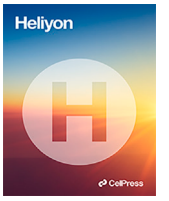
Heliyon 9 (2023) e22823

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon



Research article

How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan

Nadia Khadam [a,*], Nasreen Anjum [b], Abu Alam [b], Qublai Ali Mirza [b], Muhammad Assam [c], Emad A.A. Ismail [d], Mohamed R. Abonazel [e]

[a] Department of Law, Fatima Jinnah Women University, Rawalpini, Pakistan
[b] Department of Technical Computing and Cyber Security, University of Gloucestershire, WW103, Park Campus, Cheltenham, United Kingdom
[c] Department of Software Engineering, University of Science and Technology, Bannu, Pakistan
[d] Department of Quantitative Analysis, College of Business Administration, King Saud University, P.O. Box 71115, Riyadh 11587, Saudi Arabia
[e] Department of Applied Statistics and Econometrics, Faculty of Graduate Studies for Statistical Research, Cairo University, Giza, Egypt

ARTICLE INFO

Keywords:
Malware attacks
Cyber crimes
Cyber attacks
Deterrence
Proportionate punishments
Cyber laws

ABSTRACT

Numerous research studies have highlighted the exponential growth of malware attacks worldwide, posing a significant threat to society. Cybercriminals are becoming increasingly merciless and show no signs of pity towards individuals or organizations. It is evident that cyber criminals will stop at nothing to gain unauthorized access to confidential information. To effectively combat malware attacks, strict cyber laws are necessary, and the use of malware is punishable in many countries. However, the literature has not addressed whether these penalties create deterrence or not. This research article has addressed this gap. In this study, the effectiveness of criminal laws related to malware-related crimes in various jurisdictions was analyzed using the doctrinal research methodology. The cyber laws of the USA, UK, Ethiopia, Pakistan, and China were examined to determine whether the penalties imposed for these crimes are appropriate given the severity of the harm caused. The study concludes that malware penalties should take into account the creation or use of malicious code, targeting individuals or organizations, and the magnitude of consequences, regardless of whether mens rea is present or not.

1. Introduction

Over the years, there has been a significant increase in the number of cyber attacks worldwide, leading to extensive damage [1][2]. They are often attacks on the information system, to get, change or temper the data, hence achieving any ultimate goal e.g. economic or military gain [3]. These attacks come in various forms, and one of them is malware-based cyber attacks. The focus of this study is specifically on cyber attacks related to malware.

In today's world, we are constantly dealing with the troublesome and often devastating effects of increasingly sophisticated malware attacks. Not only criminal organizations, but even well-respected businesses and organizations have been found to be

* Corresponding author.
E-mail address: nadiakhadam@gmail.com (N. Khadam).

https://doi.org/10.1016/j.heliyon.2023.e22823
Received 18 December 2022; Received in revised form 19 November 2023; Accepted 20 November 2023

Available online 22 November 2023

involved in spreading malware. According to The AV-test institute reports, ethical hackers detect up to 560,000 instances of malware every day, resulting in an annual cost of over $55 billion [4]. One key factor driving the increase in cybercrime is the low cost and easy availability of various types of off-the-shelf malware and malware kits sold on the darknet [5][6]. On cybercrime forums like the darknet, malware can be bought for as little as $50 [7]. One does not need to be a skilled programmer or have specialized technical knowledge to purchase, design, or spread malware. With the aid of malware kits, one can easily create powerful malware and distribute it within an organization. Purchasing malware is also incredibly easy - it can be done in just a few minutes. Paid malware tools typically come with customer support, including free updates and troubleshooting services [8][2].

Numerous research reports have established a notable surge in malware attacks and scams during the COVID-19 pandemic. For instance, daily creation of around 300,000 new malicious softwares including viruses, adware, Trojans, keyloggers, etc., target individuals and organizations, resulting in billions of losses [9]. Phishing attacks surged by 600% in March 2020, and Interpol identified about “907,000 spam messages, 37 malware-related occurrences, and 48,000 malignant URLs attached to COVID-19” between January and April 2020, leading to a 60 percent drop in ransomware payments during the second quarter of 2020 [10] [11]. Google reportedly blocked 18 million malware and phishing emails to mitigate the cyber attacks [12]. Additionally, a recent study by the Clark School at the University of Maryland suggests that cyber criminals target a computer every 39 seconds, while over 75% of the healthcare industry has been infected with malware in the past year [13] [14].

The statistics presented above highlight the alarming increase in cyber security attacks, posing a significant threat with the advancements in technology. Cyber criminals have shown no mercy towards individuals and organizations, and their malicious activities continue to rise unabated. It is evident that cyber criminals will stop at nothing to gain unauthorized access to confidential information. Therefore, strict cybercrime laws must be enforced globally to address this pressing issue and ensure the safety of individuals and organizations in the cyberspace.

