Pakistan Research Letter

Volume. 1 Issue No. 2 (2022)

# Legal Responses and Challenges to Cybercrime

1. Humaira Arshad, M.Phil. Scholar, Department of Law, University of Peshawar.
2. Ali Haidar, Lecturer, Department of Law, University of Haripur.

## Abstract

This paper investigates the legal responses and challenges related to cybercrime in the contemporary digital landscape. As cybercrime becomes increasingly prevalent, transcending borders and jurisdictions, it necessitates a comprehensive legal framework that can adapt to rapidly evolving technologies and criminal tactics. The study defines cybercrime, outlining its various forms, including traditional offenses like theft and fraud, as well as newer threats such as ransomware and identity theft. It examines the historical development of cybercrime laws, emphasizing the need for international cooperation and harmonization of legal standards to effectively combat these offenses. Key legal frameworks, such as the Council of Europe's Convention on Cybercrime, provide essential guidelines for member states and facilitate cross-border collaboration. However, significant challenges persist, including jurisdictional issues, the transient nature of digital evidence, and the increasing use of cryptocurrencies in criminal activities. The paper highlights the importance of proactive legal measures and international agreements to enhance cybersecurity efforts. Ultimately, it underscores the need for continuous adaptation of laws and policies to address the complexities of cybercrime, ensuring better protection for victims and society at large.

**Keywords:** Cybercrime, Legal responses, International law, Ransomware, Digital evidence, Jurisdiction, Cybersecurity, Cryptocurrencies, Cross-border cooperation

## 1. Introduction

Cybercrime is increasingly ubiquitous in the modern world; for some, it has become part of their daily lives. It is thus necessary to have familiarity with the legal responses and challenges inherent in dealing with it. The complexity of these offenses is exemplified by their ability to transcend borders without regard for jurisdictional issues. The framework, both transnational agreements and internal laws that deal with cyber offenses, is complex and always in a transitory state of growth. This is in part due to the ever-developing technology that facilitates these offenses, necessitating a corresponding development in legal response  (Kovalenko et al. 2022)

The apprehension and punishment of cyber offenders is not, of course, the only purpose or effect of law. The provision of legal remedies for those affected by cybercrime is also of significance, considering not only the immediate interests of victims but also the cost of cybercrime to society in general. The importance of dealing with this global issue together as nations cannot be underestimated, requiring good cooperation and harmonization of laws against cybercrime

### 1.1. Definition and Scope of Cybercrime

Cybercrime is criminal activity conducted using some form of computer technology or technology infrastructure, generally characterized by the use of the internet. Cybercrime is therefore likely to include traditional offline offenses such as theft, fraud, forgery, and may be national or international in nature or spill over into related crimes such as cyberbullying, stalking, and harassment or some sexual offenses. There are a wide variety of activities or criminal offenses that can be described as cybercrime.

Interconnectedness and complexity of thousands of simultaneous and recurrent criminal conduct commitments. Cybercrimes are of growing concern to governments, businesses, and individuals, both for the harm suffered by the victims of individual transactions (and to a lesser extent criminals) and also the credibility risks to national infrastructure development they represent. There is increasing awareness of the risk of identity theft to the general community and with the growing sophistication and stories of internet fraud. Despite this, there is no clear definition of cybercrime in legislation. This lack of a standard definition and the resulting classification requirements of such behavior can create difficulties in asking legal systems to respond, develop effective policy, and generally act in this space. If policymakers, police, and courts have worked with a particular definition of cybercrime, their ability to protect the community is likely to be eroded. There are, however, some features of cybercrime that are generally agreed upon by many commentators.

## 2. Historical Development of Cybercrime Laws

With the advent of technology in the late 20th century, the world has witnessed an explosion in the number of cybercrimes committed each year (Sviatun et al. 2021). Accordingly, nations have begun to recognize forms of online behavior as cybercrime and are proactively developing laws to combat them. Some of the earliest attempts to combat cybercrime included various legislative actions to address data protection and privacy concerns. From that time to the present, many laws have been passed to address cybercrime. In 1986, significant legislative actions were taken to address cybercrime.

