Review Article
Volume 15:03, 2024

Journal of Forensic Research

ISSN: 2157-7145 Open Access

Anticipating Future Crimes: The Role of Forensics in Addressing Emerging Threats in the Next Decades of the 21st Century

Pavan Kumar Ganechary[1]* and Kollam Anjali[2]

[1]*Laboratory of Biology and Biotechnology, National Forensic Sciences University, Gandhinagar, Gujarat, India*
[2]*Laboratory of Fingerprints and Questioned Documents, National Forensic Sciences University, Delhi Campus, India*

Abstract

In the rapidly evolving world of crime, it is crucial for all the law enforcement agencies to stay at least one step ahead of criminals as rapid advancement of technology and societal changes have created a dynamic landscape for criminal activities. Forensic science has come a long way in recent years by taking small baby steps, thanks to advancements in technology and aptly supported by research. By analysing all kinds of evidence left at crime scenes, forensic experts can provide valuable insights into criminal behaviour patterns and potential modus operandi and furthermore this collected data allows law enforcement agencies to allocate resources effectively and proactively combat crime but with the rise of cybercrime and other technologically-driven offenses, traditional investigative methods alone are insufficient. Forensic experts specializing in latest forensic technologies are the need of the hour who can help uncover hidden traces left behind by cybercriminals, enabling authorities to prevent future attacks.

By investing both time and resources heavily in research and development on anticipating future crimes and equipping law enforcement agencies with cutting-edge forensic tools and techniques, society can better protect its citizens from emerging threats. The role of forensics cannot be understated in any way - it is an essential component in maintaining public safety as we navigate an increasingly complex world. Anticipating future crimes and addressing emerging threats is a daunting task, but one that can be achieved with the help of the latest technologies like advanced machine learning, artificial intelligence and incorporating forensics as a core in these. As we enter the next decades of the 21st century, it is imperative that we recognize the pivotal role forensics plays in ensuring public safety. This review article explores the various types of crimes that may emerge in the next decades of the 21st century, driven by technological, social, and economic factors and also investigates how forensic science and technology can possibly address these emerging threats and ensure effective crime prevention, investigation, and justice.

Keywords: Forensic science • Future of forensic science • Forensic investigation

Abbreviations: ACSC: Australian Cyber Security Centre; AI: Artificial Intelligence; APWG: Anti-Phishing Working Group; BEC: Business Email Compromise; DDoS: Distributed Denial of Service; DNA: Deoxyribonucleic Acid; EAC: Email Account Compromise; EC3: European Cybercrime Centre; EU: European Union; FATF: Financial Action Task Force; FBI: Federal Bureau of Investigation; FTC: Federal Trade Commission; GDPR: General Data Protection Regulation; GIS: Geographic Information System; IC3: Internet Crime Complaint Center; ICO: Initial Coin Offerings; NIST: National Institute of Standards and Technology; PCR: Polymerase Chain Reaction; RBI: Reserve Bank of India

Introduction

Overview of the changing landscape of crime in the 21st century

Over the last century or so the world has witnessed significant changes in the crime landscape, with new forms of criminal activities emerging and traditional crimes adapting to the advancements in technology and globalisation. One of the most notable changes is the rise of cybercrime fuelled by the rapid growth of internet usage, criminals have found new avenues to exploit individuals, businesses, and governments [1]. Cybercrimes include hacking, identity theft, online fraud, and data breaches and these offences have become increasingly sophisticated, posing significant challenges for law enforcement agencies worldwide [2]. Moreover, globalisation has facilitated transnational organised crime as criminal networks now operate across borders with ease, engaging in activities such as drug trafficking, human smuggling, money laundering, and terrorism. The interconnectedness of economies and societies has made it difficult for individual nations to combat such types of modern crimes effectively.

Additionally, there has been a shift towards white-collar crimes in recent years. Corporate frauds and financial scams have become more prevalent as individuals seek illicit gains through manipulation of financial systems or exploitation of loopholes in regulations. Furthermore, societal changes have also influenced crime patterns such as the increasing inequality gap has led to higher rates of property crimes such as theft and burglary. Social unrest caused by political instability or economic downturns can also contribute to an upsurge in violent crimes like riots, moblynching or protests turning violent.

To put it in a nutshell the world has seen a significant transformation in the crime landscape due to technological advancements, globalization effects on organised crime networks, rise in white-collar offenses as well as societal factors influencing criminal behaviour. Understanding these changes is crucial for policymakers and law enforcement agencies if they are to effectively address these emerging challenges and ensure public safety in this rapidly evolving world.

***Address for Correspondence:** Pavan Kumar Ganechary, Laboratory of Biology and Biotechnology, National Forensic Sciences University, Gandhinagar, Gujarat, India, E-mail: pavanganechary@gmail.com*

***Copyright:** © 2024 Ganechary PK, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original author and source are credited.*

Received: 05 February, 2024, Manuscript No. jfr-24-126926; **Editor Assigned:** 07 February, 2024, PreQC No. P-126926; **Reviewed:** 17 May, 2024, QC No. Q-126926; **Revised:** 24 May, 2024, Manuscript No. R-126926; **Published:** 31 May, 2024, DOI: 10.37421/2157-7145.2024.15.615

Importance of anticipating future crimes for law enforcement and policymakers

By identifying potential threats and developing proactive strategies, law enforcement agencies can effectively combat crime and ensure public safety. Anticipating future crimes allows law enforcement agencies to allocate resources more efficiently by analysing patterns and trends, and authorities can identify high-risk areas or individuals that require increased attention. This targeted approach not only helps prevent crimes but also maximises the impact of limited resources. Furthermore, anticipating future crimes enables policymakers to create effective legislation and policies. By understanding emerging criminal activities, lawmakers can draft laws that address new challenges and close existing loopholes as well as this proactive approach ensures that the legal framework remains relevant in a rapidly changing society.

Moreover, anticipating future crimes promotes innovation in law enforcement techniques as criminals adapt their methods, authorities must constantly evolve to keep up with them. By staying ahead of the curve, law enforcement agencies can develop cutting-edge technologies and strategies to combat crime effectively, while at the onset this approach looks interesting but it is to be kept in mind that anticipating future crimes does not without its challenges. It requires a comprehensive understanding of criminal behaviour, access to accurate data analysis tools, and collaboration between various stakeholders such as intelligence agencies, academia, and technology experts. Hence, anticipating future crimes is vital for both law enforcement agencies and policymakers.

The role of forensic science in tackling evolving criminal activities

Forensic science has always played a crucial role in the investigation and resolution of criminal activities. But, as criminals become more sophisticated and adopt new techniques, forensic science must evolve to keep up with these challenges. With the rapid advancement of technology and the widespread usage of the internet, criminals are finding new ways to exploit vulnerabilities in digital systems. In the next decade, we can expect to see an increase in complex cybercrimes related to identity theft, online fraud and other ransomware attacks and it is one of the emerging criminal activities that forensic science will have to tackle is cybercrime. Forensic scientists will need to develop expertise in digital forensics to trace and analyse evidence left behind by fraudsters/scammers/ hackers or online criminals such as rapidly examining computer systems, networks, and mobile devices for traces of illegal activities.

At the same time, Deoxyribonucleic Acid (DNA) - which carries all the genetic information in living cells and is individual, DNA analysis will continue to play a vital role in solving crimes. However, as criminals become more and more aware of DNA as an gold standard evidence and take precautions to avoid detection, forensic scientists must adapt their methods accordingly. Advanced techniques such as touch DNA analysis or partial DNA profiling or familial searching may be employed to identify perpetrators even when traditional methods fail. We will also witness significant advancements in forensic technologies, for instance, nanotechnology could revolutionise crime scene investigations by enabling scientists to detect minute traces of evidence that were previously undetectable. Additionally, artificial intelligence algorithms or machine learning may be used for facial recognition or pattern recognition purposes.

As criminal activities will surely evolve over the next decades, forensic science must keep pace with these changes to combat these threats effectively. The field will need experts who are well-versed and well adapted to cutting-edge technologies enhancing the capabilities to solve crimes efficiently. By staying at the forefront of innovation and continuously adapting their methodologies, forensic scientists can play a pivotal role in ensuring justice prevails even amidst evolving criminal activities.