Cyber security attacks are not confined to any specific jurisdiction, unfortunately, every corner of the world is affected by these actions. With IcT advances through research, technical challenges are diminishing [15], however at the same time the advantage of cyberspace actually is acting as a disadvantage at this moment when any offender use malware while sitting in one country and affecting and targeting the computer systems of any other country or jurisdiction. To penalize any offender act should be declared as an offense in any law but unfortunately, the emergence of this new crime challenged the criminal justice system of every country to counter these illegal activities.

There are two maxims explaining the concept of criminal liability. First, “nullum crimen sine lege,” meaning one cannot be punished for doing something which is not prohibited by law, and “nulla poena sine lege,” meaning that one cannot be punished for doing any act for which no punishment is prescribed in law. These principles state that any action that is not expressly prohibited by law is not a crime. These maxims explain that a person cannot be punished for any wrongful act unless it is prohibited by law, and similarly, no one can be punished if the act is not prescribed by the law. Over time, due to advancements and new kinds of wrongful acts, different actions have been committed, but people are not prosecuted until they are expressly prohibited by law. This was the time when offenders got the benefit of the non-availability of relevant laws hence they escaped from the legal liability for such acts. With the passage of time different jurisdictions made laws to combat these offenders in cyberspace. Some jurisdictions had this benefit that their traditional criminal laws were in field and able to handle these illegal activities but at certain point even those laws were not enough. Hence require special laws. Like other countries Pakistan recognized this threat and legislated laws.

1.1. Philosophy of punishments

From early times, punishment is used to combat crimes. Different scholars wrote about the philosophical perspectives of the punishment and this process developed different theories, which in modern world are called theories of the punishment. These include retributive theory, utilitarian theory, rehabilitation theory, restorative theory and deterrence theory. It is pertinent to mention that these theories are not mutually exclusive, different societies and legal systems often employ a combination of these approached. The factor that varies is due to the nature of offense and required safeguard. The philosophy of punishment is always open for deliberations for most suitable mechanism for handling of crime.

Different theories of punishment followed by the legal system around the world while defining the punishment for any crime are used including deterrence, rehabilitation or retributive 1 irrespective of the causation or the magnitude of the consequence of that act [16][17]. Deterrence theory requires punishments to be stricter to deter the offender from any future crimes. Moreover, that offenders commit acts of reduces severity to minimize punishments [18]. Rehabilitation Theory is based on the concept that punishment should be to rehabilitate the offender. Its purpose is not only the deterrence but to help offender to rehabilitate so that he reintegrate in society well. Retribution theory is based on the concept of revenge and proportionality. Offender will be punished in same proportion as he did with the victim more commonly eye for eye concept. Utilitarian theories of punishment emphasize the consequence of punishment rather than moral culpability of the offender. Restorative justice approaches emphasize healing of the harm caused by the offense and restoring the relationships between victims, offenders and the community. Criminal justice system adopts these theories for defining the punishment but other dimensions are the target based approach and consequence based approach. With reference to malware it is debatable that target based approach is to be used or consequence based approach for determining the punishments for relevant crimes but this paper will analyze the target based approach to combat the malware. The purpose is to analyse and recognize that the different targets can be made for the same malware and ultimately the magnitude and nature of effect is different. As it is mentioned that it may target an individual at one time and at other time it may target the critical information infrastructure of any state. Laws are required to vary to avoid any injustice and undue punishment and also to punish the culprits for the severity of crime. The punishment must be proportionate to the effect caused [19].