Starting in the mid-1990s, as the Internet began to grow at an exponential rate, so too did the number of cybercrimes, including hacking, investment scams, and other online fraud. These crimes necessitated an international response, as criminal activity taking place over a global communications system needs to be addressed using international agreements, as online offenses can be committed from one country and victimize people in another. In December 2000, the first comprehensive attempt at a unified international response to cybercrime was made with the drafting of a model law on electronically stored information. That model was later expanded to include substantive criminal law and an annex on procedural law. When passed, the treaty became known as the Cybercrime Treaty. The treaty has set a number of standards for online behavior, providing the basis for necessary responses to Internet crime. This outlines the main landmark agreements to provide a response to cybercrime. The important date is 1999, with the drafting of a convention on cybercrime. With each of these high-profile events, lawmakers continued to take steps to improve legislation to combat cybercrime, identifying new activities or changing old laws in light of new events. Much of this change continues today as we adapt our laws to the ever-changing technology.

### 2.1. Early Legislation and International Cooperation

The regulation of cybercrime has taken several forms, shaped by a number of different sociopolitical concerns. In its early days, cybercrime legislation was often reactive, enacted as a response to some new cyber scare. In particular, early laws at the national level were often focused on issues relevant to physical world security. One of the first and still a landmark statute in the US is the Computer Fraud and Abuse Act. Indeed, the US has also set international standards in this field with the Privacy Protection Act and the Electronic Communications Privacy Act. There have been reactions around the world, leading to national regulations in many countries.

This intermittent national response to global challenges reveals characteristics of resistance as well as characteristics of a desire for greater control over information and data. As the number of incidents rose—with the structure, speed, and intensity that are peculiar to global networks—there were growing demands for an international solution to this international problem. A series of international binding agreements have been set in place in response to a rapidly evolving problem with distinct territorial implications of data crimes. The first steps have been to define offenses and establish some capacity in terms of investigations and prosecution tools. This implicitly means that we didn't have the necessary tools in place. Similar to national laws, the earlier agreements in the 1990s have met some severe criticisms. The major charges were that drafting had mainly aimed at imposing various national ideologies on cybercrime enforcement and that the treaties had breached international human rights standards. The key treaties are the Council of Europe Convention on Cybercrime, formally certified in 2001 (Koto, 2021).

These problems led to a serious delay before the treaty was of any real importance outside the Council of Europe territories. Although being a new international order, the emergence of a global system over time necessitates the contractual partner parties to the treaty swear a psychological and substantial oath in relationship. This requirement's primary objective is to metamorphose custom and usage, a scientific consensus, and intelligent solidarity, harmonizing international information society legal standards. The need for mutual assistance will also slow down investigations as well as legislation enforcement. But it is absolutely clear that tracking and prosecutive solutions must follow the global trends and the global movement of data. Since there are a variety of rules across nations and cultures, this need for mutual assistance will also involve conciliation regarding necessary homage and flexibility in the different legal procedures. When it comes to international investigations cooperation, the only worldwide consensus is that there is no solution, but only through agreement and global cooperation is it a subject inherently interwoven into the feasibility of national laws in the current information society and intensely vulnerable to change. International law specialists and interested parties should focus greater effort on establishing global partnerships in the new information fields built around the possibility of conflict lines. Only a cohesive framework for investigations and prosecutions will allow us to trace the path of the criminals through the global network.

### 3. Key Legal Frameworks and International Conventions

DRAFT: The Importance of Legal Responses to Cybercrime

Any comprehensive preventive response to criminal behavior from such a multi-faceted perspective has facilitated the multi-level division of labor in contemporary law enforcement. Illegal acts committed either in the course of the initial attack, or in the stage when crime is committed, can, broadly speaking, be governed by national laws, as stated above. On the other hand, cooperation regarding data that such attacks disclose or involve is a different matter. It is connected with several international legal instruments, each adopted for different reasons of international consensus. The criminal law and justice accompanying this multidisciplinary approach must enforce these three international legal frameworks, apart from the several regional declarations and recommendations that play a supplementary role.

