Pakistan Journal of Criminology
Vol. 16, No. 04, October—December 2024 (701-721)

Evaluating UK Legislation Effectiveness in Prosecuting Cybercriminals and Deterring Cybercrimes: Identifying Areas for Improvement

Bader A. J. Al-Rajhi[1]

Abstract

This paper discusses the effectiveness of UK legislation in prosecuting cybercriminals and deterring cybercrimes, highlighting the importance and impacts of cyberspace and IT systems on the UK economy and society. The digital economy is among the most critical components of the UK economy; hence, any disruption is likely to impact the economy significantly. Securing UK cyberspace is necessary to safeguard national security as modern society relies on the Internet for various services and communication. After identifying risks and threats to cyberspace, the paper presents a discussion of the theory of punishment for cybercrimes, including deterrence theory, retribution, and restorative justice. Case studies are presented to demonstrate the use of legislation (e.g., Computer Misuse Act and Data Protection Act) and its effectiveness as well as identify areas for improvement and offer recommendations considering legislative reforms and investment in cybersecurity initiatives. Finally, UK legislation will be compared with other nations' legislation to identify additional areas for improvement.

Keywords: Cybercrimes, Cybersecurity Strategy, Data Protection, Punishments Theory, UK's Cyber Legislation, Legislative Gaps.

Introduction

Functioning information technology systems and cyberspace are essential for today's society and economy, leading cybercriminals to target cyberspace. Cybercrimes are becoming increasingly sophisticated as technology advances. Pawar et al. (2021) defined cybercrime as criminal acts that employ computers and the Internet. These crimes encompass hacking, phishing, identity thefts, cyberbullying, ransomware attacks, and the distribution of child-perverse material (Khosrow-Pour, 2020). The primary common factor is that these crimes exploit vulnerabilities to breach, intrude upon, or interfere with the privacy rights of an individual, organization, or nation for monetary profits, sabotage, or mere pleasure (Verma & Shri, 2022).

[1] Bader A. J. Al-Rajhi is an Assistant Professor of Criminal Law, Kuwait University, Faculty of Law, Criminal Law Department. Email:dr.alrajhi@outlook.com

Cybercrimes have become one of the greatest threats to the UK economy in recent years due to the country's advanced status and the population's strong dependence on digital technology in various spheres of life. Successful cybercrimes cause financial loss to individuals and businesses. According to ISP Beaming, more than 1.5 million UK enterprises fell victim to threat actors in 2023, resulting in a financial loss of almost £31.5 billion (Muncaster, 2024). According to the International Monetary Fund's (IMF) *Global Financial Stability Report* published in 2024, the global financial sector has experienced 20% more recorded cyber events in the last 20 years, resulting in direct losses of $12 billion for financial firms. These figures demonstrate the desperate need to ensure more effective security for the economy's financial growth and the well-being of individuals using digital services. This paper assesses the effectiveness of UK legislation in prosecuting cybercriminals and deterring cybercrimes, identifying areas for improvement.

Research Objectives

The digital economy is among the most critical components of the UK economy; hence, any disruption is likely to impact the economy significantly. Securing UK cyberspace is necessary to safeguard national security as modern society relies on the Internet for various services and communication. Therefore, the objective of this research is to discuss the effectiveness of UK legislation in prosecuting cybercriminals and deterring cybercrimes, highlighting the importance and impacts of cyberspace and IT systems on the UK economy and society.

Research Methodology

This research employed a qualitative approach to evaluate the effectiveness of UK legislation in prosecuting cybercriminals and deterring cybercrimes. The extensive review and analysis of legal texts, case law, government reports, and relevant academic literature included the critical examination of key legislative frameworks, such as the Computer Misuse Act 1990 and the Data Protection Act 2018, to assess their strengths and limitations. A thematic analysis identified recurring patterns and challenges in the enforcement of these laws, focusing on gaps in the legal framework, jurisdictional issues, and the evolving nature of cybercrime. This approach provided a deep understanding of how the current legislation operates and where improvements are necessary.

Importance of Cyberspace to the UK

a. Economic Impact

The digital economy, including online retail, is a fundamental component of the UK economy, contributing £227 billion in gross value added (GVA) and sustaining more than 2.6 million jobs. The average salary in the digital sector is approximately £45,700 per annum, which is £12,000 (37%) more than the overall salary of £33,400 in the UK (Corfe & Dupont, 2024). During the COVID-19

pandemic, the digital economy grew as everyone shifted from using physical cash and documents to mobile money. The current estimations for the UK government's overall expenditures on COVID-19 measures vary between £310 billion and £410 billion, or approximately £4,600 to £6,100 per individual (Brien & Keep, 2023). Cloud computing, artificial intelligence, and Internet of Thing (IoT) devices are among the technologies that have helped advance economic growth. The UK's digital economy is diverse, including infrastructure and IT services, software, and computer services. Provisional projections for 2022 indicated that the digital sector contributed £158.3 billion to the UK GDP (GOV.UK, 2024), underscoring the importance of digital space and its impact on the UK economy.

b. National Security

Many aspects of the UK's critical infrastructure, ranging from health and energy to transportation, rely on interconnected digital networks, thereby being at significant risk to cyber threats. Cybersecurity threats are real, and the strong possibility of shutdowns of essential services and systems should worry the general public and national defense. If hackers target a nation's infrastructure, it could lead to societal breakdown, economic downturn, and a huge loss of lives.