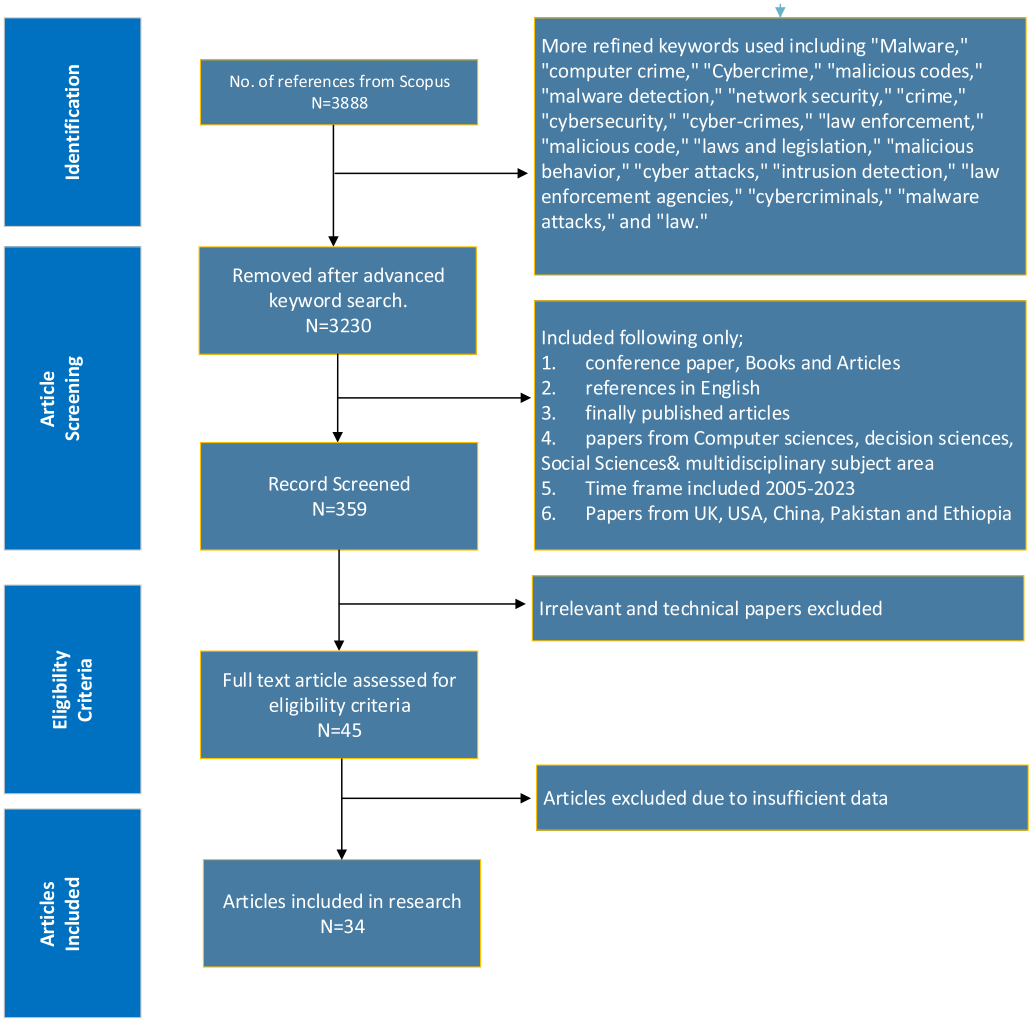


Fig. 1. Research methodology.

Our contributions in this article are as follows:

- For brevity of non-technical readers, this paper offers a comprehensive analysis of different types of malware, as well as the financial risks and damages they can inflict on individuals and organizations.
- Using the doctrinal and comparative research methodology, we evaluated the efficacy of criminal laws concerning malware-related crimes across different jurisdictions. Specifically, we compare cyber laws in the USA, UK, Ethiopia, Pakistan, and China to assess whether the penalties imposed for such offenses align with the level of harm caused by the crimes.
- Finally, this study examines the penalties assigned for offenses related to malware. The aim of analyzing these penalties is to determine whether they are commensurate with the impact of the crime.

1.2. Paper organization

This paper organizes as follows: Section 2 discusses the research methodology used to conduct this study. In Section 3, readers will find background information on various types of malware and the financial impact they can have on both individuals and organizations. Section 4 focuses on the punishments for malware crimes in Pakistan and their effects. Section 5 compares the cybercrime laws and penalties related to the use of malicious code with malafide intention in different countries, including the UK, USA, China, Pakistan, and Ethiopia, evaluating whether these penalties are proportionate to the harm caused. Finally, Section 7 presents the study's conclusions and discusses future research directions.

2. Research methodology

In this section, we present our approach to conducting a analysis of the literature. Fig. 1 provides a graphical depiction of the research methodology.

In this study, the Scopus database[1] was utilized to access a vast collection of published research papers, employing a set of specific keywords such as “Malware,” “cybercrime,” “malicious code,” “laws,” “target and consequence-based punishment,” and “deterrence” to identify relevant articles. Initially, a total of 3888 research articles were retrieved. To enhance the search, additional relevant keywords were incorporated, including “computer crime,” “Cybercrime,” “malware detection,” “network security,” “crime,” “cybersecurity,” “cyber-crimes,” “law enforcement,” “malicious behavior,” “cyber-attacks,” “intrusion detection,” “law enforcement agencies,” “cybercriminals,” “malware attacks,” and “law.”

Subsequently, conference papers, books, and articles were selected, reducing the dataset to 3128. To ensure language consistency, only articles written in English were retained, resulting in 3026 articles. Papers in press were excluded, further refining the dataset to 2989 articles. The selected papers covered various disciplines, with a focus on Computer Sciences, Decision Sciences, Social Sciences, and multidisciplinary subjects, enabling the acquisition of relevant information and knowledge. At this stage, the number of references amounted to 1765.

To maintain the relevance and recency of the sources, references’ publication years were limited to the range between 2005 and 2023, leading to 1749 articles within this time frame. Given the study’s comparative nature, focusing on the laws of the USA, UK, Pakistan, China, and Ethiopia, only articles from these specific jurisdictions were included, resulting in 359 references.

To ensure the inclusion of pertinent materials, a manual screening process was conducted to exclude overly technical papers and irrelevant sources. Consequently, the final set of relevant data included 45 references, sourced from 34 reputable publications, eliminating papers with insufficient data.