In order to confront the constantly changing global environment of crime and criminal activity, forensic science is a vital tool that provides critical investigation techniques and technical developments to solve difficult cases and uphold social justice. The next section examines the several categories of criminal activity that could arise in the coming decades and present difficulties for forensic professionals to investigate. Emerging crimes, including bioterrorism, deepfake manipulation, cyberattacks, and offenses using cryptocurrencies, are expected to increase and such kind of criminal activities pose unprecedented challenges to law enforcement and necessitate proactive measures to mitigate their impact on society.

Emerging crimes in the next decade

Cybercrimes and digital fraud: The rapid advancement of technology has undoubtedly brought numerous benefits to society. However, it has also given rise to a new breed of criminals who exploit the digital landscape for their nefarious activities. Cybercrimes and digital fraud have become increasingly prevalent in recent years, posing significant threats to individuals, businesses, and even governments. Crimes have taken on a completely new form, with cybercrimes and digital fraud becoming increasingly prevalent with the use of private browsers where it becomes difficult to identify the individuals committing the crime sitting behind the blue screens [3]. As technology continues to advance and starts penetrating deeper into societies, it is crucial to generate detailed first-hand information about emerging crimes in the next decade, with a particular focus on cybercrimes and digital fraud.

Firstly, it is essential to understand the nature of cybercrimes as these offences encompass a wide range of activities conducted through electronic means all done by hiding behind an internet generated computer wall [4]. With the increasing reliance on technology for daily activities like banking, gaming, shopping, entertainment and communication, cybercriminals exploit vulnerabilities in our network systems to gain unauthorised access or steal sensitive information. Cybercrime can include various offences such as hacking, malware distribution, DDoS (Distributed Denial of Service) attacks, identity theft, phishing, cyberstalking, and more. The focus of cybercrime is on unlawful activities carried out in cyberspace, often aiming to disrupt systems, steal data, or cause financial or reputational harm. As technology continues to spring surprises to humans and also advance at an unprecedented pace in the next decade, it is obvious that cybercriminals will develop more and more sophisticated methods to carry out their illegal activities.

Secondly, digital or cyber fraud has become a significant concern in recent years and this refers to fraudulent schemes conducted online or through electronic devices with the intention of deceiving individuals or organisations for financial gain. Examples of digital fraud include a wide array of fraudulent activities, such as online scams, identity theft, credit card fraud, Ponzi schemes, fake websites, and more. The primary intent in digital fraud is to deceive victims into providing sensitive information, transferring money, or engaging in transactions that benefit the fraudster. With advancements in artificial intelligence and machine learning technologies over the next decade, criminals may employ these tools to create more convincing scams that are difficult to detect.

To put it in a nutshell, cybercrime is a broader term encompassing a range of criminal activities committed in cyberspace, while digital fraud specifically denotes fraudulent activities conducted through digital mediums with the aim of financial or personal gain. Digital fraud is a subset of cybercrime, focusing on deceptive practices carried out using electronic devices or online platforms.

Some latest and newer methods employed by such fraudsters include

Phishing attacks: Phishing attacks remain one of the most prevalent forms of cybercrime. Hackers employ deceptive tactics such as sending fraudulent emails or creating fake websites to trick individuals into revealing sensitive information like passwords or credit card details. According to a report by the Anti-Phishing Working Group (APWG), there was a 22% increase in phishing attacks in 2020 compared to the previous year (APWG | Unifying the Global Response to Cybercrime, n.d.).

Ransomware attacks: Ransomware is a class of malicious software (virus) that uses encryption methods, usually to lock users out of their systems or encrypt files. Ransomware perpetrators demand a hefty payment in return for the decryption key or the ability to access the compromised files or systems again. Attacks using ransomware can happen *via* phishing emails with malicious attachments, malicious links, exploit kits, or by taking advantage of holes in operating systems or software. Ransomware attacks have become increasingly sophisticated, targeting both individuals and organisations. Recent examples include the WannaCry and NotPetya attacks that caused widespread disruption globally. The Federal Bureau of Investigation (FBI) reported that ransomware attacks increased by 150% in 2020 alone.

Social engineering: Social engineering techniques involve manipulating individuals into divulging confidential information or performing actions that compromise security protocols. Techniques like pretexting, baiting, or tailgating are commonly used to gain unauthorised access. In 2019, over 7 billion records were exposed due to data breaches globally, these breaches not only compromise personal information but also lead to financial losses and reputational damage for businesses.

Identity theft: Identity theft continues to be a significant concern in the digital realm. Criminals steal personal information to impersonate victims for financial gain or other malicious purposes. Some of them are Business Email Compromise (BEC), Email Account Compromise (EAC) targetted to both businesses and individuals performing transfers of funds and is frequently carried out when a subject compromises legitimate business email accounts through identity thefts to conduct unauthorised transfers of funds

Cryptocurrency fraud: Cryptocurrencies are digital or virtual currencies that use cryptography to control the generation of new units and ensure secure financial transactions. Cryptocurrencies are popular as there is no need for a central authority like a bank, they function on decentralised networks built on blockchain technology, guaranteeing transaction security & transparency. The rise in popularity of cryptocurrencies has led to an increase in related fraud schemes such as Ponzi schemes, fake initial coin offerings (ICOs), and cryptojacking - where hackers hijack computer resources to mine cryptocurrencies without consent [5]. Users of cryptocurrencies frequently enjoy some degree of anonymity, which makes it difficult to link transactions to real-world identities. This anonymity also makes it easier for fraudulent acts to occur, making it harder to find the people who are behind them. Since cryptocurrencies are not restricted to any one country, they function globally, making it difficult to coordinate investigations across borders and negotiate different legal regimes. Moreover, the swift advancement of blockchain and cryptocurrency technologies brings forth novel intricacies and on top of that lack of any legislation leads to gaps that scammers take advantage of, making it more difficult for investigators to prosecute cases.

Analysis of latest trends in cybercrimes

The frequency of ransomware attacks has witnessed a steady rise over the last decade and according to latest data from cybersecurity agencies and incident reports, the number of reported attacks has increased significantly year by year. Analysing trends in ransomware attacks provides a deeper understanding of the evolving threat landscape. Over the past decade, there has been a noticeable and concerning increase in the frequency of these attacks. The tactics employed by ransomware operators have become more sophisticated, enabling them to target a broader range of victims.

Statistical data and analysis of trends

In the year 2020 alone, there were over 305 million reported ransomware attacks globally, affecting a wide range of victims, from small enterprises to large corporations as shown in Figure 1. The COVID-19 pandemic exacerbated the situation as the abrupt transition to remote work by using the internet created vulnerabilities that ransomware operators were quick to exploit [6]. This shift in working conditions increased the attack surface, allowing threat actors to target remote workers and unprotected home networks. While the overall trend shows a consistent increase in the frequency of ransomware attacks, there have been fluctuations from year to year. Some years witnessed significant spikes, while others showed slower growth. The decline in 2019 can be attributed to a global law enforcement operation that disrupted the infrastructure of some major ransomware families, leading to a temporary decrease in attacks (Figure 1).

One of the key factors contributing to the surge in ransomware attacks is the growing sophistication of cybercriminals. They have not only expanded their attack vectors but have also honed their methods to target high-value entities. The impact of these attacks is substantial, encompassing financial losses, downtime, data breaches, and significant damage to an entity's reputation. In terms of financial losses, businesses and organisations have paid billions of dollars in ransoms and in 2020 alone, ransomware payments reached approximately $350 million, according to data from the U.S. Department of the Treasury. These payments have wide-ranging implications, including the funding of criminal activities and the perpetuation of the ransomware ecosystem. Downtime resulting from ransomware attacks has severe consequences for organisations as it disrupts regular operations, leading to not only financial losses but also significant productivity setbacks. On average, it takes businesses around 21 days to recover from a ransomware attack, as reported by cybersecurity firm Coveware (Ransomware Payments Decline in Q4 2020, n.d.).

Data breaches caused by ransomware attacks expose sensitive information and compromise individual privacy. High-profile breaches have targeted healthcare institutions, leading to the exposure of patient records and personal data. Additionally, organisations in the financial sector have suffered breaches, jeopardising the financial security of their customers. The reputation damage incurred by organisations affected by ransomware attacks is immeasurable. The loss of trust from customers and stakeholders can have long-lasting consequences, including a decrease in stock value and potential legal repercussions. The increase in the sophistication of ransomware attacks is another notable trend. Modern ransomware strains are equipped with advanced encryption, anti-analysis mechanisms, and capabilities for data theft and these features make it more challenging for victims to recover their data without paying ransoms.