The WannaCry ransomware attack in 2017 demonstrated the importance of securing cyberspace in the UK. Following this attack, thousands of appointments and surgeries were canceled, emergency services were disrupted, and the National Health Service's functioning was substantially hampered (Collier, 2017), disrupting at least 34% of trusts in England. The health service incurred an estimated cost of approximately £92 million due to the loss of services (Joint Committee on the National Security Strategy, 2023). The WannaCry attack targeted organizations' unpatched systems, highlighting the importance of cybersecurity and system updates while demonstrating the catastrophic risks that cyber offenders pose to lifeline industries and the need to improve cybersecurity.

c. Social Impact

Cybercrimes significantly affect society. With modern society utilizing a wide range of online services for communication, banking, shopping, and, arguably, all other spheres of human life, it is essential to ensure that such services are as secure as possible. Digital risks (e.g., cybercrimes, hacking, scams) reduce public confidence, discouraging the use of innovative innovations to support digital change (Johnson, 2016). The importance of safeguarding individual data to preserve the industry's popularity among consumers cannot be overstated.

Privacy and data protection are two broad parts of cybersecurity with profound implications for people's lives (Verma & Shri, 2022). As more consumers share their data online, protecting this information from attempted hacks and misuse is essential. Data protection measures guard personal information against identity

theft and other financial fraud and prevent cybercrimes that undermine customers' livelihoods (Niami, 2022). The Data Protection Act 2018 and other legislation, such as the General Data Protection Regulation (GDPR), are a crucial part of the UK's legislation and are responsible for safeguarding citizens' rights and privacy and ensuring that organizations take appropriate measures when handling personal data (Ducato, 2020).

Cyberspace occupies a significant space in the UK's economy, security, and stability. Digitalization remains an essential part of the economy as it supports the employment of millions and contributes hundreds of billions to the country's GDP. Comprehensive security measures can mitigate the threats. The four key pillars of the UK's cybersecurity strategy include defending national infrastructures, applying security for success in digital services, protecting individual privacy, and protecting data (HM Government, 2022).

Types of Cybercrimes and Their Impacts

a. Identity Theft and Fraud

Identity theft and fraud encompass many criminal activities in which an individual illicitly acquires and exploits someone else's personal information by fraud or deception, usually for financial benefit (Ahmed, 2020). Identity theft and fraud refer to the use of a victim's personal information, such as social security numbers, credit card details, or other official documents, for unauthorized operations like making purchases, withdrawing money from bank accounts, or getting credit cards (McCoy & Hanel, 2018). Cybercriminals use tactics such as phishing emails, malware, social engineering attacks, and leaked databases. For example, emails or messages appearing to originate from organizations or persons with whom the intended victim has had previous relationships induce the victim to reveal personal information, including credit card details. Meanwhile, malware can capture information without the owner's consent, and social engineering uses human behavior to make the victim reveal the secrets that the hacker desires.

The TalkTalk data breach in 2015, a famous example of identity theft and fraud in the UK, resulted in unauthorized access to approximately 157,000 customers' personal information, including bank account numbers, and more than 15,000 users' sort codes (BBC, 2019a). The company suffered hefty losses and experienced a negative image internally and externally. Impacted customers suffered an emotional toll. Based on a FICO report, approximately 1.9 million individuals in the UK, or 4.3% of the population, admitted that their personal information had been unlawfully obtained and exploited to establish financial accounts in 2023 (Bîzgă, 2024), demonstrating that identity theft and fraud are major cybercrimes in the UK.

b. Hacking

Hacking is the unauthorized and malicious use of devices (e.g., computers, smartphones, tablets, networks) to intentionally harm or manipulate systems, collect user information, unlawfully acquire data and documents, or disrupt activities linked to data. It aims to compromise the integrity of a computer system or network and its utility to individuals when a person with no right to access the system does so (Khosrow-Pour, 2020). Hackers employ penetrate different system passes in many ways, including prevailing on software chinks, brute force, and social-engineering techniques. Cybercriminals and hackers may steal usernames, passwords, credit card information, and corporate secrets and use malware to vandalize or carry out denial-of-service attacks. Some hack into corporate data networks or government databases.

In the 2018 British Airways data breach, hackers injected code into the airline's website and mobile application, collecting users' personal information (e.g., names, addresses, email addresses, credit card numbers), resulting in regulatory investigations, claims, and substantial fines for British Airways. The Information Commissioner's Office (ICO), the UK's data protection regulator, originally planned to impose a £183.39 million ($230 million) fine on British Airways (BBC, 2019c), although it reduced the fine to £20 million ($25 million) in 2020—still a significant penalty (Tidy, 2020). The event caused extensive loss of customer confidence and doubts about airlines' measures to secure transactions. It showcased the need for high-security standards to ensure safe surfing and protect customers' information from unauthorized access to the various digital platforms.

c. Cyberterrorism and Espionage

Cyber espionage is a danger to national security as it involves using computer systems and technology to attack government and private properties and steal vital information. Cyberterrorism, a subcategory of cyberwarfare, leverages computer technologies to support terrorist operations to influence public opinion, destroy critical infrastructures, and cause a loss of lives (Macdonald et al., 2022). Cyberterrorism refers to using the Internet and other information and communication technologies to intimidate or cause physical harm to acquire political or ideological influence through threats or intimidation (Blakemore 2016). Cyber espionage refers to a cyber spy's cyberattack to illicitly access, steal, or disclose classified information or intellectual property (IP) to obtain an economic, political, or competitive edge within a business or government environment (Buchan, 2019). Espionage differs from infiltration as it is the secretive acquisition of information deemed strategic for political, military, or economic objectives.