Finally, doctrinal research methodology was employed to explore the laws in different jurisdictions to combat malware related cybercrimes. This work, after explaining the background of malware and its financial impact on society, compiled the laws on cybercrime in different jurisdictions. The study examined punishments for malware based crimes in light of fundamentals of criminal law such as cause and effect of the crime act. The researcher also adopted a comparative approach to analyze and compare the malware-related laws across different jurisdictions to see the effectiveness of these provisions. This evaluation helped to identify areas where the laws were deficient or needed improvement, as well as areas where the laws were effective and could serve as a model for other jurisdictions. In short, his doctrinal and comparative research methodology provided a comprehensive and systematic analysis of the laws, and could be useful for policymakers, legal scholars, and practitioners seeking to improve criminal justice systems.

2.1. Limitations of studies

This study focuses exclusively on malware attacks and involves an analysis and comparison of the relevant laws in five specific countries: the United Kingdom, China, the United States of America, Pakistan, and Ethiopia. Other countries are not considered within the scope of this research. The analysis and comparison of laws in these jurisdictions are conducted using a doctrinal research methodology. However, it is important to acknowledge that one of the limitations of this research lies in the accessibility of case laws from all the selected jurisdictions, as reporting methods for case laws may differ among countries.

3. Background and financial impact of malware attacks on society

Today, societies from all around the globe are heavily dependent upon computers and related technologies. Unfortunately, an attack on computers is viewed as an attack on society. Malware or malicious software is one of the most successful and powerful weapons of cybercriminals to launch the cyber attacks and is presently considered a real war against our society [20][21][22].

The term “malware” is short for malicious software. The attacker design and spread malware through the internet with the goal to harm data, privacy, network, system, and services accessible to an individual or organization. Malware is commonly delivered in the form of a link or file over email and requires the user to click on the link or open the file at least once to get it executed.

Cybercriminals use malware or malicious software for many reasons. For instance:

1. To illegally obtain sensitive data from the individual via stealing or online fraud, for example, passwords, bank and credit card details and business-related data, and so on [23].
2. To acquire remote admittance to machines and networks. Here, the primary target of the attacker is not just to infect the machine yet additionally to utilize his/her virus infected computer to spread the infection through the whole organization via the Internet.
3. To disrupt the activity of a business, government, association, and, or explicit kinds of equipment and software via launching the denial of service attack.[2]
4. To send a flood of spam emails from the infected machine to the targeted individuals and organizations.

[1] https://www.scopus.com/.

[2] The Denial of Service attack is a type of attack that makes services and resources unavailable to the legitimate users. For instance, a DoS attack could use up all random access memory (primary storage) or hard disk (secondary storage) on a system so that other users are unable to use them [24].

5. To make secret or private data, for example, personal health data or company's confidential information accessible to unauthorized people [25]. Here, the cyber-criminals send off such goes after with an aim of slander, provocation, or extorting the people or the business association.
6. Last but not least, for monetary benefit, secret activities, or revenge.

The world has been enduring cyber attacks from a large number of various malware variations since the mid-1970s when the first ever virus program "Creeper" showed a message on PC screens: "I'm the creeper, get me if you can!" [26]. Creeper was not a destructive virus as compared to the viruses present today. It duplicates itself and spreads to different networks and computer systems throughout the internet intending to show irritating messages on the display screens. Subsequently, a 15 years of age secondary school understudy named Richard Skrenta designed a boot sector virus that infected Apple II PCs [27]. It spread via a then-cutting edge, removable media, for example, the floppy disk and to turn into the main significant PC virus outbreak. It was not purposely destructive, however, it was harmful.

3.1. Types of malware and their financial impact

In this section, we discuss different types of malware. Malware is categorized as viruses, worms, Trojan, spyware, adware, and ransomware. Some types of malware are more dangerous and have severely affected individuals and organizations in terms of financial loss and reputation. For instance, ransomware has proven to be more effective and dangerous during the last decade for the healthcare sector and government organizations.

3.1.1. Viruses and worms

A computer virus is much similar to the flu virus. It is designed to spread from computer to computer. It needs a host to replicate itself. In order to execute its code and cause maximum damage to its host machine, it attaches itself to some file or program such as a document, email, text message, and even social media scam links [28]. Once, the virus has infected the host machine, the virus can spread through the network and infect other machines on the same network. Mobile devices and smartphones can become infected with mobile viruses through shady App downloads. Stealing passwords, data and even bank details, logging keystrokes, corrupting files, spamming email contacts, and even taking over machines are some of the most devastating, damaging, and irritating things a virus can do.

Similar to computer viruses, worms are also capable to do devastating and damaging things to individuals and organizations. The difference between a virus and a worm is that a virus needs to attach to another program like a word processor or web browser to make it work. By contrast, a worm is self-contained and can run, copy, and send copies of itself all on its own. Some of the most dangerous computer viruses are actually worms [29].