Geographical distribution of ransomware attacks

Ransomware attacks are not evenly distributed across the globe because of the very fact that the internet is not evenly spread across the nations. Certain regions have become hotspots for these malicious activities, reflecting the global nature of the threat as evident from Figure 2. In this section, we delve into the geographical distribution and hotspots for ransomware attacks, shedding light on areas most affected by this cyber menace. As expected, North America, particularly the United States, has been a prime target for ransomware attacks. Its high concentration of businesses and critical infrastructure makes it an attractive target for cybercriminals. Large cities, including New York, California, San Francisco, Chicago, Boston and Atlanta, have experienced notable ransomware incidents, resulting in significant financial losses and operational disruptions [7] (Figure 2).

Europe is another region significantly affected by ransomware attacks. European countries, such as France, Germany, and the United Kingdom, have reported a growing number of incidents. The European Union's (EU) General Data Protection Regulation (GDPR) has also created incentives for cybercriminals to target organisations with the threat of data exposure. The Asia-Pacific region has seen a growing threat from ransomware attacks as

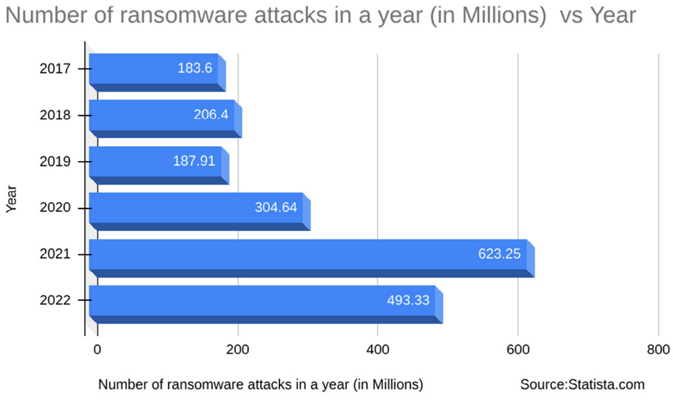

Figure 1. Statistical data of number of ransomware attacks.

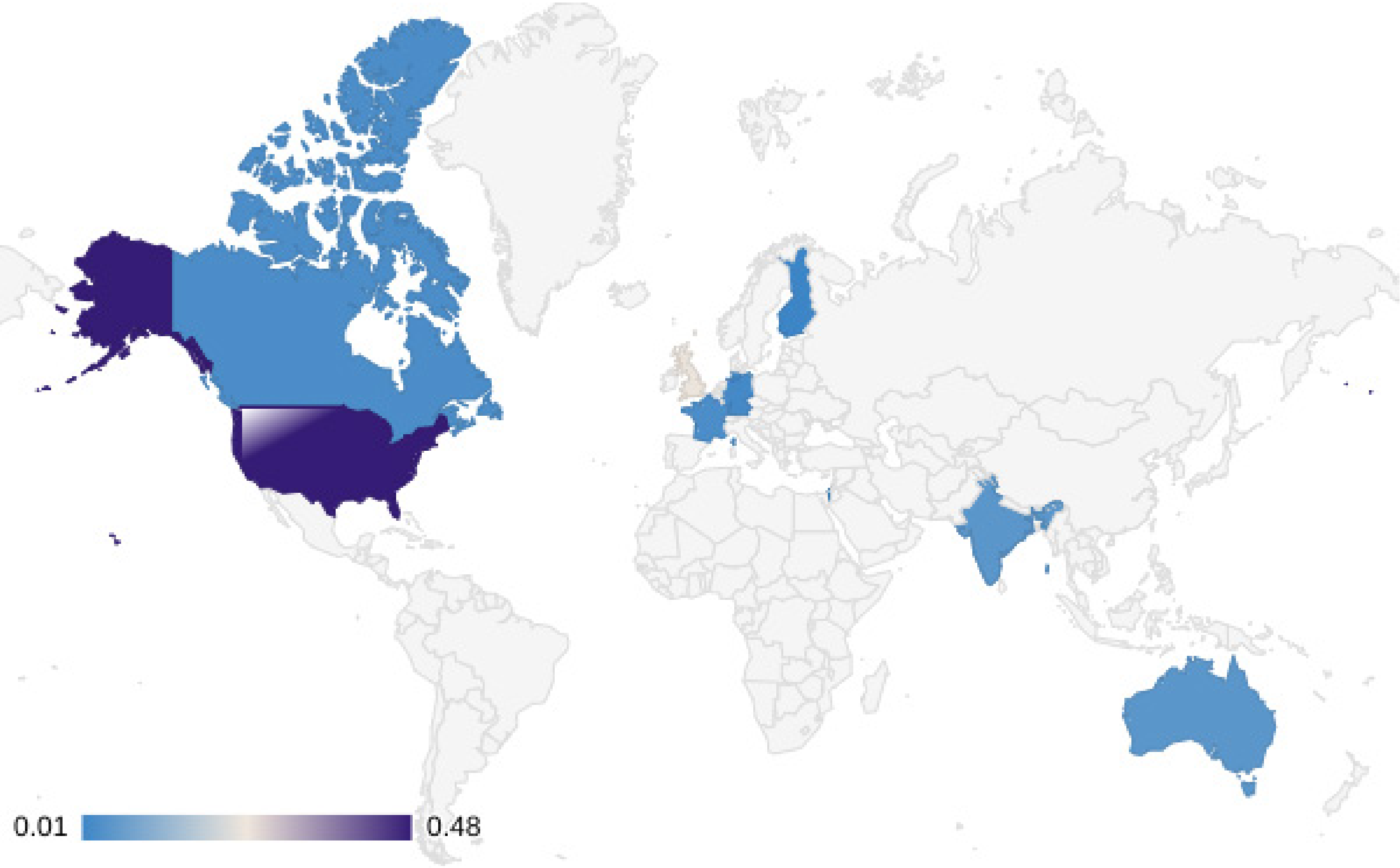

Figure 2. Geographical distribution of ransomware attacks.

countries like India and Australia have reported an increase in incidents, with the healthcare sector being a primary target. The rise of ransomware in this region can be attributed to its expanding digital infrastructure and economic growth.

The Middle Eastern and African countries have experienced a rising vulnerability to ransomware attacks as these regions face challenges related to political instability, inadequate cybersecurity infrastructure, and limited resources for combating cyber threats [8]. Several high-profile ransomware incidents have occurred in the Middle East, affecting the governments and organisations. It is important to note that Cybercriminals are not constrained by geographical borders, and their operations can target victims anywhere in the world. As a result, ransomware attacks exhibit a geographical distribution with hotspots in regions such as North American and European countries.

Online frauds and measures taken by various countries to combat cyber crimes

Online fraud has become a widespread and complex problem in the digital age as with the increasing reliance on digital transactions, criminals have adapted their techniques to exploit vulnerabilities in the online environment. The global scale of online fraud is staggering, as justified by the data from Federal Trade Commission (FTC) in the United States, consumers reported losing over $3.3 billion to fraud in 2020, with phishing and imposter scams being the most prevalent.

Europe isn't far behind and has also witnessed a significant rise in online fraud with European Cybercrime Centre (EC3) reported a 59% increase in online fraud cases from 2019 to 2020, indicating a growing problem within the European Union. In the Asia-pacific region, online fraud rates have been on the rise, with countries like India, China, and Australia experiencing an increase in various kinds of cyberattacks. According to a report by Norton, India saw a 28% increase in cyberattacks in 2020, with phishing and identity theft being the most common and as a response to the growing threat of online fraud, various countries have taken significant measures to combat it.

United States: Legislative framework and enforcement

The United States has a robust legislative framework in place to combat online fraud and the Federal Trade Commission (FTC) plays a central role in consumer protection, investigating and prosecuting cases of online fraud. The U.S. Department of Justice also focuses on cybercrime, with agencies such as the Cybercrime Unit actively pursuing cybercriminals. The U.S. government has also established cybersecurity initiatives, such as the National Institute of Standards and Technology (NIST) framework, which provides guidelines for organisations to enhance their cybersecurity measures. The Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3) provides the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected cyber-enabled criminal activity. Furthermore, public-private partnerships have been forged to facilitate information sharing and collaborative efforts to combat online fraud.