Russia's alleged interference in the UK's 2019 general election is an excellent example of cyberterrorism and espionage (BBC, 2020). Although the evidence

remains questionable, reports and concerns have emerged about state actor-sponsored cyberwarfare, especially in Russia, targeting the UK's democratic processes through, for example, cyber-sabotage (e.g., hacking political party databases), cyber-propaganda (e.g., spreading fake news through social media), and cyber-spying (e.g., accessing sensitive information regarding political candidates and/or policies). For instance, in 2023, the government alleged that the Russian intelligence service successfully infiltrated the private talks of prominent politicians and public servants to disrupt political activities in the UK (Vaughan, 2023). That another country can hack and gain unauthorized access to sensitive UK government information demonstrates the need for strong cybersecurity measures.

d. Cyberbullying and Harassment

Cyberbullying and harassment refer to the targeting of people on digital platforms to cause harm, whether physical or in the form of emotional distress (Stevens et al., 2021). Certain extreme cases have serious social and psychological impacts. Compared to normal bullying, cyberbullying may be done anonymously and share the information with more people, thereby worsening the situation. Cyberbullying victims are likely to develop depression, anxiety, and low self-esteem and may even be confined to social isolation, thus experiencing long-term effects of psychological mishaps (Santre, 2023). The National Centre for Social Research found that 47% of adolescents reported experiencing bullying when they were 14 years old (National Bullying Helpline, 2014). Due to the integration of technology in communication, such activity has become widespread, because perpetrators can trail victims and get personal information about them.

Ransomware and Malware

Ransomware and malware are new-generation cyber threats that can cause significant losses to individuals, companies, and other organizations. Ransomware is malicious software that obstructs access to a computer or its data and then demands that the user to pay ransom to access files (Patel & Tailor, 2020). UK firms incurred a staggering £30.5 billion in losses in 2023 due to cybercrime, emphasizing the significant financial, operational, and reputational consequences of ransomware assaults (Hasek, 2024). Malware harms a computer system through viruses, worms, Trojans, and spyware (Johnson, 2016) that infect systems, obtain confidential information, interfere with productivity, and require expensive fixes for victims.

Philosophy of Punishments for Cybercrimes

a. Deterrence Theory

Deterrence theory postulates that negative consequences can demoralize lawbreakers and, thus, discourage them from criminal conduct (Drucker & Gumpert, 2000). Deterrence can prevent the perpetration of cyber offenses and deter individuals from engaging in cybercrime by applying sanctions that exceed a

culprit's gains from indulging in the crime. Sanctions can include criminal remedies (i.e., fines or imprisonment) or civil remedies that impose social embarrassment or unbecoming societal images (Buchan, 2019). Deterrence is based on the pillars of certainty, severity, and swiftness of punitive measures to provide authorities with coercive measures to prevent a criminal act.

Considerable debate has centered around how well deterrence works when applied to cybercrime due to the specificity of computer crimes and issues of culpability and supervision (Drucker & Gumpert, 2000). Whereas other types of crime are more or less limited by geographical location, cybercrime is difficult to combat due to factors such as the anonymity of the Internet and technological advances outpacing legislative remediation. Although deterrence might not be definitive in combating cybercrime, it nevertheless discourages engagement in cybercrimes due to legal consequences and incorporates an ethical theory for a self-regulated society that will not condone cyber misconduct. Yet non-treatment measures should be backed by other methodologies, such as prevention, detection, and rehabilitation, to effectively counter the core reasons behind cybercriminal conduct.

b. Retribution

Justice is a sociopolitical theory posited from the idea of fair recompense for a wrong done resulting from moral culpability (Drucker & Gumpert, 2000). Deterrence posits that offenders must be punished commensurate with the harm they caused to society; the punishment should not consider any potential ripple effect. Revenge-brought justice aims to ensure that social order is maintained by avenging injustice and repaying the harm done. In the social context of cybercrimes, retribution underlines offenders' legal, social, and ethical obligations and considers their guilt and legally punishable conduct for the loss and damage they cause to both victims and society.

Many examples show retribution being used to prosecute and punish cybercriminals and make them answer for their actions, such as the arrest of several hackers who stole sensitive data during the Equifax data breach in 2017 (Federal Trade Commission, 2022) or the Yahoo data breaches in 2013 and 2014 (Daswani & Elbayadi, 2021). These cases led to criminal charges, heavy fines, and imprisonment, showing that hackers cannot escape the law. Similarly, when people participate in cyber espionage, piracy, or conning, these cases confirm the moral and ethical justification for retribution as a check on justice and the law in cyberspace.

c. Restorative Justice

Restorative justice focuses on airing grievances, renegotiating social relationships, and achieving accountability by involving victims, offenders, and the

community (Reyneke, 2019). Whereas conventional justice systems are based on punishment and demand retribution, restorative justice aims at reintegrative shaming and punishment to reduce the crime rate by restoring the harm done by a crime (Kirkwood, 2021). To implement restorative justice in cybercrime cases, all parties involved must be identified in order to collect all their requirements and foster a shared commitment to proactively thwarting and halting cybercriminal activities (Robalo & Abdul Rahim, 2023). Hence, this form of justice may not effectively combat cybercrimes in the UK.

Several benefits can be derived from restorative justice means for cybercrime victims as cyberspace offenses also cause emotional, financial, and psychological impacts. When victims can vent how they feel, narrate their experiences, and participate in decision-making processes, restorative justice can help disempower them and return them to normalcy (Daswani & Elbayadi, 2021). Furthermore, restorative justice aims to help victims and offenders find solutions; its main focus is to make victims and offenders communicate to understand each other and find closure (Saputra et al., 2022). It can save victims from the trauma of victimhood and give them hope for change. A Department of Education report rated whole-school restorative approaches as having the highest performance for avoiding bullying. A school poll revealed that 97% considered restorative approaches beneficial (Anti-Bullying Alliance, 2024). Moreover, restorative justice can enhance community harmony and social compliance because the parties in conflict and community members are involved in resolving cases and preventing the occurrences of further mistreatment (Daswani & Elbayadi, 2021). When applied to cybersecurity, restorative concepts can help policymakers, practitioners in criminal justice, and victim-support organizations foster more humane and diverse approaches to combating cybercrime that are sensitive to victims' needs while ensuring offender accountability.

