lives of ordinary people. In areas where organised crime has gained dominance, basic social values are eroded, and communities are destabilised. Criminal groups often exploit poor and vulnerable communities to recruit new members who are then involved in illegal activities.⁹⁵

In many cases, organised crime provides social and economic services where traditional institutions have failed. The mafia can offer protection or assistance in crisis situations,

⁹² Albanese, 2015, 181-203

⁹³ Bartlett, 2014, 8-12

⁹⁴ Watters, 2023, 69-71

⁹⁵ Critchley, 2009, 89-93

making it an attractive "partner" for some individuals who have no other option. This leads to a cycle of poverty and dependence on criminal organisations that gradually creates strong links in society.⁹⁶

Other social impacts are associated with violence, which is often linked to organised crime. Conflicts between criminal groups can lead to escalating violence and casualties in communities. This violent nature of crime has a devastating effect on morale and trust in the legal system. It creates informal structures that tend to replace the state as protector and arbiter in conflicts.⁹⁷

When it comes to modern organised crime, with the shift to digital platforms, there are new social problems such as cyberbullying, online fraud and defending against identity theft. These new forms of crime have similarly destructive effects on individuals and communities, as they can lead to severe psychological and financial consequences for victims.⁹⁸

3.6 Predictive Analytics and Crime Prevention

Artificial intelligence has a vital role in predictive analytics, which is used to prevent crime. Using advanced algorithms and machine learning, AI can analyse vast amounts of data, identifying patterns of behaviour and erroneous trends that could indicate potential future crimes. This approach, known as "predictive policing," helps security forces focus their efforts on high-risk areas or individuals, which can lead to faster detection and prevention of crimes before they occur.⁹⁹

Predictive analytics uses historical data, such as records of previous crimes, demographics, temporal patterns, and geographic information to create patterns of behaviour. In this way, law enforcement can better understand where and when crime is likely to occur. For example, algorithms can identify potential areas where burglaries or acts of violence could occur and deploy police in those zones before the crime actually occurs.¹⁰⁰

However, there are also a number of ethical issues associated with this technology. Of greatest concern are the issues of bias and discrimination that may be inherent in historical data. For example, when predictive models use data that reflect historical biases, they can lead to certain populations being incorrectly labelled as "high risk" based on their ethnicity

⁹⁶ Critchley, 2009, 234-239

⁹⁷ Kaplan, 2012, 275-276

⁹⁸ Holt, 2022, 334-336

⁹⁹ Eckerson, 2007, 2-3

¹⁰⁰ Prithwish, 2024, 37-38

or socioeconomic status. This can lead to uneven law enforcement and human rights violations.¹⁰¹

Another ethical issue is how predictive tools can be deployed without violating the privacy and freedoms of individuals. There is a risk that predictive technologies may be used to unduly track and monitor people based on suspicions that may not be supported by concrete evidence, which could threaten fundamental civil liberties.¹⁰²

¹⁰¹ Prithwish, 2024, 39-41

¹⁰² Prithwish, 2024, 39-41

4 LEGAL AND TECHNOLOGICAL RESPONSES TO ORGANISED CRIME

New legal and technological initiatives aimed at protecting society and security are emerging in response to the growing threat of organised crime, which is increasingly moving into the digital sphere. These responses include both a legal framework that is evolving in line with changing technologies, and new tools and methods to combat cybercrime, including the use of advanced technological options, such as artificial intelligence, to detect and prevent crime.¹⁰³

4.1 Legal Framework and International Cooperation

As organized crime becomes increasingly globalized, there is an emphasis on international cooperation and the development of a legal framework to effectively combat these organizations on a global level. Traditional legal systems that were developed to combat physical forms of crime are now facing challenges in the area of cybercrime, which knows no national borders. Criminal organisations operating in the digital space can operate on a global level and so there is an increasing emphasis on a coordinated international response.¹⁰⁴

International organisations such as INTERPOL and EUROPOL have developed mechanisms for the exchange of information and coordination of investigations between different states. These organisations assist in the tracking and apprehension of criminals operating across borders. At the same time, special legislation has been developed to address cybercrime, including directives and agreements between states to combat this new form of crime.¹⁰⁵

The next step is the passing of new cybersecurity laws aimed at reducing the risk of misuse of innovative technologies. Examples include data protection laws, such as the GDPR in the European Union, which not only protect the privacy of individuals but also require companies to comply with strict rules to ensure data security, which can reduce the scope for cybercrime.¹⁰⁶

¹⁰³ Watters, 2023, 28-31

¹⁰⁴ Watters, 2023, 43-47

¹⁰⁵ Prithwish, 2024, 31-34

¹⁰⁶ Prithwish, 2024, 19-22

4.2 Combating and preventing cybercrime

As the threat of cybercrime grows, new tools and technologies are emerging to prevent, detect and investigate these crimes. Traditional methods of investigation that relied on physical evidence and fieldwork have been supplemented by advanced technological tools. Police and security forces now use specialised software to monitor internet activity, analyse data and identify potential threats before the crime itself occurs.¹⁰⁷

Cybercrime prevention is increasingly focused on raising awareness and educating the general public about threats on the internet. Various organisations and government institutions are organising training sessions for businesses, individuals and schools to educate them about the latest types of crimes such as phishing, ransomware and online fraud. The aim is to minimise the risk of falling victim to these crimes, while raising awareness of how to protect themselves from cyber threats.¹⁰⁸

Another prevention is investing in a strong cyber infrastructure that includes advanced encryption, firewalls and antivirus systems to protect devices and data from unauthorized access. In some cases, companies are even starting to invest in their own cybersecurity and hire cyber threat experts, making it harder for organised crime groups to do their job.¹⁰⁹

4.3 Ethical and Social Challenges of AI in Crime

The use of AI in crime poses a number of ethical and social challenges that need to be carefully considered when formulating policy and laws. Although AI offers unprecedented opportunities for improving human life, its misuse in illegal activities poses a fundamental problem that has the potential to seriously undermine security, privacy and trust in society.¹¹⁰

One of the most fundamental ethical issues is the question of accountability for crimes committed using AI. Who is responsible when crimes are committed by an autonomous system or algorithm that makes decisions without human intervention? Is it the AI producer who created the technology? Or the user who misused it? Creating clear frameworks for liability is key, but there is still a lack of legislation to clearly address this issue.¹¹¹

¹⁰⁷ Holt, 2022, 9-13

¹⁰⁸ Prithwish, 2024, 35-37

¹⁰⁹ Prithwish, 2024, 41-44

¹¹⁰ Prithwish, 2024, 37

¹¹¹ Prithwish, 2024, 39-41

Other ethical challenges are issues of fairness and equality. AI can be deployed in areas such as predictive models for crime detection, leading to problems with prejudice and discrimination. For example, AI algorithms that analyse historical data may inadvertently reinforce racial or socioeconomic inequalities by targeting certain community or ethnic groups as potential perpetrators. This bias in algorithms can lead to unfair decisions and human rights violations.¹¹²

Socially, the misuse of AI in crime can destroy the lives of individuals. If people are victims of deepfake technologies, they may find themselves in a difficult life situation where it is almost impossible for them to prove the truth, especially if their personal information or identity has been used to damage their reputation. Artificial intelligence, if abused, can therefore not only disrupt security but also disrupt people's personal and professional lives.¹¹³

4.4 AI as a tool in the defence against digital crime

Artificial intelligence is not only a tool that organised crime uses for illegal activities but can also play a key role in the defence against digital crime. As AI advances, the way security agencies, governments and organisations protect their systems from cybercrime is changing. AI is becoming an invaluable tool for identifying, preventing and responding to cyber threats.¹¹⁴