Commentary International cooperation in the repression and prosecution of cybercrime is only possible, and effective, through the development of extensive, supra-national legal agreements. These include two main areas of work: (a) the harmonization of national laws to govern different types of criminality relating to digital technology, the internet, or breaches of computer system security, and to allow jurisdictions to be willing to cooperate and not to refuse extradition requests on the grounds that dual criminality does not apply; (b) the convention of legal agreements on guiding principles or best international practices, detailing what can or cannot be done in cyberspace. The Convention on Cybercrime is the key reference standard-setting text on how to govern behavior online, a universal text for all world states to follow and sign. It relies on a mixed model of law and best practice with multiple stakeholder input and represents best endeavors to act in good faith and cooperation between signatories. The Convention includes several of the legal principles that apply to criminal e-investigations (Alhadidi et al., 2020).

### 3.1. Council of Europe Convention on Cybercrime

In 2001, the Council of Europe created the permanent treaty named "Convention on Cybercrime" with the sole objective of strengthening the protection afforded to various societies against cybercrime, while facilitating international cooperation. Usually referred to as the Budapest Convention, it has become the pivotal legal framework to address the specific criminal challenges posed by global computer networks (Buçaj & Idrizaj, 2022). The convention aims to protect society against computer security threats through the criminalization of software piracy, but it also criminalizes a wide variety of conduct, ranging from some computer-related crimes to content-related crimes. In addition, it provides the legal tools for effective international cooperation by establishing specific procedures for swift international mutual assistance in the investigation and prosecution of any of those offenses, effectively combating most cybercriminal activities. Furthermore, it recognizes the need to harmonize, as much as possible, the criminalization and investigatory powers available to member states, bringing these in line with the best practices of the wider international community.

The importance of the Budapest Convention in addressing relevant practical enforcement issues related to jurisdiction, such as procedures for real-time data collection, the way to preserve data in the country of the service provider, or the precepts in relation to the protection of personal data, is so significant that they might serve as a tool to determine the real impact of a cyber security-related legal regime within a legal framework as well as within law enforcement forums. Surveys have measured the degree of regional or global compliance with global standards defined within the treaty (Halder, 2021). The work critically assesses the functioning of cross-jurisdictional inquiries within a global environment, providing two case studies that shed some light on the practical implications of these new procedures. This face-to-face analysis examines the reaction of two European states, Spain and Romania, to a potential international cybercrime in two cyber scenarios: the use of a computer virus to damage and disrupt a computer system and robot networks to launch DDoS attacks.

### 4. Challenges in Enforcing Cybercrime Laws

Despite advances in legal responses to cybercrime, the nature of this type of offending poses numerous challenges when dealing with enforcement. The characteristics of cybercrime are such that many are not detected. As a consequence, there is a dependence on the goodwill of reporting authorities. When reports are received, investigations are often complex. Such investigations are multijurisdictional in scope, and the necessary evidence can be very hard to find. This is particularly so as evidence online can be not only transient, but if necessary could be located at any place on a particular day. In many cases, having successfully identified a site containing necessary material, top-level sites can refer one through a myriad of other sites before the final site is located. These sites can be located in different jurisdictions, on different continents, and can involve language barriers. Governments can enter agreements under international conventions to aid mutual legal assistance. These sorts of agreements rely very much on the vagaries of international politics at the time a request is made.

Jurisdictional issues can have a direct impact on whether or not an offense can be successfully prosecuted. It should be remembered that just because a computer was in one jurisdiction when the act was committed does not in itself give jurisdiction to try the offense. Whether a prosecutorial authority chooses to take a case on also depends on a number of variables such as available resources, availability of relevant expertise, local criminal laws, and law enforcement priorities. Indeed, the laws in some jurisdictions may be such that offenses may fall under the category of nuisance and not be considered harmful. On the other hand, some jurisdictional lines can be blurred. For example, an internet user may access the internet through an ISP in a different country. He may be using a program which enables the user to hide a site so that law enforcement officers cannot find their true IP address, needed to locate somebody. Intergovernmental agreements may not have been set in place, and thus even obtaining something as relatively simple as subscriber details will take a long time to obtain. The goal of this paper is to examine the hurdles in law enforcement in the new technological age and to suggest ways forward in addressing those difficulties. It also examines the challenges in trying to balance privacy with protection for those involved in the new technological age.