UK Legislation

a. Computer Misuse Act 1990

The Computer Misuse Act 1990's primary objective is to safeguard the integrity and security of computer systems and data by criminalizing unauthorized access (Wang et al., 2023). The legislation makes the following illegal:

- Unlawful access to computer systems (hacking)
- Unauthorized access with the intent to commit other crimes
- Unauthorized modification of data
- Engaging in the creation, distribution, or acquisition of any item that can be utilized in committing computer-related crimes

It also outlines the consequences for offenders, who can be penalized through monetary fines, suspension or cancellation of licenses, or imprisonment based on

the severity of their offenses. The act also provides for law enforcement agencies to conduct investigations and prosecute cybercrimes effectively, protect critical assets, and safeguard national interests.

The Computer Misuse Act 1990 has been useful in readily defining manifestations of cybercriminal activities and empowering law enforcement agencies to prosecute offenders (Wang et al., 2023). Its subject matter is vast, as should be expected from an organization that deals with cybercriminals, targeting hacking, data breaches, and distributed denial-of-service (DDoS) attacks as examples of cyber threats. However, some have complained about the act's outdated language and its failure to capture more contemporary threats, such as cyber-espionage, ransomware, and insider threats (Saputra et al., 2022). Furthermore, the specificity of the legislation, legal ambiguity, and controversies over inequalities in the application of penalties have raised questions about the act as a viable deterrence to cybercrime in order to safeguard digital assets.

b. Data Protection Act 2018 and General Data Protection Regulation

The Data Protection Act 2018 and GDPR are among the most important legal instruments for data privacy and protection within the UK and the EU (Hoeren & Pinelli, 2020). These laws govern organizations' treatment of personal data and require controllers and processors to comply with certain principles to lawfully and transparently process data subjects' information. They enable individuals to process, correct, and delete personal data while organizations can apply the necessary technical measures and organize and protect data from access, disclosure, or misuse. UK firms' noncompliance with the DPA 2018 can result in fines of up to £17.5 million or 4% of their annual global sales (de Chazal, 2024). Organizations noncompliant with the GDPR may face penalties of up to £17.5 million or 4% of their total yearly revenue, whichever is higher. Businesses may incur fines regardless of whether they experience a cyberattack or data breach if they do not establish sufficient security measures for third-party data access (Watkins, 2024).

c. Cybersecurity Information-Sharing Partnership

The Cybersecurity Information-Sharing Partnership (CISP) is a joint public–private sector-driven program in the UK focused on threat information and prevention measures shared among government departments and agencies, police forces, and private companies (Zabierek et al., 2021). CISP offers a facility for the real-time information exchange about threats and potential dangers detected across the country to foster collective efforts in threat identification, prevention, and responses to threats and incidents. In particular, CISP facilitates the sharing of reliable information among UK cybersecurity industry members and fosters collaboration between them and the government, thereby improving the efficiency of the UK's cybersecurity market in dealing with various threats.

Overall, CISP has been positively received primarily due to its ability to foster cooperation and promote information sharing among stakeholders as well as ensure an effective collective response to cyber threats. CISP allows members to share threat intelligence, trends, and solutions, which helps organizations better view their environment, see what threats are evolving, and adopt appropriate protective measures. In addition, CISP helps establish the needed trust and collaboration between the government and groups involved in fighting cybersecurity threats. However, several issues need to be addressed, such as the optimization of the sharing of updated information within a short timeframe, legal and regulatory restrictions, and the expanded participation of actors from different sectors (Zabierek et al., 2021).

d. Investigatory Powers Act 2016

The Investigatory Powers Act 2016, also known as the Snoopers' Charter, is a very contentious law that gives the police and intelligence agencies broad powers to collect and intercept communications for security and investigation purposes (Curtis & Oxburgh, 2023). Under the act, communications data can be acquired in large quantities, communications can be intercepted, and electronic equipment can be tampered with by the relevant government agencies to conduct investigations pursuant to a warrant. Supporters have vehemently argued that the act is necessary given the challenges posed by terrorism and other heinous crimes in order to enhance the security within the country. Possible weaknesses of this policy are a lack of respect for individuals' freedom of privacy, legal concerns, no assessment-nuisances and balanced policies, and the tendency for government agencies to capitalize on the policy.

The highly invasive and wide-ranging nature of the act's provisions governing surveillance led to its swift and passionate dislike among privacy advocates, civil liberties enthusiasts, and technology firms, who have also raised the alarm over privacy, the freedom of speech, and the warrantless collection of data. The act denies those rights to individuals. Criticism has also arisen from the lack of judicial oversight, the scanty precautions taken regarding preserving personal data, and the state's misuse of surveillance prerogatives. Disputes concerning the act have also brought about challenges related to human rights legislation, constitutional rights and freedoms, and the right to privacy concerning international terrorism in the era of technology and cyberspace.

e. Telecommunications (Security) Act 2021

The Telecommunications (Security) Act 2021 is complex legislation aimed at enhancing the protection of several mobile companies in the UK. This legislation, which amended the Communications Act of 2003, is enforced by Ofcom and supported by the NCSC (Legislation.gov.uk, 2021). This act aims to strengthen the

UK communications infrastructure to protect it from cyberattacks, enhancing network security and resilience. The act encompasses several important provisions:

- **Procurement and Security:** The Procurement and Security Department oversees telecommunication providers' acquisition of infrastructure and services focusing on 5G networks. It aims to ensure robust software, equipment, and data safeguards.
- **Monitoring and Access:** The act mandates that communication service providers (CSPs) monitor network activity and access to identify and counteract cyber threats.
- **Security Investments:** The act requires CSPs to monitor and disclose their investments in security and data protection.
- **Incident Reporting**: Service providers must swiftly notify stakeholders of data breaches and cyber events.