One of the main uses of AI in defense is predictive analytics. Security organizations can use machine learning to analyse massive amounts of data in real time and predict potential threats or attacks. Algorithms can identify patterns and anomalies that a human analyst might miss, enabling early warning and rapid response to emerging cyber threats. This technology is particularly useful in protecting critical infrastructures such as energy grids, financial institutions or healthcare systems.¹¹⁵

Another valuable tool is AI-driven systems for detecting and preventing attacks. Security systems can use AI to monitor network traffic and detect unusual activity that may indicate cyber-attacks, such as ransomware or phishing campaigns. This technology is able

¹¹² Prithwish, 2024, 39-41

¹¹³ Prithwish, 2024, 41-45

¹¹⁴ Prithwish, 2024, 12-16

¹¹⁵ Eckerson, 2007, 2-3

to autonomously block malicious activity and isolate compromised systems, minimizing potential damage.¹¹⁶

Artificial intelligence is also used in the field of analysis and forensic investigation. AI can be used to analyse digital footprints and identify cyber criminals, which is essential for investigating complex cases such as hacktivism, cybercrime and financial fraud. Image and text recognition technology helps reveal hidden evidence, simplifying the process of evidence collection and analysis.¹¹⁷

AI is able to analyse vast amounts of data and look for patterns that would be difficult for a human to spot. This technology can help in identifying potential criminals and tracking their activities online.¹¹⁸

Artificial intelligence is used, for example, in the analysis of financial transactions, where it can detect suspicious patterns and identify money laundering or illegal trading. It is also used in the analysis of communications between criminal groups, for example on encrypted platforms, where AI can detect unusual patterns of behaviour and locate suspicious individuals or groups.¹¹⁹

In conjunction with other technologies such as machine learning and predictive analytics, artificial intelligence offers law enforcement authorities new tools to effectively predict and prevent crime. This technology can significantly speed up response times and provide better tools for tracking and combating organised crime, which today increasingly uses digital space.¹²⁰

Another significant advantage of AI is its ability to learn and adapt. As the AI system detects new types of attacks, it can adapt and improve its protection capabilities in the future. This dynamic approach to security is key in combating increasingly sophisticated threats.¹²¹

¹¹⁶ Gadde, 2021, 386-387

¹¹⁷ Holt, 2022, 375-378

¹¹⁸ Prithwish, 2024, 36-38

¹¹⁹ Prithwish, 2024, 36-39

¹²⁰ Westerlund, 2019

¹²¹ Prithwish, 2024, 41-45

II PRACTICAL PART

5 THE HISTORICAL DEVELOPMENT AND SHIFT TO DIGITAL FORMS OF CRIME IN THE U.S. AND THE UK

Organised crime in the US and the UK has a long history that goes deep into the past. In both countries, it has evolved from traditional mafia structures to modern forms of cybercrime, which today represent a major security threat. A range of factors have influenced this transition, including legislative measures, technological advances and changes in global trade.¹²²

In the US, the Italian-American Mafia, whose influence peaked in the 20th century, played a key role in organised crime. Following the passage of laws such as the Racketeer Influenced and Corrupt Organisations Act (RICO in short) in 1970, traditional mafia structures were significantly weakened. However, organized crime adapted - instead of controlling physical areas and businesses, criminal groups began using digital technology to launder money, commit fraud, or distribute illegal content.¹²³

In the UK, organised crime has had a different dynamic. While the US was dominated by the Italian mafia and later cartels, the UK was heavily influenced by Irish criminal organisations, British gangs and later Eastern European crime groups. Tighter oversight of financial operations and the increasing role of intelligence services led British criminal organisations to move online, where they found new ways to circumvent the law - for example, through hacking, trading in stolen data or ransomware attacks.¹²⁴

Both countries have thus found themselves in a phase where classic methods of organised crime are giving way to sophisticated digital strategies. While the US still has strong links to traditional mafia structures, the UK is focusing on cybercrime as a major threat to national security. This development requires new methods of fighting organised crime, which translates into legislative changes and technological innovation.¹²⁵

5.1 The economic impact of digital crime

The digital transformation of organised crime is having a significant impact on the economy in both the US and the UK. Both countries experience a range of financial losses due to

¹²² Prithwish, 2024, 22-27

¹²³ Sifakis, 1987, 490-497

¹²⁴ Critchley, 2009, 1-5

¹²⁵ Prithwish, 2024, 22-27

cyber-attacks, fraud and money laundering. These activities directly affect both large corporations and small businesses, and their impact is reflected in the global economy.¹²⁶

In the U.S., where traditional forms of organised crime continue to blend with digital methods, attacks are occurring that have the potential to disrupt the operations of large financial institutions and corporations. Ransomware attacks and sophisticated phishing campaigns lead to huge financial losses, not only through direct theft of funds, but also through the subsequent costs of restoring systems, loss of reputation and investor confidence. In addition, organised crime uses cryptocurrencies for money laundering, making it difficult to track financial flows and complicating the regulation of the financial sector.¹²⁷

In the UK, digital crime is also becoming a fundamental problem, with criminal groups often targeting the banking and financial services sector. UK businesses and government institutions face threats from cyber-attacks that can lead to disruption of business processes and a decline in customer confidence.¹²⁸

The economic losses are not only evident in the financial sector, but also in sectors where high levels of digitalisation are found, such as telecommunications and IT services. Increased investment in cybersecurity, whether in the form of innovative technology or expert staff, represents an additional cost that businesses pay to protect against these attacks.¹²⁹

Particularly in countries such as the US and the UK, where digital technologies are deeply integrated into everyday life and key sectors of the economy, the impact of organised cybercrime is particularly pronounced. Both societies face not only material damage and economic losses, but also changes in perceptions of security, trust in public and private institutions, and social impacts that shape people's everyday behaviour.¹³⁰

Overall, the digitalisation of organised crime is causing profound economic impacts that affect not only the immediate financial performance of businesses, but also the overall stability of the national economy. As attacks become more sophisticated and the digital space becomes increasingly globalised, these impacts are expected to continue to grow, placing

¹²⁶ Watters, 2023, 69-71

¹²⁷ Greer, 2017, 1-7

¹²⁸ Saunders, 2017

¹²⁹ Watters, 2023, 92-95

¹³⁰ Watters, 2023, 28-37

new demands on legislation, international cooperation and the overall cyber infrastructure in both countries.¹³¹

5.2 The impact of digital crime on the public and everyday life

The digital transformation of organised crime affects not only the economy but also the everyday lives of ordinary citizens in the United States and the United Kingdom. Online fraud, cyber-attacks and digital extortion have become a normal part of modern society, with dire consequences for individuals and entire communities.¹³²

In the US, the number of victims of cybercrime is increasing, with phishing scams, identity theft and ransomware extortion being the most common forms of attack. Many Americans fall victim to fraudulent emails or fake investment offers, which are often linked to organised groups operating outside the US. Digital crime does not only affect individuals - for example, large-scale data leaks from hospitals and government offices can lead to the exploitation of the personal data of millions of people. In addition, smaller companies whose infrastructure is not sufficiently protected can also fall victim to cyber-attacks.¹³³

In the UK, organised crime uses digital tools to target different aspects of people's lives, including online scams targeting the elderly and vulnerable groups. "Romance scams" - scams in which criminals pose as romantic partners and then manipulate victims into sending money - are also becoming increasingly frequent. Another problem is the rise of deepfake technologies that can be used to blackmail or discredit individuals. The British public also faces sophisticated phishing attacks that mimic official institutions such as banks or tax authorities, leading to the theft of personal data or direct monetary loss.¹³⁴