European Union: GDPR and enhanced cooperation

The European Union (EU) has implemented the General Data Protection Regulation (GDPR), which places strict requirements on data protection and privacy. GDPR not only enhances individuals' rights but also imposes significant fines on organisations that fail to protect personal data. This regulatory framework has a significant impact on online fraud prevention. In addition to GDPR, the EU established the European Cybercrime Centre (EC3) to coordinate efforts against cybercrime, including online fraud. The EU has also invested in research and innovation programs to develop advanced cybersecurity technologies and strengthen its cybersecurity workforce.

Australia: Cybersecurity strategy and legislation

Australia has introduced a national cybersecurity strategy to protect its citizens and businesses from online fraud and cyber threats. The strategy includes measures to enhance cybersecurity awareness, provide resources for individuals and organisations, and promote international collaboration. Australia has also passed legislation, such as the Security of Critical Infrastructure Act, which aims to secure critical infrastructure against cyber threats. The Australian Cyber Security Centre (ACSC) works to provide cybersecurity guidance, threat intelligence, and incident response capabilities.

India: National cyber security policy

India has formulated a National Cyber Security Policy to address the rising threat of cybercrimes, including online fraud. The policy focuses on strengthening the country's cybersecurity infrastructure, promoting research and development, and enhancing cooperation with international organisations. The Reserve Bank of India (RBI) has also issued guidelines to enhance the security of digital transactions and protect consumers from online fraud. These guidelines emphasise secure banking practices and the use of robust authentication methods.

International cooperation: INTERPOL and global alliances

International organisations play a pivotal role in addressing online fraud and INTERPOL's Cyber Crime Directorate fosters cooperation between countries to combat cybercrimes on a global scale because it facilitates information sharing, supports capacity building, and coordinates operations against cybercriminals [9]. Global alliances, such as the Financial Action Task Force (FATF), work to combat money laundering, which often supports online fraud. FATF's recommendations and assessments help countries strengthen their legal frameworks and enhance financial regulations to prevent and detect fraudulent activities.

Forensic techniques for tracing digital footprints and evidence collection

All kinds of digital devices and online activities on the internet leave behind a trail of digital footprints, which can serve as valuable evidence in investigations of cybercrimes. The systematic process of collecting digital evidence includes identification, preservation, analysis, and presentation are done carefully, ensuring the maintenance of the chain of custody and integrity of the evidence [10].

Data imaging: Use of imaging tools to create a bit-by-bit copy of digital storage media, ensuring that no alterations are made to the original evidence.

File recovery techniques: For recovering deleted or hidden files, which can provide crucial evidence in investigations.

Timeline analysis: Reconstructing timelines to establish the sequence of events, providing context to digital evidence [11].

Internet history analysis: Examination of web browser histories and cache files to trace online activities, which can be pivotal in cybercrime investigations.

Email analysis: Examination of email headers and contents, which can uncover communication networks and digital trails.

Metadata examination: Significance of metadata, such as date and time stamps, geolocation data, and user information, in verifying the authenticity and source of digital files.

Environmental crimes

Environmental crimes, as they are popularly known as include environmental offences or eco-crimes, refer to illegal activities that harm the environment, violate environmental laws, and threaten the well-being of ecosystems, wildlife, and human health. These crimes can take various forms, such as pollution, deforestation, illegal wildlife trade, and hazardous waste dumping [12]. Environmental crimes are rising by 5-7% annually which is 2–3 times the rate of the global economy.

Such crimes against nature not only damage the environment but also have severe consequences for flora and fauna habituating in these areas and human health and well-being in general. These crimes encompass a wide range of actions that damage or exploit the natural world, often for personal gain or profit. Unlike any other known crime, environmental crimes are aggravated through their additional cost and impact on the environment and cost to future generations [13]. Understanding environmental crimes is essential for the protection and preservation of our planet. The most prominent consequences of Environmental Crimes are listed below:

Ecological damage: Environmental crimes can cause irreversible harm to ecosystems, leading to habitat destruction and species extinction.

Health impacts: Pollutants from illegal activities can contaminate the air, water, and soil, leading to health issues in communities exposed to them.

Economic costs: Environmental crimes can result in economic losses due to damage to natural resources and the cost of cleanup and restoration.

Social unrest: In some cases, environmental crimes can lead to conflicts and social unrest, especially in areas where communities rely on the environment for their livelihoods.

Discussion of environmental crimes

Illegal wildlife trade: The illegal wildlife trade is by some estimated at 7–23 billion USD per year.

Poaching: The illegal hunting, capturing, or killing of protected or endangered species, such as elephants, rhinoceroses, tigers, and pangolins, for their body parts, fur, or exotic pets [14].

Wildlife trafficking: The illicit smuggling and trade of wildlife and their products, which includes live animals, animal parts, and traditional medicines derived from endangered species [15].

Smuggling of protected species: The illicit trade of protected species, live or dead, and their products, such as corals, seashells, and exotic animals.

Deforestation

Illegal Logging: Unlawful cutting of trees, often in protected or conservation areas, for timber or other forest products.

Slash-and-burn agriculture: The practice of clearing land by burning forests, which contributes to deforestation, loss of biodiversity, and carbon emissions.

Wildlife habitat destruction: The destruction of critical wildlife habitats through activities like land reclamation, urban development, and infrastructure expansion, which disrupts ecosystems and threatens biodiversity.

Pollution

Air pollution: Activities that emit harmful pollutants into the air, such as emissions from industrial facilities, vehicles, and energy production, exceeding regulatory limits.

Water pollution: The unauthorised discharge of pollutants, chemicals, or toxins into water bodies, leading to contamination and harm to aquatic ecosystems.

Noise/sound pollution: Excessive noise from industrial, commercial, or recreational activities, which can disturb ecosystems, disrupt wildlife behaviour, and impact human health.

Marine pollution: The release of pollutants, including oil spills, plastic waste, and chemicals, into oceans and seas, which harms marine life and ecosystems [16].

Hazardous waste dumping

Illegal dumping: The unauthorised disposal of waste, such as industrial chemicals or medical waste, in landfills, bodies of water, or natural environments.

Waste dumping: The disposal of electronic waste, which contains hazardous materials like lead and mercury, into developing countries where it is improperly processed, leading to environmental and health risks.

Land and soil contamination: The unauthorised disposal of hazardous materials into the ground, contaminating soil and impacting land quality for agricultural or industrial purposes.

Fisheries crimes

Overfishing: The excessive and unsustainable harvesting of fish, often exceeding sustainable levels, which depletes fish stocks and disrupts marine ecosystems.

Fishing in protected areas: Unauthorised fishing in marine protected areas or during restricted seasons.

Illegal mining

Unregulated extraction: Mining operations conducted without proper permits, leading to habitat destruction, soil and water pollution, and release of toxic substances into the environment.

These environmental crimes have far-reaching consequences, including Species Extinction as rise in poaching and wildlife trafficking contributes to species extinction and imbalances in ecosystems. Zoonotic Disease Risk - illegal wildlife trade poses a significant risk for zoonotic diseases, as it brings humans into closer contact with wild animals [17]. Economic Impacts - loss of biodiversity can disrupt economies dependent on ecotourism, natural resources, health risks, economic costs, and social unrest. Law enforcement agencies, legal regulations, and international agreements are essential components in the efforts to combat and prevent these offences and protect the environment for current and future generations.

Forensics in tracking and prosecuting environmental offenders

Forensics and forensic methods play a crucial role in identifying the source of pollutants or hazardous materials. Forensic science provides the tools and expertise necessary to investigate, collect, and analyse evidence, ultimately contributing to the prosecution of those responsible for environmental crimes. Chemical analysis can determine the composition of a pollutant found at a crime scene, linking it to a specific industry or individual. Additionally, DNA analysis is used to identify illegally traded animal products or track down poachers. Forensic techniques help establish causality between an offender's actions and environmental damage. By analysing soil samples or water quality data near a suspected crime site, experts can provide scientific evidence that supports legal claims against the perpetrator [18].

Furthermore, forensic methods are essential for ensuring that justice is served, and the criminals are punished in environmental cases. The use of advanced technologies like remote sensing and geographic information systems (GIS) allows investigators to map out crime scenes accurately and this helps prosecutors present compelling visual evidence in courtrooms. By providing scientific evidence that links perpetrators to their crimes and establishes causality between actions and environmental damage, forensics plays a vital role in protecting our planet's natural resources for future generations [18].