Noncompliance with the act entails potential penalties for UK mobile carriers and broadband service providers amounting to £117K per day or 10% of their annual revenues (Kron, 2024). The aim is to ensure that mobile carriers and broadband service providers strive to combat cybercrimes and protect UK residents from cybercrimes.

f. Changes in Legislation

In recent years, few changes have been made to the UK cybercrime legislation to fight against circulating cyber threats and develop cybersecurity measures. Some of the laws revised include the Computer Misuse Act 1990 to increase penalties for cybercrimes, data protection laws to meet GDPR standards, and surveillance laws to address shortcomings, including the lack of transparency and accountability. For instance, in 2021, the Home Secretary declared an examination of the Computer Misuse Act 1990. The initial assessment stage involved a public call for information to gather input from stakeholders and the general public to identify and comprehend activities in the act's jurisdiction that may be causing harm and are not effectively addressed by existing offenses (GOV.UK, 2023). New legislation, including the Online Safety Bill and the National Cyber Strategy, has been enacted to address some of the regulatory challenges resulting from harms within online spheres, cybersecurity readiness, and security. The Online Safety Bill establishes a fresh obligation for online platforms to proactively address illegal and potentially "harmful" content their users generate (Rahman-Jones & Vallance, 2023). The Cyber Security Strategy of the Ministry of Justice outlines a plan for ensuring that every essential function within the department be capable of withstanding cyberattacks. The objective is to integrate the mindset of "Secure by Design" into all department activities, guaranteeing that all individuals can competently fulfill their security obligations (Ministry of Justice,

2023). These changes and initiatives aim to maintain the UK's responsiveness to cybercrimes.

Legislation Effectiveness

The Government Cyber Security Strategy 2022 to 2030 has been predominantly successful despite not being fully implemented. The strategy, which provides a plan for the UK government to build a cyber-resilient public sector (HM Government, 2022), is significantly more comprehensive than its predecessor. The previous 2016 plan focused on cyber as a security concern, with efforts to protect the UK from cyberattacks, discourage hostile individuals or groups, and foster the growth of the UK cybersecurity sector. The strategy has positioned the UK in global cybersecurity rankings, establishing it as one of the leading countries well-equipped to handle a cyberattack (Madnick, 2023). Most major cybersecurity incidents that have affected the UK have demonstrated the country's responsiveness and dedication to combating cybercrimes. These cases enforce justice by punishing those who perpetrate cybercrimes, deter other potential offenders, strengthen public confidence in the police force and other regulatory agencies, and protect cyberspace.

The prosecution of individuals involved in large-scale data breaches, cyber-espionage, or any other advanced Internet crimes requires policies, members of law enforcement agencies, and even lawyers. For instance, the TalkTalk cyberattack in 2015 facilitated the successful prosecution of hackers to support increased and effective cybersecurity measures, including comprehensive response procedures among the private sector firms and the police. Daniel Kelley was sentenced to four years in jail for his involvement in the incident (BBC, 2019b). Likewise, three individuals believed to be espionage agents working on behalf of Russia in the UK were apprehended and charged (BBC, 2023). However, the number of cybercrimes continues to be high in the UK. The government's Cyber Security Breaches Survey 2024 disclosed that 50% of UK firms had experienced a cyberattack or security breach within the preceding 12 months—an increase over the reported 39% in 2022 (TwentyFour IT Services Ltd., 2024). Thus, cybercrimes remain a considerable challenge despite the successful steps taken to address them.

A. Challenges in Prosecution

Despite the growing number of cybercriminals apprehended and tried in the courts, key challenges remain when enforcing cybercrime legislation and punishing offenders. Indeed, numerous barriers exist, including jurisdiction, technical issues, and evidence presentation, which can be significant hurdles in the prosecution process (Leukfeldt et al., 2017). A jurisdictional dispute arises when cybercriminals commit crimes across jurisdictions; it becomes highly complex to determine which law applies and in which jurisdiction the criminal will be prosecuted for crimes

committed on the Internet. Sometimes the technical nature of the attacks makes it difficult to investigate and collect the necessary evidence due to factors like encryption, anonymization, and obfuscation methods used by cybercriminals. Proving intent, attribution, and causation in cybercrimes is complex, and certain issues must always be addressed, such as the preliminary evidence, to give the legal proceedings their evidentiary foundation. This needs professional efforts and high-tech devices and tools.

b. International Cooperation

International partnerships are necessary due to cybercrime's transnational character and issues, such as jurisdictional strife in prosecution. Treaties, conventions, agreements, and measures provide for extradition, information sharing, cooperation, and mutual assistance among independent states. For instance, the treaty on extradition between the UK and the United States explains the legal manner in which a suspect believed to have committed a crime in either of the two countries can be extradited from the other country to stand trial (Leukfeldt et al., 2017). Other international treaties and agreements include the Budapest Convention on Cybercrime and the Council of Europe Convention on Cybercrime, which establishes international standards according to which the members should operate to align the legal provisions on combating computer-related crimes (Le Nguyen & Golman, 2021). Within these treaties, the countries agree upon protocols to deal with cybercriminals, exchange information, and enhance security. These treaties address the means by which nations can strengthen their laws and regimes in addressing cyber risks and improve regional and international stability and security. However, an extradition treaty does not automatically ensure the extradition of an individual to the government making the request. Indeed, the UK denied the extradition of Lauri Love, a British hacker, to the United States (BBC, 2018).