However, the impact of digital crime on everyday life is not only financial. The feeling of constant threat and distrust of digital services can lead to psychological stress and anxiety. People are afraid to use online banking, to shop online or to share personal data, which has long-term consequences for the overall acceptance of digital technologies in society.¹³⁵

The United States and the UK thus face a common challenge - how to protect citizens from organised digital crime without limiting digital services and innovation. With the growing reliance on the online environment, preventing cybercrime is becoming not only a

¹³¹ Watters, 2023, 6-9

¹³² Watters, 2023, 39-41

¹³³ Holt, 2022, 559-560

¹³⁴ Tandana, 2022, 129-132

¹³⁵ Watters, 2023, 105

national security issue, but also an essential element of protecting citizens' rights and privacy.¹³⁶

¹³⁶ Prithwish, 2024, 31-32

6 CURRENT CHALLENGES AND CONSEQUENCES OF DIGITAL CRIME FOR SOCIETY AND SECURITY IN THE US AND THE UK

The impact of organised crime in the digital era on society and security in the two countries analysed - the United States of America and the United Kingdom - cannot be understood as a technical or economic problem alone. Cybercrime has much deeper and more complex implications that reach every layer of society and in many cases directly affect the functioning of the state, the business environment and ordinary citizens.¹³⁷

Both the US and the UK face similar challenges, although the manifestations may differ in some respects due to the specificities of each system. Both countries are experiencing a massive increase in cyber-attacks, which are not just random acts by individuals, but systematic operations led by well-organised groups, often with an international reach. The linking of cybercrime with other forms of organised crime, such as drug trafficking, arms trafficking and money laundering, brings these activities to the level of hybrid threats, where it is difficult to distinguish purely criminal motives from political or ideological objectives.¹³⁸

The security implications are not limited to state institutions or large enterprises. Ordinary citizens are increasingly becoming victims not only of hacking attacks, but also of fraud, extortion and misuse of personal data. Loss of trust in the security of the online environment, fear of surveillance, privacy concerns and the perception that the state is unable to protect citizens adequately are leading to a long-term erosion of trust in democratic institutions. This phenomenon is evident in both societies, and in the US context it is often linked to concerns about the influence of state agencies on privacy, whereas in the UK context the dominant theme is more about financial and consumer risks.¹³⁹

Economic impacts then represent another critical area that exacerbates societal tensions. Small and medium-sized enterprises, often with limited ability to invest in advanced protection, find themselves under pressure and in many cases cease to operate or are forced to rethink their business models. Large companies are investing billions of dollars

¹³⁷ Marsh, 2019, 193-200

¹³⁸ Watters, 2023, 38-41

¹³⁹ Critchley, 2009, 60-61

and pounds in cyber security, yet attacks continue. This creates a climate of insecurity that affects not only the corporate sector, but also employees, investors and consumers.¹⁴⁰

Finally, the transformation of the social structure should also be pointed out. The significant increase in cybercrime is changing value orientations, especially among the younger generation. The access to darknet marketplaces, the possibility to easily obtain illegal income and the natural technological savvy of young people lead to the fact that certain layers of youth are beginning to perceive online crime as "less serious" than traditional crime. At the same time, social cohesion is worsening as less digitally literate populations find themselves in a riskier situation than more technologically literate individuals. This increases inequalities not only between individuals but also between entire regions.¹⁴¹

The above shows that the impact of organised cybercrime cannot be seen as an isolated problem of several sectors. It is a phenomenon that directly affects quality of life, sense of security and stability, not only economically but also socially. Cybersecurity is no longer the domain of technical experts and specialists but is becoming a common topic of public debate and a fundamental aspect of everyday reality. Both the US and the UK will be forced in the coming years not only to look for new protection tools but also to deal with the societal impact of this new form of crime, including changes in education, legislation and protection of vulnerable groups.¹⁴²

6.1.1 Overview of the most significant attacks and their impact

This section will focus on a few key cyber-attacks that have had a significant impact on the economy, public safety and trust in digital infrastructure. These examples demonstrate how organised crime is using technological advances to carry out illicit activities and the long-term consequences for the targeted actors and wider society.

¹⁴⁰ Holt, 2022, 144-145

¹⁴¹ Prithwish, 2024, 9-12

¹⁴² Watters, 2023, 68-71

Table 2 Known attacks

Attack	Type of attack	Year	Target organisation	Impact
Target data breach	Data Theft	2013	Target (USA)	110 million customers affected, over \$300 million in damages
Attack on OPM (Office of Personnel Management)	Data breach	2015	Office of Personnel Management (USA)	21.5 million civil servants' data stolen, a national security risk
Tesco Bank hack	Financial fraud	2016	Tesco Bank (UK)	£2.5 million lost, 9,000 customers affected
WannaCry attack on NHS	Ransomware	2017	NHS (UK)	Over 200,000 systems affected, Thousands of surgeries and medical procedures cancelled
Colonial Pipeline	Ransomware	2021	Colonial Pipeline (USA)	East Coast fuel outage, damage estimated at \$4.4 million
British Library hack	Ransomware	2023	British Library (UK)	Massive data leak, disrupted institution for weeks, impact on research community

(Source: Own elaboration based on ¹⁴³, ¹⁴⁴, ¹⁴⁵, ¹⁴⁶, ¹⁴⁷, ¹⁴⁸)

- Target data leak (2013): this attack showed how easily consumer data can be misused and the significant impact it can have on public trust in online shopping. Data privacy

¹⁴³ Krebs, 2014

¹⁴⁴ U.S. House of Representatives Committee on Oversight and Government Reform, 2016

¹⁴⁵ BBC News, 2016

¹⁴⁶ National Audit Office, 2018

¹⁴⁷ INSURICA, 2024

¹⁴⁸ British Library, 2024

has become a key issue in commerce and e-commerce, leading to stricter cybersecurity and privacy regulations.¹⁴⁹

- Attack on OPM (2015): This incident highlighted not only the vulnerability of government agencies, but also the risk to national security. The attack led to a highly sensitive data leak, which had a direct impact on security policy and caused huge changes in the management and protection of government information.¹⁵⁰
- Tesco Bank hack (2016): This attack on a UK bank highlighted the need for strong protection in the online banking sector, particularly against fraud. Tesco Bank had to deal with a major financial fraud as well as damage to its reputation, leading to greater regulation of the banking sector.¹⁵¹
- WannaCry (2017): WannaCry not only showed how easily ransomware can cripple key institutions but also raised huge public concerns about public health vulnerabilities. This attack had a global reach and highlighted the importance of regular security updates to prevent similar threats.¹⁵²
- Colonial Pipeline (2021): the Colonial Pipeline outage showed how dependent the modern economy is on a stable cyber infrastructure, and how vulnerable energy infrastructure is to cyber threats. This attack had a far-reaching impact on the economy and public safety and led to a rethinking of security standards in the energy sector.¹⁵³
- British Library hack (2023): This attack showed how cybercrime can affect cultural and scientific institutions, with implications for global research and intellectual property protection. The attack on the British Library remains a warning to all institutions managing sensitive information.¹⁵⁴

¹⁴⁹ Krebs, 2014

¹⁵⁰ U.S. House of Representatives Committee on Oversight and Government Reform, 2016

¹⁵¹ BBC News, 2016

¹⁵² National Audit Office, 2018

¹⁵³ INSURICA, 2024

¹⁵⁴ British Library, 2024

6.2 The US and UK Approach to Digital Changes

Organised cybercrime, although initially focused on political, economic or industrial actors, has in recent years begun to make a strong impact on the everyday lives of ordinary people. In many ways, it has changed the way individuals perceive their personal security, finances and private sphere. Whereas cybercrime used to be primarily associated with large-scale hacking attacks on corporations and state institutions, today it is increasingly focused on individuals and their everyday online activities.¹⁵⁵