In 2004, a very infectious virus named Mydoom caused $38 billion financial damages to business organizations and individuals. While another virus SQL Slammer (worm) cost an estimated $750 million across 200,000 computer users in 2003. In 2016, Slammer worm took banks and ATM machines offline in the U.S. and Canada. In September 2020, one of the potentially largest computer virus attacks in medical history hit Universal Health Services. The attack forced the cancellation of surgeries and made healthcare workers switch to paper records [30]. Stuxnet worm is reported to have destroyed Iranian nuclear centrifuges by sending damaging instructions [31].

3.1.2. Ransomware

Ransomware attack attempts to prohibit computer users from retrieving data stored on a computer or accessing the computer system. The attacker encrypts the whole storage media or some data stored on it and then demands the ransom from the victims to allow access to it. Users are shown instructions on how to pay a ransom to get the decryption key. For the reason that attackers and cybercriminals remain intractable, they demand ransom to pay in cryptocurrency such as Bitcoin which is an anonymous and virtual currency. Some ransomware can also spread to other machines in a network such as, in May 2017 Wannacry malware seriously disrupt and damage the healthcare sector. Similar to easy access viruses and worms kits, ransomware kits are also available on the dark web to carry out the ransomware attacks also known as *ransomware-as-a-service*.

Ransomware attacks continue to increase this year. Numerous studies show that the vast majority of business organizations and healthcare sectors have experienced significant loss in revenue, damage to the brand's reputation and, even closure of the business due to the successful ransomware attacks. Business and healthcare organizations are struggling to protect themselves from their damaging effects. According to [32], ransomware damage cost is expected to reach $265 billion by 2031. 66% of organizations reported significant revenue loss as a result of a ransomware attack. 80% of organizations that paid a ransom demand was threatened a second time, and of those, 46% believed they were targeted by the same hackers. Amongst those that paid a ransom to restore their systems, 46% said at least some of their data was corrupted. 53% of organizations indicated that their brand and reputation were damaged as a result of a successful ransomware attack and many lost their jobs [33].

Ransomware attacks are on the rise. A full recovery of data is not guaranteed even after fulfilling the ransom demands of the attacker. In reality, it has exacerbates the number of ransomware attacks by encouraging the attackers. There is an urgent need to establish, enforce and implement strict cyber laws and punishments to mitigate them.

3.1.3. Spyware

Spyware is malicious software that is used by cyber criminals to spy on the victim's information and activities. Upon downloading on the victim's device, it secretly monitors and records all the activities of the victim such as login name and password credentials,

credit card and bank details, and browsing and searching history. This information is then transferred to the attacker via the Internet who uses this information for his own benefits or sells it to a third party such as advertisers, spammers, scammers, or hackers [34]. Spyware can also cause other severe damages such as locking a victim's device, disabling antivirus programs or security related notifications, recording live videos and taking pictures using a mobile camera (front and back camera), viewing device specifications, installing or uninstalling apps, recording conversations using the microphone, track victim's current geographic location and transferred it to the third party, record incoming and outgoing calls and so on.

3.1.4. Adware

Adware is a type of malware that automatically generates and displays unwanted and irritating advertisement notifications on computer screens to generate revenue for its developer. Some adware is extremely malicious and upon clicking on the advertisement, redirects the users to the malicious websites containing adult content. It harms the device by slowing down its speed and performance. It also installs unwanted plug-ins, toolbars and extensions in the browser without the consent of a user. Some adware also creates a backdoor for cyber criminals. Fireball, Appearch, DollarRevenue, Gator, and DeskAd, are the most popular adware softwares. Developed in 2015 by the afotech, a Chinese digital marketing agency, Fireball has infected more than 250 million computers and one-fifth of corporate networks around the world. DollarRevenue, developed in Netherland in 2005 has infected 22 million devices worldwide by the end of 2007. Its developer was punished by fined one million euros in 2007, however, the decision was revoked after six years of punishment [35].

3.1.5. Torjan

A Trojan is a deceptive malware that disguises itself as a legitimate program and upon downloading on the victim's device continues to spy on the victim's activities or steal private information. Like viruses, Trojan hides into a file or document to be downloaded and attach to an email, then transfer to the victim's device upon downloading the file or document. Like viruses and worms, they spread from computer to computer through the internet and network.

Cyber Criminals use Trojan to gain backdoor access into the business organization and control the devices and network remotely without the consent of the users. A cyber criminal turns a computer system into a zombie to continue the spread of malware into the network. The zombie computer system is also known as a botnet.

4. Correlations between conviction and malware crime rate

Laws need to be updated and upgraded with the passage of time and with new requirements. Technology is the factor which largely brings instances on daily basis where countries should be vigilant to enact new laws timely. Development in cyber space and that too for offenses need special attention. If the law treats the person A using malicious code with huge loss and affect same as any sort of effect through malicious code, then as per the deterrence theory of punishment, offenders will keep doing as the lesser punishment for severe crimes are failed to create deterrence to the offender. Because the fear of punishment is considered a major incentive in deterring crime, deterrence theories are often associated with the idea of severe, disproportionate punishment [36].