Potential Areas for Improvement

a. Legislative Gaps and Loopholes

Examining the weak points and legal lacunae in present-day cyberspace laws to mitigate deficiencies and improve coherent legal frameworks to curb digital-related crimes is essential. First, charging cybercriminals is more complex than charging individuals engaged in other crimes. The Gary McKinnon case best shows the difficulties in bringing forth cybercrime prosecutions. British hacker McKinnon was arrested in 2001 and 2002 for breaking into 97 systems operated by NASA and the US military. Because the crime was committed in the UK while the targets were in the US, the case was beset with jurisdictional problems that complicated the choice of the appropriate country for prosecution (BBC, 2012). This made negotiating bilateral agreements and international law necessary and brought to light the difficulties in dealing with crimes that crossed national boundaries. In

objecting to the US's request for McKinnon's extradition, his defense team contended that his mental health issues—depression and Asperger's syndrome—would subject him to inhumane treatment and an excessively punitive sentence in the US. Consequently, the UK Home Secretary refused the extradition in 2012 on human rights grounds (Smith-Spark, 2012). This ruling demonstrated the challenges faced when pursuing cybercrimes compared to traditional offenses, the critical role of human rights considerations in extradition cases, and the possible inconsistencies between national and international law standards.

The TalkTalk data breach is another case that highlights the complex difficulties involved in pursuing cybercrimes. This case was difficult because teenagers were involved in the breach (Kunle, 2015), which required working within the juvenile justice system, where many factors differ from the adult legislation system. The case also presented questions relating to the division of corporate versus individual responsibility. Despite obvious complex legal issues regarding identifying the culpable hackers and the corporate entity in question, TalkTalk held a supreme role in safeguarding customers' information. This incident illuminated the increased threats of personal data breaches and the inadequacies of corporations in terms of cybersecurity regulation and responsibility toward consumers. The case also highlights the challenges of combining legal, ethical, and practical issues and underscores the complex requirements for prosecuting cybercriminals, particularly when minors and business data are involved.

Addressing cybercrimes presents more intricacy than traditional crimes due to various pivotal factors. Cybercriminals employ advanced techniques to execute illicit activities, thereby concealing their whereabouts and identities. The 2015 TalkTalk breach is a prime example of the need for sophisticated digital forensics to identify criminals. It was also difficult to determine the liability between the company and the hackers; because minors were accused of committing serious cybercrimes, it was difficult to determine the best way to charge them. International jurisdiction is another essential factor to be considered. As cybercriminals often cross international borders to commit crimes, extradition and international cooperation are required. However, the McKinnon case demonstrates the difficulties of dealing with such incidents. As these cases highlight, existing challenges and loopholes may make it difficult to combat cybercrimes in the UK; these challenges and loopholes must be identified to determine the best strategies and measures to improve the effectiveness of dealing with cybercrimes. This will help to develop laws and reforms that will combat cybercrimes.

b. Enhancing International Collaboration

Enhancing links with other countries is essential, as battling cyber threats and enforcing jurisdiction in computer crimes involve two or more sovereign

jurisdictions. International treaties and agreements grant jurisdiction cooperation for some problems, yet international collaboration should be strengthened concerning sharing information, legal assistance, and joint investigations (Le Nguyen & Golman, 2021). The EU model of cybersecurity, based on creating cybersecurity agencies, information exchange platforms, and common instruments for dealing with cybersecurity incidents, is an example of efficient cooperation (Rantos et al., 2020). Policies can help different states enhance the response mechanisms when policymakers improve diplomacy to ensure that everyone trusts each other by being transparent and interoperable in terms of being ready to respond to cyber threats that may affect similar countries.

c. Technological Advancements and Law

As new technologies are introduced, the application of laws becomes challenging, which requires applying the latest methods, such as predictive policing and artificial intelligence, to better deal with threats and enhance optimum cybersecurity. Predictive policing involves analyzing data and patterns within law enforcement databases with the help of machine-learning tools, which may help establish correlations that can identify and prevent potential cybercrimes. Enhanced cybersecurity technologies, including threat intelligence platforms, anomaly-detection systems, and artificial intelligence for automated incident response, can support human efforts, improve awareness of the situation, and decrease cybersecurity threats in real time (Santre, 2023). Policymakers can incorporate prospective sophisticated technical breakthroughs in the field into policy to create strong and research-based reactive and sustainable measures for managing cybercrime and its enforcement.

D. Strengthening Public–Private Partnerships

Strengthening partnerships between public sector departments and private institutions improves cybersecurity, facilitates threat information sharing, and fosters collaborative solutions. Organizations play a key role in security as they manage the network assets that hackers target. By collaborating with government agencies and cybersecurity experts, companies can access valuable information to enhance their defenses against cyber threats. Incentives such as tax cuts, legal protection, and regulatory leniency encourage businesses to invest in cybersecurity and report threats. Policymakers can further improve cybersecurity by fostering strategic collaboration with businesses and addressing multiple threats.

Conclusion

This paper has analyzed the legislation in the UK for prosecuting cybercriminals and preventing cybercrimes while also identifying areas that require improvement by discussing different laws and regulations, such as the Computer Misuse Act 1990, the Data Protection Act 2018 and GDPR, the CISP, and the

Investigatory Powers Act 2016 to evaluate the effectiveness of addressing cybercrimes. The paper also analyzed different cases to determine issues and opportunities for improvement in prosecuting cybersecurity offenses and building protection against them.