In recent years, cybercrime has become increasingly personalised. In both the US and the UK, cases are emerging where individuals are facing serious financial losses because of various scams and identity theft. Phishing attacks, malware, ransomware, and digital currency fraud are common and have a direct impact on the everyday lives of ordinary people. Reports of loss of confidential data such as credit card numbers or bank account access details are becoming more frequent, leading to growing concerns about the security of online transactions and communications.¹⁵⁶

An interesting phenomenon is the difference in approach to digital crime between US and UK residents. In the US, the perception of cybercrime is often associated with major scandals and security incidents, such as hacked voting systems or massive leaks of personal data, for example in the cases of the hacking of well-known companies such as Equifax. In contrast, in the UK, people are typically more focused on fraud that directly affects individuals, such as misuse of bank details or online shopping scams. Britons are more familiar with everyday crimes such as phishing, payment fraud and identity theft, which affect not only individuals but also small businesses and non-profit organisations.¹⁵⁷

Another significant difference between the US and the UK lies in the perceived balance between personal freedoms and protection from digital crime. In the US, there has long been debate about surveillance programmes such as PRISM, which allows agencies such as the NSA to monitor online communications. This approach is perceived by some members of the public as a violation of personal rights and privacy. On the other hand, there are controversial laws in the UK that regulate the encryption of communications and oblige service providers to retain communications for investigative purposes. Britons are therefore more willing to accept some loss of freedom in the name of security, which is different from

¹⁵⁵ Greer, 2017, 1-9

¹⁵⁶ Greer, 2017, 1-11

¹⁵⁷ Berghel, 2020

the American approach, where the protection of personal rights has traditionally been put first.¹⁵⁸

Table 3 Differences in Legislation

Country	USA	United Kingdom
Key Legislation	Computer Fraud and Abuse Act (US. 1986) - punishes unauthorized access to computer systems; USA PATRIOT Act (US. 2001) - expands powers to monitor and combat terrorism and organized crime.	Computer Misuse Act (UK. 1990) - UK equivalent of the CFAA; Serious Crime Act (UK. 2015) - targets organised crime and allows for "prevention orders"
Institution	Federal Bureau of Investigation (FBI), Department of Justice (DoJ), Cybersecurity and Infrastructure Security Agency (CISA)	National Crime Agency (NCA), National Cyber Crime Unit (NCCU), Metropolitan Police Cyber Crime Unit.
International cooperation	Active participation in J-CAT, INTERPOL, member of the Budapest Convention (Council of Europe. 2001); cooperation with European and Asian partners	Participation in Europol (EC3), cooperation with USA, Commonwealth countries; signatory to the Budapest Convention (Council of Europe. 2001)
Emphasis on regulation of digital platforms	Rather security and infrastructure orientation (e.g. cooperation with technology companies in CISA)	Increased focus on content regulation and online safety – Online Safety Bill, Data Protection Act (2018).
Rights-based approach vs. repressive tools	Emphasis on national security, often criticized for the scope of surveillance powers.	Attempts to balance between data protection and repression, partly more focused on users' rights

¹⁵⁸ Holt, 2022, 56-58

*(source: Own elaboration based on
US,1986;US,2001;CISA,2024;UK,1990;UK2015;NCA,2024)*

Other negative impacts of organised cybercrime include high unemployment rates in some sectors, especially in IT and technology firms. Some companies in the US and the UK are moving to massive redundancies following cyber-attacks, as they need to focus on ensuring that security incidents are remediated. This trend has led to the labour market in these countries facing a decline in confidence in certain occupational groups, with some firms prioritising investment in security over expanding job roles in other areas.¹⁵⁹

The loss of trust in online systems is also reflected in a decline in user interaction on certain platforms, be it social networking, online banking or shopping platforms. People are becoming more cautious about sharing personal data and increasingly security conscious when using online services. In the UK, these concerns are particularly strong, especially in relation to the use of cryptocurrencies and online finance, which are perceived to be vulnerable to fraud and abuse.¹⁶⁰

Organised cybercrime has far-reaching implications not only for the economy and politics, but also for society itself as it has to cope with these changes. These impacts are not limited to the loss of money or information, but also affect the social fabric, public trust in technology and the way people relate to the online world. Within the US and UK, several key social consequences can be observed as a result of rising digital crime.¹⁶¹

One of the main consequences of cybercrime is the loss of trust in internet services. In both the US and the UK, more and more people are concerned about the security of their online activities. Frequent reports of attacks on large technology companies, data leaks or the proliferation of ransomware attacks have led to the public becoming more cautious in their use of the internet. People are worried about sharing their personal information on social networks, shopping online or conducting banking transactions over the internet.¹⁶²

In the US, this fear is strongly linked to various scandals such as the Equifax hack, which led to huge financial losses for millions of individuals who had their personal data misused. In the UK, on the other hand, it is common to discuss the constant attacks on small

¹⁵⁹ Holt, 2022, 143-148

¹⁶⁰ United Kingdom Government, 2024

¹⁶¹ Prithwish, 2024, 19-20

¹⁶² Prithwish, 2024, 20-22

and medium-sized businesses, resulting in a loss of confidence in online trading and e-commerce.¹⁶³

Organised cybercrime does not only affect the economy or individuals but also has a direct impact on the younger generation who are increasingly involved in online activities. Cyberbullying is one of the most widespread phenomena that is closely linked to digital crime. Many organised criminal groups, particularly in the context of trafficking illegal content on the dark web, are involved in spreading rumours and misusing sensitive information.¹⁶⁴

In the US, as in the UK, more and more schools and universities are facing issues where young people face bullying or abuse through social media. Such incidents can have long-term negative effects on the mental health of victims, and the rise in cyberbullying indicates how organised cybercrime is inseparable from the everyday lives of young people.¹⁶⁵

With cybercrime threats on the rise, many companies, particularly in the technology and IT sectors, are having to focus on higher levels of security, often resulting in layoffs or temporary loss periods. In the US and UK, the nature of work in the IT sector has changed due to increasing cyber-attacks. Companies have been forced to largely shift their investment in securing their systems, meaning that job growth in the technology sector is slower compared to other industries. Although there is a demand for cyber security professionals, some organisations prefer automated solutions or outsourced services rather than investing in wider labour market development.¹⁶⁶

Organised cybercrime is having a particularly strong impact on small businesses, both in the US and the UK. These businesses, which often lack the financial resources to prevent cyber threats, become easy targets for hacker attacks. In the US, there are many cases where small businesses have been hit by ransomware attacks, leading to their financial collapse. Similarly, in the UK, small businesses have been attacked by fraudsters who exploited their weaknesses in data protection. Because of these attacks, small businesses face losses in customer trust and reputation, which in some cases can lead to their shutdown.¹⁶⁷

¹⁶³ Berghel, 2020

¹⁶⁴ Holt, 2022, 334-336

¹⁶⁵ Holt, 2022, 334-336

¹⁶⁶ Prithwish, 2024, 19-20

¹⁶⁷ Holt, 2022, 144-145

6.3 Political and security consequences

Digital crime has become one of the biggest security challenges for governments worldwide. Attacks on government systems, leaks of sensitive data and manipulation of information are changing the dynamics of political decision-making. In many cases, digital crimes are aimed at threatening national security or destabilising political regimes. For example, in the case of attacks on government websites or election data management systems, hacker groups can break into the system and manipulate election results, undermining democratic processes.¹⁶⁸