Adequate funding and training for individuals present at the ground level as well as to teams monitoring the protected or conserved areas are essential to ensure effective enforcement.

Biotechnology and biosecurity threats

Biotechnology, which is the application of biological principles and techniques to develop products or processes, offers tremendous benefits to society, from advances in medicine to sustainable agriculture. However, these same biotechnological advances can also pose threats if misused or harnessed for harmful purposes. Whereas biosecurity is the protection of biological materials and technologies from misuse or theft, is essential in managing these risks.

Exploration of biosecurity threats like bioterrorism and synthetic biology risks

Biotechnology threats:

Biological weapons: Recent advances in biotechnology have raised concerns about the potential development of biological weapons, including engineered pathogens that could be used in bioterrorism. The intentional release of such agents could cause widespread harm and devastation [18].

Genetic engineering: Genetic engineering allows for the modification of organisms, including microorganisms, plants, and animals. The misuse of this technology may result in the creation of dangerous or invasive species, posing ecological threats [19].

Gene editing tools: The ease of availability of gene-editing tools like CRISPR-Cas9 makes it easier to modify genetic material, potentially leading to the creation of dangerous or highly infectious organisms [20].

Dual-use research: Some research areas in biotechnology can have both beneficial and harmful applications. Dual-use research can involve experiments that lead to insights about pathogenic microorganisms or toxins, which could be exploited for malicious purposes.

Synthetic biology: Synthetic biology enables the design and construction of biological systems and organisms. While it has many constructive applications, it could be used to design and create dangerous pathogens [19].

Biosecurity threats:

Theft of biological materials: Laboratories and facilities working with potentially hazardous biological materials must safeguard their stocks to prevent theft or unauthorised access. Theft of pathogens or research materials can lead to the misuse of these materials [18].

Bioterrorism: The deliberate release of harmful biological agents or bioweapons by individuals or groups can lead to public health crises and significant social disruption. Effective biosecurity measures are vital in preventing and responding to bioterrorist acts.

Designer pathogens: Synthetic biology allows for the creation of custom-designed microorganisms, including pathogens, which could be used for malicious purposes. These engineered organisms may be resistant to existing treatments [17].

Accidental releases: Laboratories working with pathogens, including those involved in vaccine development or diagnostics, must ensure strict containment protocols. Accidental releases can occur, causing unintentional outbreaks or contamination.

Abuse of research: Some research may inadvertently or intentionally lead to the creation of harmful biological agents. Appropriate oversight and regulations are needed to mitigate these risks.

Lack of security awareness: Insufficient awareness of biosecurity issues among researchers, laboratory workers, and policymakers can result in lax security measures, increasing the vulnerability to biotechnology threats.

Role of forensic genetics and forensic biotechnology in preventing and responding to biocrimes

Forensic genetics and forensic biotechnology plays a critical role in preventing, detecting, and responding to bio-crimes, biotechnology threats and biosecurity threats. These specialised professionals offer essential tools and methodologies for law enforcement, public health agencies and researchers in managing these multifaceted yet daunting challenges. Here's an overview of their roles:

Forensic genetics in bio-crime prevention and response

DNA profiling: Forensic genetics relies on DNA profiling techniques to identify individuals and link them to crimes. In cases of bio-crimes, such as bioterrorism or the intentional release of pathogens, DNA analysis can help identify the perpetrators or contaminated individuals.

Identifying pathogen sources: In cases of bioterrorism or outbreaks of infectious diseases, forensic genetics can be used to trace the source of the pathogen. This is crucial in determining the origin of a bio-crime and its potential spread.

Victim identification: Forensic genetics can help identify victims of bio-crimes, mass casualties, or accidents involving biological agents. This is vital for providing closure to families and for public health responses.

Database comparison: Genetic databases can be used to compare DNA profiles from crime scenes with known individuals, assisting in the identification and tracking of bio-crime suspects.

Forensic biotechnology in bio-crime prevention and responses

Pathogen detection: Forensic biotechnology tools, such as polymerase chain reaction (PCR) and its various types, can be used to detect and identify pathogens in environmental samples or victims, aiding in bio-crime investigations.

Genomic sequencing: Genomic sequencing technologies can provide detailed information about the genetic makeup of pathogens, helping to understand their origins and any engineered modifications [21].

Epidemiological studies: Forensic biotechnology can be applied in epidemiological studies to trace the spread of infectious diseases, whether natural or intentionally caused.

Biotechnology threats and biosecurity threats

Threat assessment: Forensic biotechnology and genetics contribute to the assessment of biotechnology and biosecurity threats by analysing the potential risks and vulnerabilities associated with research, pathogens, or bioterrorism.

Surveillance and monitoring: Continuous surveillance and monitoring of emerging biotechnology threats are essential. Forensic genetics and biotechnology provide the means to detect unusual or unauthorised activities that may pose biosecurity risks [21].

Investigation and attribution: In cases of biotechnology threats or biosecurity breaches, forensic genetics can help identify those responsible and establish a basis for legal action [21].

Riskmitigation: Biotechnology and biosecurity threats require comprehensive risk mitigation strategies. Forensic biotechnology and genetics contribute to the development of safety protocols and regulatory frameworks.

Public awareness

Raising public awareness about the implications of bio-crimes, biotechnology threats, and biosecurity is essential. Forensic genetics and biotechnology can play a role in educating the students and public about the importance of these issues [22].

Hence, forensic geneticists and biotechnologists play an indispensable role in the prevention, detection, response, and mitigation of bio-crimes, biotechnology threats, and biosecurity threats arising in the next few decades. Their combined use provides the scientific foundation for legal action, surveillance, and global cooperation to protect public health and security in the face of evolving challenges in the biotechnology and biosecurity domains [21].

Data manipulation and deep fake crimes

In this digital age, advancements in technology have brought about numerous benefits, but they have also opened the door to novel forms of criminal activity and among these emerging threats, data manipulation and deep fake crimes have gained notoriety for their potential to deceive, manipulate, and undermine the integrity of information. Such crimes are rooted in the manipulation of data, audio, video, or images, often with malicious intent.

Data manipulation

Data manipulation refers to the unauthorised or deceptive alteration of digital information and it involves the modification of databases, financial records, or other forms of data to achieve various criminal objectives, including fraud, identity theft, or corporate espionage. Data manipulation crimes can disrupt critical systems, compromise personal information, and have far-reaching consequences for individuals, organisations and even governments.

Deep fake crimes

Deep fakes are synthetic/artificial media created through advanced artificial intelligence and machine learning techniques and these media often involve hyper-realistic alterations of audio, video, or images, superimposing individuals' faces or voices onto other content. Deep fake crimes encompass the use of such media to deceive, impersonate, or manipulate individuals or public discourse. Such types of crimes have the potential to erode trust, spread misinformation, and compromise the authenticity of content.

Both data manipulation and deep fake crimes are a testament to the evolving landscape of digital deception. As technology continues to advance, the challenges associated with preventing and addressing these crimes grow. To combat these threats effectively, it is crucial to stay informed about the latest developments in cybersecurity, artificial intelligence, and forensic techniques, all of which play a pivotal role in the battle against data manipulation and deep fake crimes.

Examination of data

The advent of deepfake technology has ushered in an era where the manipulation of digital content has reached unprecedented levels of sophistication. Deep Fakes as explained earlier are created using artificial intelligence and machine learning algorithms. Such technologies allow malicious actors to convincingly alter or fabricate content, making it appear as though individuals are saying or doing things they never did. This remarkable progress in digital manipulation raises concerns about the potential for deep face technology to be harnessed for malicious purposes. Deepfake technology has advanced rapidly in recent years, fueled by the availability of vast datasets, improved algorithms, and more powerful computing resources. It allows for the seamless blending of one person's likeness, voice, or behaviour with another's, creating highly realistic and deceptive content. What was once a tool primarily for entertainment and artistic expression has now become a potential weapon in the hands of those with nefarious intent!.

Misinformation campaigns: Deepfakes can be used to spread false narratives, manipulate public opinion, and influence elections. Malicious actors can create convincing videos of public figures making controversial statements, sowing confusion and discord.

Blackmail and extortion: Deepfake technology can be used to create compromising videos or audio recordings that target individuals, putting them at risk of extortion or reputational harm.