Overall, adequate measures exist in UK legislation to combat cybercriminals and prevent cybercrimes. However, there is still ample room for improvement to ensure comprehensive legislative and law enforcement frameworks and undertake enhanced bilateral and multilateral efforts. Nevertheless, legislation must be enacted to address the existing gaps, engage the international community in providing legal solutions, and modify the laws to address modern innovations and cybercrime challenges. Regarding accessibility, it is imperative that legislative efforts actively seek to address emerging risks, find ways to improve cross-border collaboration, and adapt new technologies to counter evolving threats from cybercriminals.

Cybercrime in the UK is a broad lens through which the retribution of economic, social, and national effects can be viewed. It continues to consume billions of pounds yearly and to destabilize organizations' operations, erode public confidence in digital services, and pose threats to the nation's structures and safety. Furthermore, cybercriminal activities impose devastating effects on persons, organizations, and groups, such as the loss of money, tainted image, and even post-traumatic stress disorder. Combating cybercrime is possible only by adopting multi-sectoral, legislative, cybersecurity, educational, and global partnership approaches.

Thus, to enhance cybersecurity and combat cybercrimes effectively, the following recommendations should be considered:

- **Policy and Legislative Reforms:** New laws should be enacted to close existing legal loopholes and amend existing legislation to incorporate provisions that address emerging cybersecurity threats.
- **Strategic Initiatives:** Investing in cybersecurity-related developmental frameworks and research is advisable to bolster reporting and forensic mechanisms and increase social awareness and preparedness.
- **Emerging Trends and Technologies:** Policymakers should monitor advances in other relevant fields, including artificial intelligence, quantum computing, and the Internet, to evaluate the impact they might have on cybersecurity. Laws should be enacted and reformed to accommodate emerging technologies and trends.
- **Policy and Legal Analysis:** Cybercrime laws and policies should be compared and contrasted across jurisdictions to identify areas that need improvement and what can be borrowed from other jurisdictions.

References

Ahmed, S. R. (2020). *Preventing identity crime: identity theft and identity fraud: an identity crime model and legislative analysis with recommendations for preventing identity crime*. Brill.

Anti-Bullying Alliance. (2024). *What is restorative practice?* https://anti-bullyingalliance.org.uk/tools-information/all-about-bullying/responding-bullying/restorative-practice/what-restorative#:~:text=The%20Restorative%20Justice%20Council%20said,rated%20restorative%20approaches%20as%20effective.

BBC. (2012, December 14). Profile: Gary McKinnon. *BBC News*. https://www.bbc.com/news/uk-19946902

BBC. (2018, February 19). Lauri Love case: US abandons extradition case. *BBC News*. https://www.bbc.com/news/uk-england-suffolk-43119355

BBC. (2019a, May 21). TalkTalk data breach customer details found online. *BBC News*. https://www.bbc.com/news/business-48351900

BBC. (2019b, June 10). TalkTalk hacker Daniel Kelley sentenced to four years. *BBC News*. https://www.bbc.com/news/uk-wales-48587207

BBC. (2019c, July 8). British Airways faces record £183m fine for data breach. *BBC News*. https://www.bbc.com/news/business-48905907

BBC. (2020, July 16). "Almost certain" Russians sought to interfere in 2019 UK election – Raab. *BBC News*. https://www.bbc.com/news/uk-politics-53433523

BBC. (2023, August 15). Suspected spies for Russia held in major UK security investigation. *BBC News*. https://www.bbc.com/news/uk-66504350

Bîzgă, A. (2024). *Nearly 2 million Brits say they fell victim to identity theft crimes in 2023*. https://www.bitdefender.com/blog/hotforsecurity/nearly-2-million-brits-say-they-fell-victim-to-identity-theft-crimes-in-2023/

Blakemore, B. (2016). *Policing cyber hate, cyber threats and cyber terrorism*. Routledge.

Brien, P., & Keep, M. (2023). *Public spending during the Covid-19 pandemic*. House of Commons Library.

Buchan, R. (2019). *Cyber espionage and international law*. Hart.

Collier, R. (2017). NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal, 189*(22), E786–E787.

Corfe, S., & Dupont, J. (2024). *State of the UK digital economy*. Computer & Communications Industry Association.

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in "real world" policing and law enforcement. *The Police Journal, 96*(4), 573–592.

Daswani, N., & Elbayadi, M. (2021). *Big breaches: Cybersecurity lessons for*

everyone. Apress.

de Chazal, E. (2024). 20 biggest GDPR fines of all time. *Skillcast.* https://www.skillcast.com/blog/20-biggest-gdpr-fines

Drucker, S. J., & Gumpert, G. (2000). Cybercrime and punishment. *Critical Studies in Media Communication, 17*(2), 133–158.

Ducato, R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review, 37*.

Federal Trade Commission. (2022, December). *Equifax Data Breach Settlement*. Federal Trade Commission. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

GOV.UK. (2023, November 14). *Review of the Computer Misuse Act 1990: consultation and response to call for information (accessible)*. https://www.gov.uk/government/consultations/review-of-the-computer-misuse-act-1990/review-of-the-computer-misuse-act-1990-consultation-and-response-to-call-for-information-accessible

GOV.UK. (2024, September 3). *Digital sector economic estimates gross value added 2022 (provisional)*. https://www.gov.uk/government/statistics/dcms-and-digital-sector-gva-2022-provisional/digital-sector-economic-estimates-gross-value-added-2022-provisional

Hasek, T. (2024). *The human impact of ransomware attacks: how can businesses protect their security professionals?* https://www.itsecurityguru.org/2024/03/22/the-human-impact-of-ransomware-attacks-how-can-businesses-protect-their-security-professionals/

HM Government. (2022). *Government cyber security strategy: Building a cyber resilient public sector*. https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

Hoeren, T., & Pinelli, S. (2020). The new Californian data protection law—In the light of the EU general data protection regulation. *SSRN Electronic Journal*.