In some cases, organised crime groups or even states can use cybercrime as a tool to gain political advantage. In the US, for example, there has been extensive debate about foreign interference in electoral processes through cyber-attacks, which has led to the adoption of new security measures and the creation of more advanced protection mechanisms for electoral infrastructure. In the UK, there have been concerns about the potential for misinformation on social media to influence public opinion, which may affect political decision-making and public perception of political parties or candidates.¹⁶⁹

Cybercrime has a direct impact on elections and political processes in many countries where electoral systems and processes are under threat. In the US, there were significant cyber-attacks on electoral infrastructure during the 2016 presidential election, with reports of attacks designed to obtain sensitive voter data and manipulate election results. One of the most notorious cases was the attack on the Democratic Party's servers, which led to the leak of emails and other internal information that affected the electoral process and public perception. This incident led to accusations of Russian interference and the creation of new rules to protect US election infrastructure.¹⁷⁰

In the UK, the impact of cybercrime on elections and public opinion has also been noticeable, particularly in the context of the referendum on Britain's withdrawal from the European Union (Brexit). Massive manipulation of information through social media and illegal data analysis has been identified. The manipulation of public opinion through unverified information and misinformation has created considerable polarisation and influenced voter decision-making. As a result, the UK authorities have introduced new

¹⁶⁸ Prithwish, 2024, 4-6

¹⁶⁹ McFaul, 2019, 5-8

¹⁷⁰ McFaul, 2019, 8-13

regulatory mechanisms to ensure the transparency and integrity of political campaigns on the internet.¹⁷¹

Digital platforms also play a key role in the financing of illicit activities, including organised crime and terrorism. Organised criminal groups and terrorist organisations use the anonymity offered by the internet to finance their activities. Cryptocurrencies, the dark web and other digital infrastructure enable rapid and illegal transactions that are beyond the reach of traditional financial controls.¹⁷²

For example, in the case of terrorist organisations such as ISIS, digital platforms have been used to raise funds through online donations, the sale of illegal goods or even through ransom collection. Similarly, organised criminal groups have used online systems to launder money, trade in drugs, weapons and other illegal commodities. This new form of financing criminal activities is efficient, difficult to monitor and contributes to the continued destabilisation of society at a global level.¹⁷³

A comparison of the approach to cyber security protection in the US and the UK shows the different strategies and structures that have been developed in response to the growing threat of digital crime. In the US, cybersecurity protection is coordinated primarily through the Department of Homeland Security (DHS), which is responsible for protecting critical infrastructure and is also concerned with preventing cyber-attacks. DHS focuses on protecting federal systems and works with various government and private organizations to develop and implement cybersecurity policies.¹⁷⁴

In the UK, the National Cyber Security Centre (NCSC), part of Government Communications Headquarters (GCHQ), is responsible for cyber security. The NCSC is responsible not only for protecting government and public systems, but also for providing support and advice to the private sector. The UK's cyber security strategy is built on collaboration between government, the private sector and the public to improve risk awareness and prevent cyber-attacks on the general public.^{175, 176}

Although both countries have developed strong security structures, there are differences in approach and methods of protection. The US focuses more on protecting critical

¹⁷¹ Oliver, 2013, 5-11

¹⁷² Prithwish, 2024, 7-8

¹⁷³ Holt, 2022, 334-336

¹⁷⁴ United States Department of Homeland Security, 2025

¹⁷⁵ Government Communications Headquarters, 2025

¹⁷⁶ National Cyber Security Centre, 2025

infrastructure and national interests, while the UK emphasises broad collaboration with industry and the public to respond more quickly to cyber threats.¹⁷⁷

6.4 The Dark Web and Anonymous Finance, Impacts on Society

The Dark Web, a part of the Internet not indexed by conventional search engines, is known for its high degree of anonymity and encryption. This anonymity provides ideal conditions for various illegal activities, including organised crime. In recent years, not only has the amount of criminal activity on the dark web expanded but so has its impact on wider society. Both the US and the UK are facing an increasing number of cybercrimes associated with this dark corner of the internet, and their responses to this problem are becoming highly relevant.¹⁷⁸

In the US and the UK, the dark web is considered an extremely dangerous space where criminal organisations and individuals trading in illegal goods, including drugs, weapons, stolen data or even human beings, can operate. In response to this threat, both countries have highly sophisticated strategies to combat illegal activities on the dark web, focusing on different aspects:

- The US focuses on international cooperation between agencies such as the FBI, DEA and DHS (Department of Homeland Security). US authorities also use sophisticated surveillance technologies to identify and prosecute illicit markets. The most famous example is Operation DisrupTor, which focused on dismantling the largest marketplaces on the dark web, including Silk Road, the most notorious dark web marketplace for drug sales.¹⁷⁹
- The UK is focused on ensuring the safety of citizens through the National Cyber Security Centre (NCSC), which works with the European Union and other international organisations to monitor and detect illegal activity on the dark web. Within UK legislation, there is an emphasis on cybersecurity and encryption principles, with the NCSC focusing on working with the private sector and ISPs to remove content associated with illegal activities. UK authorities are also taking

¹⁷⁷ United States Digital Service, 2024

¹⁷⁸ Prithwish, 2024, 5-11

¹⁷⁹ Kulm, 2020, 11

advantage of the development of innovative technology and securing its application against anonymous transactions on the dark web.¹⁸⁰

Cryptocurrencies, in particular Bitcoin, Ethereum and other altcoins, have become key tools for financing illegal activities on the dark web. Their anonymity and decentralised nature make transactions difficult to trace, which attracts organised crime and individuals involved in cybercrime.¹⁸¹

- In the US, cryptocurrency has been intensively scrutinised in recent years in connection with money laundering and the financing of illegal activities. US regulators such as the Financial Crimes Enforcement Network (FinCEN) are targeting cryptocurrency exchanges and platforms that allow anonymous trading and exchange. In addition, legislation has been passed to regulate cryptocurrencies, requiring companies to record transactions and identify customers when trading cryptocurrencies.¹⁸²
- In the UK, cryptocurrencies are becoming an increasingly high-profile topic. The UK government has moved to create a legislative framework for the regulation of cryptocurrencies and blockchain. HMRC (Her Majesty's Revenue and Customs) encourages British citizens to declare their cryptocurrency income and uses advanced analytical tools to search for illegal transactions. Privacy and cryptocurrency encryption protocols allow organised criminals to conduct transactions in drugs, weapons and other illegal products without being tracked.¹⁸³

6.4.1 Case studies (Silk Road in the US vs. UK cryptocurrency scams)

One of the most famous cases related to the dark web and cryptocurrencies is Silk Road, a dark web marketplace used to sell illegal drugs and weapons. This market was shut down by the FBI in 2013, but it showed how easily organized groups can exploit the anonymity of the internet to fund criminal activity. Silk Road is an example of how cryptocurrencies serve as a means of payment for illegal activities, which has led to a global push for regulation and controls on cryptocurrency transactions. In response to this threat, U.S. governments have

¹⁸⁰ Commonwealth Secretariat, 2025, 31-36

¹⁸¹ Prithwish, 2024, 9-11

¹⁸² Greer, 2017, 1-7

¹⁸³ His Majesty's Revenue and Customs, 2025

begun to push for greater transparency in cryptocurrency markets and in 2015 introduced new laws aimed at preventing money laundering through cryptocurrencies.^{184 185}

In the UK, examples of cryptocurrency fraud are growing, particularly in the area of "pump and dump" schemes, where criminal groups manipulate the value of cryptocurrencies to deceive investors. In 2020, several scandals were uncovered where UK fraudsters used cryptocurrencies to raise funds for the illegal drug trade. These developments have led the UK government to introduce stricter regulatory measures for cryptocurrency exchanges and more pressure on anonymous transactions.^{186 187}