Identity theft: Criminals can use deepfakes to impersonate individuals in video calls or audio recordings, potentially gaining access to sensitive information, or deceiving family and friends.

Fraud and scams: Deepfakes can be utilised in various fraudulent schemes, such as voice phishing (vishing) attacks, where individuals are tricked into believing they are communicating with someone they know and trust.

Forgery: Deepfakes can be used to create convincing counterfeits of legal or financial documents, further complicating fraud detection and prevention.

Cybersecurity threats: With the rise of biometric authentication systems, deepfake technology can pose a significant cybersecurity threat. Criminals may use deepfake videos to defeat facial recognition or voice recognition systems.

Forensic methods for detecting and verifying manipulated media

As deep fake technology advances, so does the need for robust forensic methods, techniques and tools to detect and verify manipulated media. Deep fake crimes pose significant challenges and to combat these threats effectively, forensic experts as of now have these techniques and technologies at their disposal:

Metadata analysis: Metadata includes information about the creation and modification of digital media. Forensic analysts examine metadata to identify inconsistencies or signs of manipulation. Metadata can reveal details like timestamps, device information, and editing history [23].

Reverse image and video search: Forensic investigators use reverse image and video search tools to trace the origins of media content. By identifying the original sources or similar content, they can uncover manipulated or deep fake elements.

Digital watermark analysis: Watermarks, often used to protect the authenticity of images and videos, can be analysed to verify the integrity of media. Altering or removing watermarks is a common sign of manipulation.

Error level analysis: Error level analysis examines compression artefacts in media files. When an image or video is edited, it may produce different error levels in various parts of the file, suggesting tampering.

Cryptographic signatures: Cryptographic techniques can be used to establish the authenticity of digital media. Signatures and hashes can confirm that the content has not been altered since it was created [24].

Machine learning algorithms: Machine learning models can be trained to detect deep fakes based on patterns and anomalies, moreover these models analyze in depth facial expressions, speech patterns, and other features to identify inconsistencies [24].

Audio analysis: Audio forensics experts can verify the authenticity of voice recordings by examining acoustic characteristics, pitch, and speech patterns. Discrepancies in these elements may indicate manipulation.

Lip sync detection: Deep fakes often involve the manipulation of lip movements to match synthesised speech. Lip sync detection tools can identify discrepancies between audio and visual cues.

Face recognition: Facial recognition technologies can help identify whether the face in a video matches known reference images. Deep fake faces may not align with genuine references.

Image forensics software: Specialised software tools, like Adobe Photoshop's Forensic Toolkit, are designed to detect image manipulation. They can reveal signs of cloning, splicing, or other editing techniques.

Blockchain verification: Some platforms use blockchain technology to timestamp and secure digital media as Blockchain can provide immutable records, making it challenging to alter or delete content without detection [25].

Human expert analysis: Experienced forensic experts play a critical role in verifying manipulated media as the human brain is much more capable of identifying inconsistencies that automated tools might miss, applying their knowledge of media forensics.

Social media analysis: Social media platforms are common distribution channels for deep fake content. Forensic investigators monitor these platforms to identify and report suspicious media.

Multimodal analysis: Combining different forensic techniques, such as analysing both image and audio components, can enhance the accuracy of deep fake detection [24].

Transnational organised crimes

Transnational organised crime represents a pervasive and evolving global threat, characterised by criminal enterprises that operate across international borders, often with sophisticated structures and networks. These criminal activities extend beyond traditional local or national boundaries, impacting countries, economies, and societies on a worldwide scale [26]. Transnational organised crime encompasses a wide range of illicit activities, from drug trafficking and human smuggling to cybercrime and money laundering, making it a complex and multifaceted challenge [27]. At the heart of transnational organised crime lies a convergence of criminal intent, organisational complexity, and global connectivity. Criminal syndicates and networks exploit advancements in technology, transportation, and communication to facilitate their operations, creating a shadow world where traditional laws and regulations struggle to keep pace and thus, serves as a gateway to understanding the multifarious dimensions of transnational organised crime, the threats it poses, and the efforts made to combat and mitigate its impact on the global stage [28].

Analysis of evolving transnational crimes

Transnational crimes, such as human trafficking and drug smuggling, continue to evolve, presenting complex and ever-changing challenges for law enforcement agencies and governments worldwide [26]. Understanding the dynamics, trends, and responses to these crimes is essential in the fight against them.

Human trafficking: It involves the recruitment, transportation, transfer, harbouring, or receipt of individuals through force, coercion, or deception, with the aim of exploiting them for forced labour, sexual exploitation, or other illicit purposes. Here is an analysis of its evolution:

Globalization and vulnerability: The globalisation of labour markets has created opportunities for traffickers as they can find takers in any part of the world. Vulnerable populations like the poor or marginalised sections of the society seeking better economic prospects are often targeted by such criminals.

Online facilitation: The internet plays a significant role in human trafficking. Traffickers use social media, online classifieds, and encrypted communication tools to recruit victims and coordinate operations.

Economic incentives: The profitability of human trafficking continues to attract criminal organisations. Victims are often trapped in cycles of debt bondage, making it difficult for them to escape.

Legal frameworks: Many countries have strengthened their legal frameworks to combat human trafficking. International cooperation and agreements, such as the United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons, have been established to facilitate prosecution yet these criminals find a loophole here and there to exploit [29].

Victim-centred approaches: A shift toward victim-centred approaches has been observed. Greater emphasis is placed on providing support, rehabilitation, and protection to victims.

Drug smuggling: Drug smuggling involves the illegal transportation of narcotics and psychotropic substances across international borders for distribution and sale. It is a significant component of the global illicit drug trade. Here is an analysis of its evolution:

Routes and methods: Drug traffickers continually adapt their transportation routes and methods. Traditional trafficking routes have diversified, and traffickers use increasingly sophisticated techniques, such as concealed compartments in vehicles, drones, and tunnels.

Drug types: The types of drugs being smuggled have evolved. While traditional drugs like cocaine, heroin, and marijuana remain prominent, synthetic drugs like methamphetamine and fentanyl have gained traction.

Global drug trade networks: These groups have expanded their networks and diversified their criminal portfolios to include other illegal activities.

Technological advancements: Technology has impacted drug smuggling, both in terms of detection and trafficking. Advancements in drug detection methods and surveillance technologies have increased law enforcement capabilities but these smart criminals have devised strategies to overcome or combat these advancements.

Transnational crimes like human trafficking and drug smuggling are continuously evolving, posing significant challenges to governments and international communities [30]. Effective responses require a combination of legal, law enforcement, and humanitarian efforts, along with a commitment to adapt to the ever-changing nature of these criminal activities.

International forensic cooperation to combat organised crime

International cooperation among the nations and the law enforcement agencies that lay emphasis on addressing the root causes of these crimes are both essential as well as the need of the hour to combat their influence on a global scale [29]. International forensic cooperation is a critical tool in the global fight against organised crime. Organised crime groups often operate across borders, making it essential for law enforcement agencies and forensic experts from different countries to collaborate. Here's an in-depth look at the importance and use of international forensic cooperation in combating organised crime:

Global reach of organised crime: Organised crime transcends national boundaries. Criminal organisations engage in activities like drug trafficking, human trafficking, cybercrime, and money laundering that involve multiple countries. Effective responses require international cooperation to track, investigate, and dismantle these criminal networks.

Information sharing: Forensic cooperation enables the sharing of critical information, evidence, and intelligence among nations which includes sharing data on criminal organisations, their members, and their activities [29]. Cross-border information exchange is vital in building a comprehensive understanding of organised crime networks.

Standardized protocols and procedures: International cooperation helps establish standardized protocols and procedures for forensic investigations which also in turn ensures that evidence collection, analysis, and preservation follow recognized best practices, enhancing the reliability of evidence in legal proceedings [29].

Expertise and resources: Different countries possess varying forensic expertise and resources. Collaborative efforts allow for the pooling of knowledge, technology, and resources, enabling more effective and efficient investigations.

Transnational evidence: Organised crime often involves the movement of evidence, assets, and individuals across borders. International forensic cooperation aids in tracking, identifying, and recovering these elements, which are crucial for successful prosecutions [9].

Cross-border legal processes: International cooperation supports the legal processes necessary to extradite suspects and prosecute them in the relevant jurisdictions [9]. Mutual legal assistance treaties and extradition agreements facilitate the extradition of individuals involved in transnational organised crime.