International Monetary Fund. (2024). *Global financial stability report, April 2024*. IMF.

Johnson, M. (2016). *Cyber crime, security and digital intelligence.* Routledge.

Joint Committee on the National Security Strategy. (2023). *A hostage to fortune: ransomware and UK national security*. House of Commons and House of Lords.

Khosrow-Pour, D. B. A. (Ed.). (2020). *Encyclopedia of criminal activities and the Deep Web*. IGI Global.

Kirkwood, S. (2021). A practice framework for restorative justice. *Aggression and*

Violent Behavior, *63*(63), 101688.

Kron. (2024). *UK's Telecommunications Security Act (TSA) code of practice*. https://krontech.com/uk-s-telecommunications-security-act-tsa-code-of-practice.

Kunle, M. (2015, October 30). Second teenager arrested over TalkTalk cyberattack. *The Wall Street Journal*. https://www.wsj.com/articles/second-teenager-arrested-over-talktalk-cyberattack-1446208574

Le Nguyen, C., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, *40*(1), 105521.

Legislation.gov.uk. (2021). *Telecommunications (Security) Act 2021*. https://www.legislation.gov.uk/ukpga/2021/31/contents

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*, *67*(1), 39–53.

Macdonald, S., Jarvis, L., & Lavis, S. M. (2022). Cyberterrorism today? Findings from a follow-on survey of researchers. *Studies in Conflict & Terrorism*, *45*(8), 727–752.

Madnick, S. E. (2023). *The continued threat to personal data: Key factors behind the 2023 increase*. https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf

McCoy, E. L., & Hanel, R. (2018). *Identity theft: Private battle or public crisis?*. Cavendish Square Publishing, LLC.

Ministry of Justice. (2023). *Ministry of Justice cyber security strategy: 2023 to 2028*. GOV.UK.

Muncaster, P. (2024, February 13). UK businesses lose £31bn to security breaches in a year. *Infosecurity Magazine*.

National Bullying Helpline. (2014). *Cyberbullying and online harassment advice*. https://www.nationalbullyinghelpline.co.uk/cyberbullying.html

Niami, M. (2022). The urgency of authentication and protection of personal data in online transactions. *Law and Justice*, *7*(2), 196–212.

Patel, A., & Tailor, J. (2020). A malicious activity monitoring mechanism to detect and prevent ransomware. *Computer Fraud & Security*, *2020*(1), 14–19.

Pawar, S. C., Mente, R. S., & Chendage, B. D. (2021). Cyber crime, cyber space and effects of cyber crime. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *7*(1), 210–214.

Rahman-Jones, I., & Vallance, C. (2023, October 26). Online safety bill: divisive internet rules become law. *BBC News*.

https://www.bbc.com/news/technology-67221691

Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., & Katos, V. (2020). Interoperability challenges in the cybersecurity information sharing ecosystem. *Computers*, *9*(1), 18.

Reyneke, R. P. (2019). A restorative approach to address cyber bullying. In M. Kowalczuk-Walędziak, A. Korzeniecka-Bondar, W. Danilewicz, & G. Lauwers (Eds.), *Rethinking teacher education for the 21st century* (pp. 340–354). Verlag Barbara Budrich.

Robalo, T. L. A. S., & Abdul Rahim, R. B. B. (2023). Cyber victimisation, restorative justice and victim–offender panels. *Asian Journal of Criminology*, *18*(1), 61–74.

Santre, S. (2023). Cyberbullying in adolescents: a literature review. *International Journal of Adolescent Medicine and Health*, *35*(1). 1–7.

Saputra, R. A., Amrullah, R., Triono, A., & Refsi, B. (2022). Management of improvement of cyber crime at the time of the COVID-19 pandemic happening restorative justice. *Scholars International Journal of Law, Crime and Justice*, *5*(7), 286–293.

Smith-Spark, L. (2012, October 16). UK blocks hacker McKinnon's extradition to US. *CNN*. https://www.cnn.com/2012/10/16/world/europe/uk-us-mckinnon-extradition/index.html

Stevens, F., Nurse, J. R. C., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367–376.

Tidy, J. (2020, October 16). British Airways fined £20m over data breach. *BBC News*. https://www.bbc.com/news/technology-54568784

TwentyFour IT Services Ltd. (2024, September 5). *UK cybercrime statistics 2024*. https://www.twenty-four.it/services/cyber-security-services/cyber-crime-prevention/cybercrime-statistics-uk/

Vaughan, H. (2023). Russian hackers used "spear-phishing" to steal information from UK politicians, government says. *Sky News*. https://news.sky.com/story/russian-hackers-used-spear-phishing-to-steal-information-from-uk-politicians-13024300

Verma, A., & Shri, C. (2022). Cyber security: A review of cyber crimes, security challenges and measures to control. *Vision: The Journal of Business Perspective*, 09722629221074760.

Wang, Q. H., Geng, R., & Kim, S. H. (2023). Chilling effect of the enforcement of computer misuse act: Evidence from publicly accessible hack forums. *Information Systems Research*. https://doi.org/10.1287/isre.2019.0346

Watkins, L. (2024, April 9). UK ICO unveils new fine calculation guide for data

protection infringements. *Global Privacy & Security Compliance Law Blog.* https://www.globalprivacyblog.com/2024/04/uk-ico-unveils-new-fine-calculation-guide-for-data-protection-infringements/

Zabierek, L., Bueno, F., Kennis, G., Sady-Kennedy, A., Kanyeka, N., & Kolbe, P. (2021). *Toward a collaborative cyber defense and enhanced threat intelligence structure.* Belfer Center for Science and International Affairs, Harvard Kennedy School.