The Dark Web provides criminal groups with an opportunity to increase the effectiveness and anonymity of their illegal activities. Criminals can not only sell goods on the dark web, but also provide services such as hacking for hire, trading stolen data or extortion through ransomware. This means that criminals are able to globalize and operate in secrecy, making it difficult for traditional forms of policing to combat these activities.¹⁸⁸

For ordinary citizens, this means a constant risk associated with sensitive data leaks, identity theft, or loss of funds through fraud, ransomware attacks, etc. Unlike traditional forms of crime, the dark web does not just target specific geographic areas - it can affect anyone in the world, increasing its danger and global impact.¹⁸⁹

Another challenging issue is the ever-improving technology of hackers who are improving their skills thanks to the anonymity of the dark web. By remaining anonymous and using cryptocurrencies for their transactions, criminal groups can continue their activities without being exposed to direct interference. This change in behaviour means that today's organised crime is increasingly tech-savvy, with major implications for public safety and trust in the online environment.¹⁹⁰

The case studies were selected based on several key criteria that reflect the main objective of this thesis, namely, to analyse and compare the specific manifestations of organised crime in the digital environment in two Anglo-Saxon countries. The first criterion was direct relevance to the topic of digital organised crime. The two chosen studies, i.e. the

¹⁸⁴ Holt, 2022, 462-465

¹⁸⁵ U.S. Commodity Futures Trading Commission, 2015

¹⁸⁶ Holt, 2022, 744

¹⁸⁷ The Guardian, 2024

¹⁸⁸ Prithwish, 2024, 6-9 9-11,19-22

¹⁸⁹ Prithwish, 2024, 9-11,19-22

¹⁹⁰ Holt, 2022, 460-465

Silk Road case in the USA and the cryptocurrency fraud cases in the UK, are directly related to the use of digital technologies to commit organised crime.¹⁹¹

The second important consideration was geographical balance. By including the United States and the United Kingdom, it is possible to compare two different approaches within the Anglo-Saxon legal and cultural tradition. The third criterion was the significance and impact of the cases on society, as both cases not only significantly influenced the perception of cybercrime but also contributed to legislative changes and influenced the attitudes of security forces.¹⁹²

The last aspect was the diversity of methods of organised crime. The Silk Road case presents a complex marketplace for illegal trade on the dark web, while the UK cryptocurrency scams illustrate sophisticated financial machinations in the digital environment.¹⁹³

Thus, the selection of these two case studies allows not only for a detailed analysis of different forms of digital organised crime, but also a comparison of institutional responses, the level of public awareness of these phenomena and the effectiveness of law enforcement.

6.5 Legal and ethical implications of the fight against digital crime

Digital crime, especially organised and internationally connected crime, poses not only security and economic threats, but also legal and ethical dilemmas. While states seek to protect their citizens and infrastructures, they must also balance issues of protecting human rights, privacy, and freedoms. In this context, the United States and the United Kingdom represent two examples of different, yet partly similar, approaches to the issue.¹⁹⁴

- Privacy vs. security measures (US - surveillance programs, UK - encryption ban)^{195, 196}
- One of the most debated topics in digital security is the balance between privacy and security.

¹⁹¹ Holt, 2022, 462-465

¹⁹² Prithwish, 2024, 19-22

¹⁹³ Holt, 2022, 462-465

¹⁹⁴ Prithwish, 2024, 19-22

¹⁹⁵ Wired, 2016

¹⁹⁶ United Kingdom Government, 2016

- The US has become a symbol of large-scale surveillance programmes after the events of 11 September 2001 and especially after Edward Snowden's revelations in 2013. The NSA and other authorities have gained access to the private data of millions of Internet users, even without any direct suspicion of criminal activity. This approach has sparked a heated debate about the ethical limits of government surveillance, with many arguing that excessive surveillance undermines fundamental rights and citizens' trust in the rule of law.^{197, 198}
- The UK has focused on regulating encryption technologies as part of its approach to digital security. Following several terrorist attacks and increasing crime associated with the use of encrypted communications, the UK government has considered introducing an obligation for service providers to decrypt communications on request from the authorities. While a blanket ban on encryption has not occurred, pressure to restrict end-to-end encryption remains. However, this approach has been criticised as a risk to the privacy and security of ordinary users.^{199, 200}

Cybercrime reduces citizens' trust in the rule of law and its ability to protect their rights and security. Cases where millions of people are harmed by data leaks or fraud and state institutions are unable to bring the culprits to justice undermine public trust. The loss of sensitive information, the ineffectiveness in dealing with ransomware groups or the inability to prevent attacks on infrastructure create an atmosphere of insecurity and frustration.²⁰¹

In addition, the increasing digitalisation of everyday life means that citizens are increasingly dependent on the online environment and thus more vulnerable. If the state fails to react quickly enough to threats, the scope for cybercriminals grows, while citizens' faith in the effectiveness of state institutions declines. In the long term, this may have serious negative effects on social cohesion and respect for the law.²⁰²

Organised digital crime is inherently global. Hacker groups and organised gangs operate across borders, exploiting the anonymity of the internet and international legal loopholes. This requires active international cooperation. The FBI plays a key role in combating cybercrime not only in the U.S., but also internationally. It works with other

¹⁹⁷ The Guardian, 2013

¹⁹⁸ PBS, 2015

¹⁹⁹ United Kingdom Government, 2016

²⁰⁰ Wired, 2016

²⁰¹ Prithwish, 2024, 19-20

²⁰² Prithwish, 2024, 22-27

agencies in so-called "Joint Cybercrime Task Forces" to help disrupt global cybercriminal networks. The US also uses its diplomatic position to pressure technology companies and states that provide safe havens for cybercriminals.²⁰³

Europol and its European Cybercrime Centre (EC3) are the main European actor in this area. Europol coordinates operations against the dark web, ransomware groups and cryptocurrency fraud. Europol often cooperates not only with EU Member States, but also with the United States, Canada, and other non-EU partners.²⁰⁴

Interpol provides an international platform for sharing information and coordinating operations in the fight against digital crime. It places particular emphasis on capacity building in developing countries and strengthening the cyber capabilities of national police forces. Joint operations, such as 'Operation Disruptor' against the dark web or international crackdowns on ransomware gangs, demonstrate that cooperation between the US, UK, EU, and other states is key to tackling the threats posed by digital crime.²⁰⁵

Going forward, it will be crucial to strike a balance between effectively fighting cybercrime and protecting fundamental rights, including the right to privacy. Society will have to face dilemmas such as-to what extent can governments monitor their citizens, where does the right to security end and the right to privacy begin, or if encryption is a right or a security risk.²⁰⁶

Both countries, the US, and the UK, will have to adapt legislation to the dynamic evolution of cybercrime and technology in the coming years. The key question will remain whether countries will be able to adapt their legal systems to preserve democratic values while protecting citizens from growing digital threats.²⁰⁷

6.5.1 Future developments and predictions

The evolution of digital organised crime and state defence mechanisms will be influenced by a number of factors in the coming years, in particular technological advances, and changes in the global security environment. The US and the UK, as key actors in the cybersecurity field, will face similar but also specific challenges.²⁰⁸

²⁰³ Prithwish, 2024, 31-34

²⁰⁴ Prithwish, 2024, 35

²⁰⁵ Prithwish, 2024, 22

²⁰⁶ Prithwish, 2024, 22-24

²⁰⁷ Prithwish, 2024, 22-24

²⁰⁸ Prithwish, 2024, 41-44

In the near and more distant future, digital crime can be expected to continue to grow, not only in volume but also in sophistication. Organised crime groups are likely to focus on several key areas in the future. Key threats include targeted attacks on critical infrastructure such as energy grids, healthcare facilities or transport systems, which can be used to blackmail or destabilise the social order. Another risk is the misuse of artificial intelligence to create disinformation, deepfake videos and voice spoofing. These technologies can have a major impact not only on the financial sector, but also on political discourse and overall security.²⁰⁹