Disruption and dismantling: Organised crime thrives on its global reach and interconnected nature. International cooperation is key to disrupting and dismantling these criminal networks. By targeting their leaders, infrastructure, and financial assets across borders, law enforcement can weaken these organisations.

Prevention and deterrence: Collaborative efforts also extend to prevention and deterrence. Sharing information about trends and emerging threats helps nations implement proactive measures to prevent organised crime activities.

Public safety: Ultimately, international forensic cooperation serves the interest of global public safety which ultimately helps in the protection of communities from the devastating effects of organised crime, including drug addiction, human exploitation, and financial losses.

Extraterritorial jurisdiction: Many transnational crimes involve acts committed in one country that have impacts in another. International collaboration enables the exercise of extraterritorial jurisdiction, allowing countries to prosecute individuals who commit crimes abroad.

Multinational operations: Coordinated multinational operations, such as joint law enforcement efforts and task forces, are more likely to succeed in disrupting and dismantling transnational criminal networks. These operations are often only possible through international collaboration.

Challenges and ethical considerations

Ethical dilemmas and privacy concerns in forensics and use of advanced forensic technologies:

The rapid advancement of forensic technologies has revolutionised the field of criminal investigation and justice. However, these innovations have also introduced a range of ethical dilemmas as well as privacy concerns that law enforcement, forensic experts, and policymakers must grapple with. Here, we explore some of the key ethical dilemmas associated with the use of advanced forensic technologies:

Privacy *vs.* security: One of the central ethical dilemmas is the balance between individual privacy and public security. Advanced technologies, such as facial recognition and DNA databases, raise concerns about unwarranted surveillance and intrusion into individuals' private lives'.

Informed consent: The use of advanced forensic technologies often requires the collection of biological samples, biometric data, or other personal information. Obtaining informed consent from individuals for the use of their data can be challenging, especially in cases involving suspects or victims who may not fully understand the implications.

Discriminatory practices: Forensic technologies have the potential to perpetuate discrimination and bias. Racial, gender, or socioeconomic biases may be encoded into algorithms, leading to disproportionate impacts on certain groups.

Chain of custody and data integrity: Maintaining the integrity of forensic evidence is an ethical imperative. Challenges arise when handling digital evidence, as issues related to data tampering, hacking, or chain of custody breaches can compromise the integrity of evidence [10].

Data storage and security: Advanced forensic technologies generate vast amounts of sensitive data. The ethical dilemma lies in ensuring the security and privacy of this data, particularly in the face of cyber threats or insider misconduct.

Misuse of technology: The potential misuse of advanced forensic technologies for surveillance, harassment, or other illicit purposes is a significant ethical concern. Unauthorised access to databases or the weaponization of forensic tools can lead to harm.

DNA ancestry testing: Commercial DNA ancestry testing services raise questions about the privacy and consent of individuals whose genetic information is shared with third-party companies. Moreover, the potential for unintended familial discoveries can lead to ethical dilemmas.

Forensic profiling and stigmatisation: The practice of forensic profiling based on genetic, behavioural, or biometric data may lead to stigmatisation and discrimination, potentially affecting an individual's reputation and opportunities.

Erosion of presumption of innocence: The prevalence of forensic evidence can influence public perception and legal proceedings, potentially eroding the presumption of innocence. Accused individuals may face social stigma, even if they are later acquitted.

Ethical use of predictive technologies: The ethical use of predictive forensic technologies, such as predictive policing and recidivism prediction, raises concerns about bias, accuracy, and the potential for self-fulfilling prophecies.

Accountability and transparency: The transparency of forensic technologies, their algorithms, and the methods used in investigations is essential for accountability. Ethical dilemmas arise when proprietary technology hinders transparency.

Dual-use technologies: Some advanced forensic technologies have dual-use applications, both in law enforcement and potentially harmful activities like hacking - ethical or unethical. Striking a balance between legitimate uses and safeguarding against misuse is challenging.

Long-term data retention: The ethical implications of long-term data retention by law enforcement agencies relate to the security of the data and the potential for abuse. Safeguards to prevent misuse are essential.

Access to justice: Ensuring that advanced forensic technologies do not disproportionately affect marginalised or underserved communities is an ethical challenge. Access to justice and equitable treatment must be upheld in almost all the cases.

Balancing security and individual rights

Most technological advancements come with profound ethical dilemmas and privacy concerns that must be carefully navigated to strike a balance between security and individual rights. Here's an exploration of these dilemmas and concerns:

Surveillance and privacy

Ethical dilemma: The use of surveillance technologies, such as facial recognition and biometric tracking, in public spaces can enhance security but at the expense of privacy. The indiscriminate collection and storage of individuals' data raise concerns about unwarranted surveillance and invasion of personal space.

Privacy concern: Striking a balance involves crafting policies and regulations that define the limits of surveillance. Implementing clear guidelines on data retention, lawful use, and the need for judicial warrants is crucial to protect individual privacy.

Biometric data and DNA profiling

Ethical dilemma: The collection and analysis of biometric data, including DNA, for forensic purposes raise ethical dilemmas regarding informed consent and the potential for genetic discrimination. While these tools are invaluable for identifying suspects and solving crimes, they involve sensitive personal information.

Privacy concern: Balancing individual rights entails ensuring that informed consent is obtained for the collection of biometric data. Additionally, robust legal safeguards against genetic discrimination are vital.

Data security and cyber threats

Ethical dilemma: Advanced forensic technologies rely on vast data repositories. Ensuring the security and integrity of these databases is a complex ethical challenge. Cyber threats and data breaches could expose sensitive information to malicious actors.

Privacy concern: Maintaining stringent data security measures is essential. Encryption, authentication protocols, and continuous monitoring of data repositories are necessary to protect individual rights while using advanced technologies.

Algorithmic bias

Ethical dilemma: Algorithms used in forensic technologies are susceptible to bias, which can disproportionately impact marginalised communities. Bias may lead to unfair treatment or the misidentification of individuals.

Privacy concern: Eliminating bias and ensuring fairness in algorithmic decision-making require transparency, scrutiny, and regular audits. Ethical practices demand the development of algorithms that are both accurate and equitable.

Predictive technologies

Ethical dilemma: The use of predictive technologies in criminal justice, such as predictive policing or recidivism prediction, raises ethical questions about profiling, surveillance, and the presumption of innocence.

Privacy concern: Striking a balance necessitates implementing safeguards to prevent discrimination and misuse of predictive technologies. Regular reviews and impact assessments are crucial to protect individual rights.

Public perception and accountability

Ethical dilemma: The public's perception of forensic practices and their trust in law enforcement can be influenced by the use of advanced technologies. The erosion of the presumption of innocence is an ethical concern.

Privacy concern: Law enforcement agencies must communicate transparently about their practices and adhere to ethical principles that uphold individual rights and due process. Accountability mechanisms should be in place to address potential violations.

Long-term data retention

Ethical dilemma: The long-term retention of data, even when no longer relevant to a case, poses an ethical dilemma. It can create opportunities for abuse and compromise privacy.

Privacy concern: Legal frameworks should specify the conditions under which data can be retained and for how long. The deletion of data that is no longer necessary for investigations is essential.

Striking the right balance between security and individual rights in technologically evolving forensic practices requires a multi-faceted approach. This approach should encompass legal safeguards, regulatory frameworks, public awareness, ethical guidelines, and ongoing scrutiny. Privacy and individual rights should remain at the forefront of decision-making processes to ensure that technological advancements benefit society without infringing on fundamental freedoms.

The role of international cooperation

The significance of global collaboration in combating transnational crimes

Transnational crimes as mentioned earlier in the text, such as human trafficking, drug smuggling, cybercrime, and terrorism, pose significant threats to global security and stability. These crimes often transcend national borders, making them challenging to combat through unilateral efforts [27]. Global collaboration plays a pivotal role in combating transnational crimes, which have far-reaching consequences. The significance of global collaboration in addressing transnational crimes is paramount because criminal activities have become increasingly interconnected and sophisticated, hence international cooperation becomes essential to protect the security and well-being of individuals, families, societies and nations worldwide. It enables a collective response that is more effective, efficient, and harmonised, ultimately working towards a safer and more secure global community.