For example, in Pakistan Section 2 & 3 Prevention of Electronic Crimes Act 2016 (PECA) penalizes the writing or provision of malicious code by any one with intention to harm any information system or affect in any way. The punishment is imprisonment up to two years or fine or both.

Here no distinction is made with reference to the magnitude of the affect. Punishment is two years only that is unable to create deterrence. Significance of punishment is broadly defined under four theories: retribution, rehabilitation, incapacitation, and deterrence, out of all deterrence is widely referred because "deterrence based research can be directly translated into policy action" [37].

It is important for legislators to foresee the technological developments and the time requirement for updated laws. Punishment creates deterrence, in two forms, general or special. General deterrence is for the non-criminals who otherwise would have been willing to commit crimes, fearful enough of punishment to avoid it by refraining from crime. However special deterrence restricts recidivism [38]. Deterrence can occur only to the extent that prospective offenders perceive a risk of punishment. Without this perception, there can be no deterrent effect.

The impact of punishment on the deterrence effect of that punishment can be recognized by the proposition that the greater the certainty, severity, and swiftness (celerity) of punishment, the lower the crime rate will be.

At policy levels it is discussed that punishments deter people and this is true but not at all times. In small kind of offenses lesser punishment can be inflicted but for repeated offenders and in case of heinous crimes punishments should be increased as per the needs [39]. It is also stated that punishment variability effects the choice to commit a crime or not [40].

This discussion is referring towards policy development for state where they handle criminal act without looking into the magnitude of its effect. Criminal law principles appreciate the recognition of the effect caused by the criminal act. In this study it was observed that use of malicious code can differ in its effect of different acts, hence it refers to the conclusion that effect of the act must be recognized by the law and offender should be punished accordingly to restrict and combat people to commit similar nature of crimes.

Cyber security and cyber deterrence goes hand in hand concepts [41]. In traditional world punishments are given to deter the offender and similarly in cyber space. There are many examples around the world where criminal in cyberspace are handled iron-

handedly. In 2011 Aaron Swatz hacked the JSTOR the academic data base and affected the MIT network and he was charges with penalty of $1 million in fines, 35 years in prison, and asset forfeiture and the later committed suicide.[3]

Another example is from China, where in 2011 the Supreme People's Court prepared for a trial to punish the people who unlawfully breached the network to obtain information or plant malware by "interpretation of the law for computer information criminal case." The Supreme People's Procuratorate discussed the illegal provision of or buying of materials and tools of hacking. It was observed that these activities are growing and must be penalized to control. After this case, provision of software for illegal purpose is declared as crime. Perhaps this "indirect" law is subject to the Criminal Code and it will allow those who commit this offense to be jailed for up to ten years.

The above case is very important to discuss that in a society punishment play important role to keep rule of law and peace and security. Theories of punishment mention that there should be purpose of punishment. Over the period of time different scholars defined the purpose of punishments and the philosophy behind the punishments as referred in the introduction part. When lesser punishments are not helping to deter crime in society legislations increase the punishment with particular emphasis of the effect of those crimes. With regard to the current study, previous section mentions that law criminalizes the use of malicious code when effect the information systems but these incidence increases day by day and also effecting the critical information infrastructures. Law is not differentiating the critical nature of the system hence, minor and major offenses are handled in lighter way.

A deterrence theory of punishment holds that the institution of criminal punishment is necessary or justified because punishment serves to deter crime. Deterrence theory is usually associated with rational choice theory, that means a person takes always a conscious decision and it is presumed for the offender also, so if offender think about the severe punishment. Deterrence theory holds that severe and disproportionate punishments are justified to create fear to the public to refrain from committing any crime.

This discussion mentioned that severity for punishment would help to deter crime but more importantly the punishment proportionate to the effect caused would be a better mechanism as these cyberspace tools effects differently.

In actual, the scientific knowledge requires the law to recognize the effect and on basis of this, prescribe punishments. The smaller target offense the lesser the punishment and vice versa. Here the deterrence theory of punishment must be discussed, greater punishments deter people from committing crimes.

5. Punishments of malware use in different jurisdictions (Pakistan, USA, Ethiopia, China, UK)

Computer virus is used to damage the information systems through affecting the working and damaging the systems. Globally, general cybercrime legislations are adopted, countries made effort to lessen the legal gaps to punish cyber offenders [42] [43].

In this section, we provide detailed discussion and explained the major legislation on cyber crimes in some jurisdictions including UK, USA, Pakistan, China and Ethiopia. Moreover, laws regarding use of malicious codes for criminal activities are compared in these mentioned jurisdictions.

5.1. Punishments of malware use in Pakistan

With a brief history in 2002 Electronic Transaction Act (ETO 2002) was promulgated in Pakistan to handle the issue in electronic world.