Criminals will continue to increasingly exploit the connections between the physical and digital worlds. For example, they may target Internet of Things (IoT) devices, autonomous systems, or smart city infrastructures, putting public services and individual privacy at risk. Specifically in the US, attacks targeting critical infrastructure and the financial sector are expected to increase due to the scale and globalisation of the US economy. The UK, on the other hand, will have to deal with increasing cybercrime in the financial services sector and the problems associated with the manipulation of public opinion and hybrid threats.²¹⁰

The development of artificial intelligence and machine learning will bring new opportunities not only for security forces, but also for perpetrators. Criminal groups will be able to automate attacks, create highly personalised phishing campaigns, and develop more effective ransomware. In addition, the use of cryptocurrencies and decentralised financial systems, which allow anonymous transactions and are difficult to regulate, will remain a challenge. Quantum computers, whose computing capabilities could break today's encryption algorithms, will also be a major factor in the future. If this happens, the current security architecture will change fundamentally and new ways of protecting data will have to be found.²¹¹

On the other hand, security forces will have more advanced tools to detect cybercrime networks, analyse data, predict behaviour, and monitor financial flows. As attacks become more frequent and have a real impact on everyday life, it is to be expected that society will begin to place more emphasis on cybersecurity. This will be reflected both at an individual level, for example in efforts to better secure home devices and raise awareness of online

²⁰⁹ Prithwish, 2024, 41-44

²¹⁰ Prithwish, 2024, 29,42

²¹¹ Prithwish, 2024, 36-38

threats, and at a governmental level, where the focus will be on legislation and preventive measures.²¹²

There may be significant changes in the approach to digital security compared to today. Citizens may be more willing to accept certain privacy restrictions in exchange for a higher level of security. If state institutions prove effective in combating cyber threats, public confidence in their capabilities may also increase. At the same time, however, there will be a growing need to address ethical and legal issues around privacy and digital rights, especially if governments are forced to deploy more invasive surveillance and control tools.²¹³

Overall, cybercrime will become a key security issue in the future. It will no longer just be an area of interest for digital security experts, but a broad societal challenge that will affect the daily lives of people around the world.

²¹² Prithwish, 2024, 43-44

²¹³ Prithwish, 2024, 39-41

7 SUMMARY OF THE COMPARATIVE ANALYSIS OF THE UNITED STATES AND THE UNITED KINGDOM

The following table presents a summary of the key differences between the United States and United Kingdom approaches to the issue of digital organised crime. It focuses on the legislative framework, institutional arrangements, access to cryptocurrencies, levels of surveillance and technological response. The aim is to highlight the country specificities and to help facilitate the overall comparison.²¹⁴

Table 4 Comparison of practical approaches to digital organised crime in USA and UK

Country	USA	United Kingdom (UK)
Legal framework	Federal legislation (e.g. Computer Fraud and Abuse Act, PATRIOT Act)	National laws (e.g. Computer Misuse Act 1990, Serious Crime Act 2015)
Focus of legislation	Primarily on protection of national security, prevention of terrorism, cyber defence	Emphasis on balance between security and civil liberties, data protection
Key institutions	FBI Cyber Division, NSA, CISA, DHS	NCA (National Crime Agency), NCSC, GCHQ
Management structure	Centralised federal management, strong position of national agencies	Multi-level approach: cooperation between agencies, police and private sector
Surveillance and monitoring	Extensive surveillance programs (e.g. PRISM after Edward Snowden's revelations)	More limited monitoring, but efforts to legislate approach to decryption of communications

²¹⁴ Prithwish, 2024,

Encryption and technology	Repeated efforts to force backdoors into devices and applications	Discussion of legal obligation to disclose encrypted communications
Reaction to cryptocurrencies	Already in 2015 laws to combat money laundering through cryptocurrencies	Reaction rather reactive - e.g. after the crypto drug financing scandals (2020)
Approach to crypto	Strict regulation, increased oversight by SEC, FinCEN	More flexible approach, but trying to catch up with regulations (especially after cryptocurrency abuse by fraudsters)
Criminal policy	Tougher sentences, frequent use of conspiracy and terrorist financing laws	More lenient sentences, more use of restorative justice and preventive approaches
Involvement of the private sector	Cooperation, but also coercive demands on technology companies (Google, Apple, Amazon)	Rather a partnership approach - sharing threats and recommendations, appeal to ethical standards
Prevention and education	Cyber literacy programmes within CISA and school initiatives	Active education campaigns led by NCSC and school institutions
Coping with Emerging Threats (AI)	Investing in research to defend against AI misuse in cybercrime through NSA and DARPA	NCSC highlights AI risks and calls for common European cybersecurity standards
International cooperation	Active membership of groups such as Five Eyes, often dominant position	Commonwealth cooperation, Council of Europe, approach balances security and sovereignty

Approach to change	in the US environment responds more quickly legislatively, often strictly	The UK has a more cautious legislative approach, more consultation and impact assessment
Ethical framework	Greater emphasis on national security over privacy, especially after 9/11	Stronger emphasis on privacy, public discussion of limits of government control
Transparency	Many programmes (e.g. surveillance) secret, only made public by whistleblowers	Greater transparency and parliamentary scrutiny of surveillance programmes

(source: Own elaboration based on
US,1986;US,2001;CISA,2024;UK,1990;UK2015;NCA,2024,^{215, 216, 217, 218, 219, 220})

²¹⁵ Krebs, 2014

²¹⁶ U.S. House of Representatives Committee on Oversight and Government Reform, 2016

²¹⁷ BBC News. 2016

²¹⁸ National Audit Office, 2018

²¹⁹ INSURICA, 2024

²²⁰ British Library, 2024

CONCLUSION

This thesis aimed to analyse how digitisation and the advent of artificial intelligence have affected organised crime in Anglo-Saxon countries, specifically the United States and the United Kingdom. Based on the theoretical and practical part, it can be concluded that this objective has been fulfilled. The analysis showed that the digitalisation of organized crime is not only a matter of technological change but has profound social and structural implications. Cybercrime, increasingly linked to traditional forms of crime, is fundamentally changing the way states view their security strategies, their legal frameworks and their institutional responses.

Organized criminal groups now have more flexible and effective tools to operate on a global scale. In addition to hacking, fraud and extortion, they use means such as cryptocurrencies, anonymous communication channels and the dark web. The impact of AI is still in its infancy, but it already suggests the potential to fundamentally transform methods of operations – both by criminals and security forces.

Comparisons between the United States and the United Kingdom have shown that, although both countries face similar emerging challenges, their approaches to addressing the issues are partly different. However, they both share the necessity to continuously adapt to a rapidly changing environment and an emphasis on international cooperation, both between government institutions and in collaboration with the technology and academic sectors.

As a result, digitalisation and new technologies are not only affecting the nature of crime itself, but also the structure of societies and the security policies of states. Organized crime in the digital era is a fluid and highly adaptive phenomenon that requires innovative, flexible and legally anchored response. Going forward, it will be crucial to develop prevention tools, strengthen cyber security, and at the same time pay attention to the legal and ethical aspects of the use of these new technologies in the fight against organized crime.