Conclusion

It is anticipated that the panorama of criminal activity will shift as human society evolves and technology continues to improve and advance further and confirming the same is the recent trends in criminal activity and in the coming decades, cybercrime and other criminal activity are expected to be the front-runner as digital technology spreads, hacking will probably become more common, which will increase cybercrimes including ransomware attacks, identity theft, and data breaches. Artificial Intelligence (AI) has the potential to be used as a weapon for a number of illegal acts, such as the production of deepfakes, automated hacking, and more complex online scams. The creation of designer pathogens, genetic identity theft, and bioterrorism are possible outcomes of biotechnology and biosecurity advancements. Crimes pertaining to illegal logging, poaching, pollution, and wildlife trafficking are predicted to increase as environmental issues become more pressing. Transnational criminal organisations will continue to engage in activities like drug trafficking, human smuggling, and cybercrimes, taking advantage of globalisation. Evolving financial crimes, including cryptocurrency fraud, money laundering, and investment scams, will accompany the digital financial revolution. As innovation continues, the theft of intellectual property, trade secrets, and patented technology will remain a concern. The use of emerging technologies, like AI and biotechnology, may raise ethical concerns regarding privacy, bias, and the responsible use of these innovations and the increasing availability of surveillance technology and personal data may lead to more instances of privacy invasion, data breaches, and stalking.

Forensic science, the scientific application of principles and techniques to solve crimes, plays a pivotal role in addressing emerging threats and anticipated crimes in the coming decades and the stakeholders involved must continuously adapt to analyse complex digital evidence and uncover the perpetrators behind virtual crimes and advanced forensic analysis of samples and the development of new detection methods and also staying abreast of rapidly evolving technologies and integrating them into forensic practice is a continuous challenge. By anticipating and addressing emerging threats, forensic science can aid in preventing crimes before they occur, rather than solely reacting to them. In essence, being at the forefront of research and innovation in forensic science is essential for protecting society from emerging threats and ensuring a just and secure future.

Declarations

We confirm that the manuscript has been read and approved by all named authors and that there are no other persons who satisfied the criteria for authorship but are not listed.

Ethics Approval and Consent to Participate

Not Applicable.

Consent for Publication

Not Applicable.

Availability of Data and Material

We do not generate any datasets, because our work proceeds within a theoretical approach. One can obtain the relevant materials from the references below. (Not Applicable).

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Author Contributions

Study conception and design: Pavan Kumar Ganechary, Kollam Anjali.

Review the relevant literature: Pavan Kumar Ganechary.

Draft Manuscript preparation: Pavan Kumar Ganechary, Kollam Anjali.

All author(s) reviewed and approved the final version of the manuscript.

Acknowledgement

We thank National Forensic Sciences University for supporting us to carry out the research.

Conflicts of Interest

The author(s) declare that they have no conflict of interest.

References

1. Holt, Thomas J., Adam M. Bossler and Kathryn C. Seigfried-Spellar. “Cybercrime and digital forensics: An introduction.” Routledge (2022).
2. DeTardo-Bora, Kimberly A. and Dhruba J. Bora. "Cybercrimes: An overview of contemporary challenges and impending threats." *Dig Forensics* (2016): 119-132.
3. Ahmed, Adnan, Abdul Rehman Javed, Zunera Jalil and Gautam Srivastava, et al. "Privacy of web browsers: A challenge in digital forensics." Springer Singapore 14 (2022): 493-504.
4. Woods, Daniel W. and Lukas Walter. "Reviewing estimates of cybercrime victimisation and cyber risk likelihood." *EuroS&P* (2022): 150-162.
5. Furneaux, Nick. “Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence.” *John Wiley & Sons* (2018).
6. Wolff, Josephine. "Trends in cybercrime during the COVID-19 pandemic Emerald Publishing Limited (2023): 215-227.
7. Sharif, Md Haris Uddin and Mehmood Ali Mohammed. "A literature review of financial losses statistics for cyber security and future trend." *WJARR* 15 (2022): 138-156.
8. Mphatheni, Mandlenkosi Richard and Witness Maluleke. "Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions." *IJBSS* 11 (2022): 384-396.
9. Klevtsov, Kirill. "International cooperation in the fight against cybercrime: Current state and development prospects." In materials of All-Russian scientific and practical conference" Criminal Procedure and Criminalistic Problems of Combating (2020).
10. Casey, Eoghan. “Digital evidence and computer crime: Forensic science, computers, and the internet,” Academic Press (2011).
11. Al Abaidani, Raida Said Salim and Faizal Hajamohideen. "Techniques Involved in Forensic Evidence Collections: A Short Communication."
12. Oosthuizen, Tersia, Loene M. Howes and Rob White. "Forensic science and environmental offences: Litter, DNA analysis and surveillance." *Forensic Sci Int* 2 (2022): 100042.
13. Van Uhm, Daan P. and Rick CC Nijman. "The convergence of environmental crime with other serious crimes: Subtypes within the environmental crime continuum." *Eur J Criminol* 19 (2022): 542-561.
14. Duffy, Rosaleen V. and Dan Brockington. "Political ecology of security: tackling the illegal wildlife trade." *J polit ecol* 29 (2022): 21-35.
15. Harper, Cindy K. "Poaching forensics: animal victims in the courtroom." *Annu Rev Anim Biosci* 11 (2023): 269-286.
16. García Ruiz, Ascensión, Nigel South and Avi Brisman. "Eco-crimes and ecocide at sea: Toward a new blue criminology." *Int J Offender Ther Comp Criminol* 66 (2022): 407-429.
17. Gokhale, Chanchal, Ridamjeet Kaur and Bhavesh Mali. "Microbial Forensic–An Investigative Approach." *IJRESM* 5 (2022): 48-50.
18. Sun, Tao, Jie Song, Meng Wang and Chao Zhao, et al. "Challenges and recent progress in the governance of biosecurity risks in the era of synthetic biology." *Biosafety Biosecurity* 4 (2022): 59-67.
19. Zeng, Xiaomei, Hailun Jiang, Guangying Yang and Yakun Ou, et al. "Regulation and management of the biosecurity for synthetic biology *Synth Syst Biotechnol* 7 (2022): 784-790.
20. Castro, Arizaldo E and Maria Corazon A. De Ungria. "Methods used in microbial forensics and epidemiological investigations for stronger health systems." *Forensic Sci Res* 7 (2022): 650-661.
21. Pauwels, Eleonore. "How to Protect Biotechnology and Biosecurity from Adversarial AI Attacks? A Global Governance Perspective." Cham: Springer International Publishing (2023): 173-184.
22. Lee, Ying-Chiang J. Xuanqi Chen and Siddharth Marwaha. "The Need for Biosecurity Education in Biotechnology Curricula." *Biodesign res* 5 (2023): 0008.
23. Volevodz, Alexander G. Alexander N. Ivanov, Evgenyi S. Lapin and Denis S. Khizhnyak. "Forensic tools of obtaining and use of digital information in criminal procedure." *EpSBS* (2022).
24. Obioha, Jane Iveatu, Amaliya Princy Mohan and Habib Louafi. "Digital evidence collection in IoT environment." In Innovations in Digital Forensics (2023): 263-292.
25. Kebande, Victor R., Richard A. Ikuesan and Nickson M. Karie. "Review of blockchain forensics challenges." Cham: Springer International Publishing (2021): 33-50.
26. Reichel, Philip and Jay Albanese, eds. “Handbook of transnational crime and justice.” *SAGE* (2013). 27-26
27. Syaufi, Ahmad, Aurora Fatimatuz Zahra and Fatham Mubina Iksir Gholi. "Employing forensic techniques in proving and prosecuting cross-border cyber-financial crimes." *IJCC* 17 (2023): 85-101.
28. Anagnostou, Michelle and Brent Doberstein. "Illegal wildlife trade and other organised crime: A scoping review." *Ambio* 51 (2022): 1615-1631.

29. Cozine, Keith, Renee Graphia Joyal and Huseyin Ors. "From local to global: Comparing network approaches to addressing terrorism and transnational crime." *JPICT* 9 (2014): 117-134.

30. Williams, Lynne and Andrew J. Campbell. "Technology, ethics, and elements of pervasive digital footprints." In Exploring Ethical Problems in Today's Technological World (2022): 234-248.

How to cite this article: Ganechary, Pavan Kumar and Kollam Anjali. "Anticipating Future Crimes: The Role of Forensics in Addressing Emerging Threats in the Next Decades of the 21st Century." *J Forensic Res* 15 (2024): 615.