**4.1. Jurisdictional Issues and Cross-Border Investigations**

A significant challenge facing cybercrime law enforcement is the matching of laws with physical territory. In many cases, a cybercriminal will seek to evade detection by launching attacks through compromised computers around the globe to hide their true physical location. Jurisdictional competition frequently prevents countries from cooperating in the investigation and prosecution of cybercrime. As cybercriminals often work from multiple locations across different countries, the situation has the potential to dramatically slow down and add complexity to cross-border investigations, and it is often difficult to determine which of the potentially numerous jurisdictions concerned should take the lead in an investigation (Minarosa, 2022).

International Treaties and Agreements: There are a number of bilateral and multilateral agreements that are aimed at assisting with the resolution of such jurisdictional conflicts, or that address issues associated with mutual assistance. Generally, these conventions require each party to adopt laws to deal with the types of conduct the parties have agreed should be criminal, typically focusing on crimes against computer information systems. The legal issues associated with cybercrime investigations are complex. General legal principles in relation to jurisdiction have been established in a number of agreements, many of which are based on the principle of harmonizing national jurisdiction. Some of the main principles governing jurisdiction are the territorial or objective principle, the nationality principle, the passive personality principle, the universality principle, the protective principle, the principle of extradition, and the principle of dual criminality.

It is difficult for most national legal jurisdictions to control cross-border law enforcement agencies. By harmonizing laws, conditions, and processes internationally, cross-border cooperation can be better managed, promoting more effective control. Several global organizations are active in the international fight against cybercrime. The seriousness and timing of the action in Malaysia and the subsequent decision by the Australian intelligence researchers to abandon the monitoring program are instructive of the effect that international tensions between signatories of legal instruments have on flows of intelligence and evidence in incidents of alleged computer misuse.

## 5. Emerging Trends in Cybercrime

The digitization of society led to the expansion of opportunities available for cybercriminals. In the past 15 years, numerous technological trends and societal changes have resulted in new cybercrimes. Many forms of cybercrime are fast becoming a major source of threat to ordinary citizens, corporations, and governments, yet do not receive adequate attention in criminology. Global data indicate that ransomware and attacks on cryptocurrencies, such as fraud, have become more common. Trends include not only the regular use of ransomware but also the targeting of critical infrastructure in Western countries. Similarly, cryptocurrencies have become not only tools for extortive attacks such as ransomware but are also used in international drug trafficking, the trade of images of sexual abuse of children, and schemes using a virtual private network to launder money. These attacks have become prevalent in many parts of the Western world and beyond. The relatively low cost and the availability of programs on the dark web make it easier for inexperienced criminals to try to launch attacks (Robalo & Abdul Rahim, 2021).

In recent years, cybercriminals have been increasingly able to build "trust" with their victims. For instance, many victims pay ransoms and get the promised decryption key. In "ransomware attacks," which have received much media attention, the attack may lead to considerable costs for the victim, including incident-response capabilities and public relations management. For businesses, the effects of these developments include face-to-face payment transactions or the use of bank branches and other financial services to avoid the use of technology where the crime was committed. It is particularly hard to combat such crimes due to the evolution of digital technology. New operating systems, social media platforms, or cryptocurrencies continuously challenge existing criminal laws and, most importantly, make it increasingly costly for law enforcement agencies to enforce them. In our digital age, when computer technology and cloud storage can be updated several times a year and algorithms for cryptocurrencies can be altered constantly, new technologies make policing streets significantly easier because they produce evidence in more sophisticated ways, but also make it harder to counteract cybercrimes. In turn, more attention is now being paid to "cyberintelligence" at the international level. These entities aim to preempt cybercriminal tactics that remain unfeasible for traditional reactive law enforcement. Discussing these strategies is important because they are likely to evolve alongside these emerging trends. They are solid tactics to preempt developing patterns and subsequently spill into the already existing approaches to combat cybercrime as an adaptive challenge (Agina, 2022).