Analyzing the ETO 2002 provisions more in depth, firstly, the provisions are very limited in scope and secondly the term information system is not used in effective manner. With the increase in use of computer, new ways were created and none of them was included in this Ordinance to make more effective legislation. The effect of this legislation is that mostly offenders easily escape from the law and judges are unable to charge them. Meanwhile Pakistan had some temporary legislation, those were repealed. Later in 2016 Prevention of Electronic Crime Act (PECA, 2016) was promulgated to handle the cyber space offenses with more specialized approach. This work will analyze provisions of these laws to highlight the provision dealing with offense done through use of malware. This is most practiced mechanism of committing crime in cyberspace.

Pakistan Penal Code 1860 contains general substantive criminal law. Special laws are initiated to cover the special subjects such as cybercrimes, cyber terrorism, anti- corruption and others. In the year 2002, after accepting the challenging situation created by the increasing use of internet vis-a-vis electronic commerce, efforts were made to regulate this area and ETO 2002 was promulgated to recognize and facilitate the electronic form of document and other information. The words "electronic, electronic document and electronic signature" were for the first time defined in any statute. 'Cyber crimes' were made known in ETO of 2002, wherein unauthorized access and damage to any information system was penalized. ETO 2002, was developed after the need of the regulations for e-commerce was felt in Pakistan. In 2000, an Information Technology Law Forum was created to facilitate the development of provisions related to e-transactions and electronic commerce. This initiate included various lawyers from law and IT discipline. The forum made consultations with various other departments like, financial sectors and legal community to draft the Electronic Transactions Ordinance. It also looked into the United National Commission on International Trade Law (UNCITRAL), model laws and other international guidelines.

It is very important to mention the main purpose of the enactment of this law, which was to make Pakistan to use the electronic based transactions instead of paper-based transactions to enhance governance, economic situation and service to citizens. Sections 34,

[3] News Office, MIT, 2013 https://news.mit.edu/2013/mit-releases-swartz-report-0730.

35, 36 and 37 of the said law deal with the offenses whilst section 38 mentions that these offenses are non-bailable, compoundable and cognizable. The proper forum for trial of these offenses is Court of session as mentioned in Section 39.

Sections 36 & 37 are two sections penalizing the wrongful act. Section 36 criminalizes a person who gains or attempt to gain and try to approach the information system with mens rea or not. Punishment for such wrongful act id imprisonment upto seven years or fine or both. Whereas section 37 prescribes a punishment of seven years for the offender if a person alter, change or store any information from information system, which he knows is not authorized or where a person impairs the working of any information system with mens rea.

In previous sections term information system is used which is defined in Section: 2 of Ordinance as follows;

Section 2(p)

"Information system" means an electronic system for creating, generating, and sending, receiving, storing, reproducing, displaying, recording or processing information.

Sections 36 and 37 penalize the various forms of hacking and malicious code through the provision titled 'violation of privacy of information'. The Ordinance is however silent on offenses like "Obscenity", "Cyber Fraud" and others.

In December 2007, a detailed Ordinance named Prevention of Electronic Crimes Ordinance (PECO 2007) has been introduced but it was never made a permanent law and after one time re-promulgation it was repealed in 2009. After 7 years a detailed law was promulgated titled "Prevention of Electronic Crimes Act" in 2016 (PECA 2016). Along with cybercrimes different cyber security issues were also addressed. One of the crime is DDoS attacks using malicious codes.

At this point it is important to discuss that how the offenses using malicious codes are penalized and how these are combating these crimes. Offenders use malicious code to effect the information systems. Section 23 of PECA 2016 penalizes the certain acts related to malicious code, such as willfully and without authorization writing or creation or transmission of malicious codes with malafide intention to affect the information system. In these situations 2 years punishment is fixed with one million rupees fine or both.

Explanation: For the purpose of this section, the expression "malicious code" is defined in the PECA 2016 as "a computer program or a hidden function in a program that damages an information system or data or compromises the performance of such system or availability of data or uses it without proper authorization" [44].

Section 23 penalizes the offender who uses malicious code with malafide intention with imprisonment upto two years. This work will analyze the effect of this punishment. Malicious code might be used to cause greater harm or lesser but legislation prescribes one punishment that is maximum 2 years. Keeping in view the sensitivity of the offense two years is very meager punishment and it would fail the purpose of deterrence.

Gaining unauthorized access to any information system is penalized under Section 3 which prescribes maximum punishments of three months or fine which may extend to fifty thousand Pakistani rupees (approx. 200 US $), when a person gains unauthorized access to any information system or data with mala-fide intention.

However, another section penalizes, if a person with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both [45]. Punishment of 2 years is prescribed for a person who interferes with or damages or causes to be interfere or damages a the information system or data any part or whole of an information system or data [44].

Above provisions are related to individual system but PECA, 2016 also defines the effect to critical information infrastructure

It is important to mention that critical information infrastructures are vital for the working of a state, Simple information systems and data carry different importance but at state level these critical infrastructures are very significant. Law defines "critical infrastructure" as critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in major detrimental impact on the availability, integrity or delivery of essential services including those services, whose integrity, if compromised, could result in significant loss of life or casualties, taking into account significant economic or social impacts; or impact on national security, national defense, or the functioning of the state.