BIBLIOGRAPHY

- Afilipoaie, Adina, and Patrick Shortis. 2018. *Crypto-market Enforcement: New Strategy and Tactics*. Policy, 54: 87–98.
- Albanese, Jay S. 2015. *Organized Crime in Our Times*. 6th ed. Oxon: Routledge.
- Bartlett, Jamie. 2014. *The Dark Net: Inside the Digital Underworld*. Brooklyn: Melville House
- BBC News. 2016. *Tesco Bank attack: What happened and what it means for you*. London: BBC. Available at: <https://www.bbc.com/news/business-37891742>
- Berghel, H. 2020. The equifax hack revisited and repurposed. *Computer*, 53(5), 85.
- British Library. 2024. *Learning Lessons from the Cyber-Attack: British Library Cyber Incident Review*. London: British Library. Available at: <https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf>
- Commonwealth Secretariat. 2025. *Commonwealth Cyber Journal: Volume 3*. Available at: <https://thecommonwealth.org/publications/commonwealth-cyber-journal-volume-3>
- Council of Europe. 2001. *Convention on Cybercrime (Budapest Convention)*. ETS No. 185.
- Cybersecurity and Infrastructure Security Agency (CISA). 2024. *About CISA*. [online]. Available at: <https://www.cisa.gov/>
- Dickie, John. 2004. *Cosa Nostra: a history of the Sicilian Mafia*. New York, Palgrave, Macmillan,
- Eckerson, Wayne W. 2007. *Predictive Analytics: Extending the Value of Your Data Warehousing Investment*. TDWI Best Practices Report, 1: 1–36.
- Gadde, Hari. 2021. *AI-Driven Predictive Maintenance in Relational Database Systems*. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 12(1): 386–409.
- Ganguli, Prithwish. 2024. *The Rise of Cybercrime-as-a-Service: Implications and Countermeasures*. Heritage Group of Institutions.
- Government Communications Headquarters. 2025. *About Us*. Available at: <https://www.gchq.gov.uk/hom>
- Greer, B. 2017. *The Growth of Cybercrime in the United States*. Unpublished academic paper, Utica College.
- His Majesty's Revenue and Customs. 2025. *About HMRC*. [online]. Available at: <https://www.gov.uk/government/organisations/hm-revenue-customs>

- Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. 2022. *Cybercrime and Digital Forensics: An Introduction*. 3rd ed. Oxon: Routledge.
- INSURICA. 2024. *Cyber Case Study: Colonial Pipeline Ransomware Attack*. Available at: <https://insurica.com/blog/colonial-pipeline-ransomware-attack/>
- KAPLAN, D. E., & DUBRO, A. 2012. *Yakuza: Japan's Criminal Underworld*, University of California Press.
- Krebs, Brian. 2014. *The Target Breach, By the Numbers*. KrebsOnSecurity. Available at: <https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/>
- Kulm, A. 2020. *A Framework for Identifying Host-Based Artifacts in Dark Web Investigations*. Master's Thesis, Dakota State University.
- Marsh, Ian, and Gaynor Melville. 2019. *Crime, Justice and the Media*. 3rd ed. New York: Routledge.
- McFaul, M., & Kass, B. 2019. Understanding Putin's intentions and actions in the 2016 US presidential election. *Securing American Elections*, 1.
- Montel, Laurence. 2010. Critchley David, *The Origin of Organized Crime in America. The New York City Mafia (1891-1931)*: New York, London, Routledge.
- National Audit Office. 2018. *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office. Available at: <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/>
- National Crime Agency. 2024. *National Cyber Crime Unit*. [online]. Available at: <https://www.nationalcrimeagency.gov.uk/>
- National Cyber Security Centre. 2025. *About Us*. Available at: <https://www.ncsc.gov.uk/section/about-ncsc>
- Oerlemans, J.J., and van Toor, D.A.G. 2022. Legal Aspects of the EncroChat Operation: A Human Rights Perspective. *European Journal of Crime, Criminal Law and Criminal Justice*
- Oliver, T. L. 2013. Europe without Britain: assessing the impact on the European Union of a British withdrawal.
- Paul Dettmann. 2024. *British Gangs From 1900 to 1950*. Great Britain, Pen & Sword True Crime
- PBS. 2015. *How the NSA Spying Programs Have Changed Since Snowden*. Public Broadcasting Service. Available at: <https://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden/>

- Saunders, J. 2017. Tackling cybercrime – the UK response, *Journal of Cyber Policy*, 2(1), pp. 4–15.
- Shelley, Louise. 2018. *Dark Commerce: How a New Illicit Economy Is Threatening Our Future*. Princeton, NJ: Princeton University Press.
- Sifakis, Carl. 1987. *The Mafia Encyclopedia*. New York, N.Y.: Facts on File.
- Tandana, E. A. 2022 AMID THE THREAT OF CYBERCRIME, *QUAERENS: Journal of Theology and Christianity Studies*, 4(2), pp. 129-147
- The Guardian. 2013. *NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained*. Guardian News & Media. Available at: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>
- The Guardian. 2024. *Global investigation exposes alleged billion-dollar Russian money-laundering network*. Guardian News & Media. Available at: <https://www.theguardian.com/business/2024/dec/04/global-investigation-exposes-alleged-billion-dollar-russian-money-laundering-network>
- U.S. Commodity Futures Trading Commission. 2015. *CFTC Staff Issues Advisory for Virtual Currency Products*. Commodity Futures Trading Commission. Available at: <https://www.cftc.gov/PressRoom/PressReleases/7731-18>
- U.S. House of Representatives Committee on Oversight and Government Reform. 2016. *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*. Washington, D.C.: U.S. Government. Available at: <https://oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/>
- United Kingdom Government. 2016. *Encryption and Counter-Terrorism: Getting the Balance Right*. HM Government. Available at: <https://www.gov.uk/government/speeches/encryption-and-counter-terrorism-getting-the-balance-right>
- United Kingdom Government. 2024. *Digital Development Strategy 2024 to 2030*. Available at: <https://www.gov.uk/government/publications/digital-development-strategy-2024-to-2030>
- United Kingdom. 1990. *Computer Misuse Act 1990*. London: The Stationery Office.
- United Kingdom. 2015. *Serious Crime Act 2015*. London: The Stationery Office.
- United States Department of Homeland Security. 2025. *About DHS*. Available at: <https://www.dhs.gov/about-dhs>

- United States Digital Service. 2024. *USDS Impact Report 2024*. Available at: <https://www.usds.gov/resources/USDS-2024-Impact-Report.pdf>
- United States General Services Administration. 2024. *Digital Government Strategy*. Available at: <https://www.gsa.gov/technology/government-it-initiatives/digital-strategy>
- United States. 1986. *Computer Fraud and Abuse Act*, 18 U.S.C. § 1030.
- United States. 2001. *USA PATRIOT Act. Public Law 107–56*. Washington, D.C.: U.S. Congress.
- Watters, P. A. 2023. *Cybercrime and cybersecurity*. 1st ed. CRC Press.
- Westerlund, Mikael. 2019. *The Emergence of Deepfake Technology: A Review*. Technology Innovation Management Review, 9(11): 40–53.
- Wired. 2016. *Government Plans to Make Tech Firms Hand Over Encrypted Messages*. Condé Nast. Available at: <https://www.wired.com/story/uk-government-encryption-snoopers-charter/>

LIST OF FIGURES

LIST OF TABLES

Table 1 Forms of crime	21
Table 2 Known attacks.....	47
Table 3 Differences in Legislation.....	50
Table 4 Comparison of practical approaches to digital organised crime in USA and UK ..	63

LIST OF ABBREVIATIONS

VPN Virtual private network

DDoS Distributed

CaaS Crime as a Service

AI Artificial Intelligence

ID Identification

DEX Decentralised exchanges

GDPR General Data Protection Regulation

Prism Product Safety Risk Assessment Methodology

ISP Internet service provider

APPENDICES

APPENDIX P I: FIRST APPENDIX TITLE