### 5.1. Ransomware and Cryptocurrency

Ransomware is a particularly lucrative form of cybercrime. Using encryption, cybercriminals hold an organization's data hostage until a ransom—frequently in cryptocurrency—is paid. Unlike breaching a network to steal data, attackers need not then attempt to monetize the stolen data; rather, victims need to pay for the data to be decrypted. Ransomware cases also pose potential risks of broader social and economic impacts. The 2017 ransomware attack, for example, affected the normal operations of one-third of the United Kingdom's National Health Service trusts, resulting in the care of six thousand outpatients being disrupted, along with surgical procedures being postponed. The associated cleanup efforts incurred costs of cleanup estimated at £92 million. The more recent ransomware attack on the Colonial Pipeline, the largest refined products pipeline in the United States, resulted in the company shutting down operations for six days, causing fuel shortages in the eastern United States and rapidly rising gasoline prices. The company paid a ransom of 75 Bitcoins, valued at $4.4 million at the time the payment was made.

Another characteristic of recent ransomware attacks is their use of cryptocurrency. Experts agree cryptocurrency frequently appears as a realistic and feasible option, with insufficient address and response to date. "Almost all ransomware operators have moved from using banking systems and e-monies to cryptocurrencies" given their advantages. Following a general research approach, earlier research has noted the association of cryptocurrency with ransomware. The trend is seen particularly in "highly publicized attack campaigns," and has been seen "most recently" prior to the report's publication. The study shows a transition from 2018 by ransomware actors in favor of using cryptocurrencies such as Monero, which offers features that are likely to confuse the tracing of transactions on the blockchain. National governments see the same challenge posed by the increased use of Monero and Zcash in ransomware campaigns, which are both designed to provide private and untraceable transactions. These developments have proved particularly difficult for policymakers to address as tracking ransom payments has become "exceedingly difficult" given the privacy features unique to the cryptocurrencies, made evident by lower recovery of ransoms. By September of 2019, a firm alone assisted with over 350 ransomware incidents in which ransom payments in excess of US $100,000 had been demanded. Given the data, it is clear that this vector is not only widespread but also impactful. These data only account for those organizations that reported the incident, suggesting the actual figure is likely significantly higher (Musofiana, 2021).

**References:**

Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: economic and legal aspects. WSEAS Transactions on Business and Economics, 18, 751-762. academia.edu

Buçaj, E. & Idrizaj, K. (2022). The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews. malque.pub

Koto, I. (2021). Cyber crime according to the ITE law. International Journal Reglement & Society (IJRS), 2(2), 103-110. bundamediagrup.co.id

Robalo, T. L. A. S. & Abdul Rahim, R. B. B. (2023). Cyber victimisation, restorative justice and victim-offender panels. Asian journal of criminology. springer.com

Musofiana, I. (2021). Legal Protection For Victims Of Cybercrime In The Digital Era In Strengthening Cyber Democracy In Indonesia Post 2019 General Election. The 2nd International Conference And Call Paper. unissula.ac.id

Agina, E. M. (2022). Efficacy of the Cyber Security Legal Framework in Addressing Cybercrime: A Focus on Kenya. uonbi.ac.ke

Halder, D. (2021). Cyber victimology: Decoding cyber-crime victimisation. [HTML]

Alhadidi, I., Nweiran, A., & Hilal, G. (2020). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. Heliyon. cell.com

Kovalenko, V., Kryzhanovskyi, A., Kolb, O., Soroka, S., & Popadynets, H. (2022). Criminal law and forensic support in the fight against cybercrime. Cuestiones Políticas, 40(73). [HTML]

Minarosa, M. (2022, January). Legal Protection of Personal Data Owners as Cybercrime Victims Based on regulations regarding Electronic Information and Transactions. In Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia. eudl.eu