This entails that the effect to these infrastructures would hamper the working of the state and it may halt any vital service within any country. For instance effecting the online health care system, when no data can be accessed. Bank databases are effected where the bank is unable to give its services. Malicious code can affect all these simple infrastructure, information system, digital data with different magnitude. And if the system is critical information infrastructure then the story is different and dangerous too.

In 2007, websites of Estonian Parliament, ministries and banks were affected through denial of service attacks and it was first of its kind attack affecting government infrastructure at serious level. (World Bank Group: Security in cyberspace).

The wrongdoers effecting the critical infrastructure using malicious codes they might affect big or small. But unfortunately this aspect is not handled in law and all offenders using malicious code are gauged at similar footing and effect of wrong act is not considered. For instance, suppose attack 1 & 2 are same in mode, through attack 1 a personal information system is effected and it only effected the working of the system for few hours on the other hand through attack 2 an information system which is part of state machinery is targeted and it affected the system to respond on behalf of the state. Same nature of malicious code is used but the effect is different so deterrence theory of law suggests to keep strict punishment for more heinous crimes. Or it should be proportionate to the damage caused.

Another example is, it is possible that a person using malicious code effect the person's personal computer which he/she can restore by using advanced software. But at the same time a malicious code can be used to effect the working on online banking service of any bank, effecting public at large. If we move further, there might be situation that use of malicious code might help the

Table 1
Offence and Penalty for the cyber-criminal.

Offence / Crime	Penalty for the cyber-criminal
Unauthorised, or malicious, tampering with material stored on a computer.	A six-month sentence in prison with a possible fine of \5,000
Intention to commit a cybercrime.	A five-year prison sentence or unlimited fine.
Modifying, removing, or ransoming data.	A five-year prison sentence or unlimited fine.
Aiding in computer misuses.	A ten-year sentence or unlimited fine [52].

offender to get the access of important state information from any information system, and transmitted and used for ulterior motives, hence the effect is very large.

Through a malicious code in 2021 Pakistan Federal Board of Revenue's data was in unauthorized way accessed and sold on dark web and this is huge loss for Pakistan [46].

5.2. Punishments of malware use in USA

It is a unique situation in USA that both federal and general law was applicable. The outcomes and then legal implications out of malware use are not certain. The nature of offenses could vary that is the reason different jurisdictions dealt this criminal act differently. USA signed the Convention on cybercrime in 2006 and USA implemented the provisions through federal law. Computer Fraud and Abuse Act 1984 CFAA created seven computer-specific offenses for unauthorized access to computers, though it applies only to "protected computer[s]," specifically those used by financial institutions. The CFAA has been subsequently amended, notably by the 2001 USA Patriot Act and the 2008 Identity Theft Enforcement and Restitution Act. For Computer Hackers in USA punishment is 10 years and in case of repeated offender it is 20 years. Attempt to affect the computer system is also penalized. The affect to computer system during hack attempts is calculated on year basis. Criminal provisions are introduced in Federal Criminal Code for any kind of damage to computer system, intrusion to those systems or effecting them through malicious codes and DDoS. The sentencing is enhanced for cyber crimes. When cybercrime is done due to criminal intent, punishment might be raised to 20 years. More importantly when damage to human life is caused, punishment could lead to life imprisonment. USA adopts the target based approach and if the malware is effecting the computer used by government or by financial institutions is a federal crime under the Computer Fraud and Abuse Act [47]. In 1999 an offender named David L. Smith was punished with five years sentence for creating and distributing malware. This malware caused $80 million in damage. The uniqueness of this attack as that it affected computers owned by individuals and government. In 2002 Cyber Security Enhancement Act was promulgated to legislate on privacy protection, punishments variations in computer crime and guide for enhanced penalties. Significantly, this law amended the article 225 of Computer Fraud and Abuse Act by recognizing the heinous nature of crime. It penalized the offender with mens rea to imprisonment of 20 years. This shows that every different aspect is recognized. USA raised the punishment to 20 years of act is done with criminal intention from the act done with mistake. This rule enunciates two dimensions first, that offender may give the benefit of doubt that act is mistakenly done without criminal intent but if proved serious punishment is given. Secondly it supports the present study that is criminal intent to target the individual's information system is different and targeting critical information infrastructure is different. So criminals must be dealt differently.

5.3. Punishments of malware use in Ethiopia

On the other hand, Ethiopia at lowest level of internet penetration promulgated its first law on the subject of cybercrime in 2004 [48]. Through this law hacking, dissemination of malware and denial of service attacks were penalized. Later on keeping in view the new challenges new law was promulgated in 2016. The major change in the new law was with reference to the enforcement agencies. Principles of criminal law envisage one of the elements of crime is the criminal intent and without that only few exceptional instances can be penalized, however in Ethiopia using malwares without intention is penalized with 3 months of punishment or fine [49]. Secondly if the intention is only to damage the target system the punishment prescribed is imprisonment not less than 3 months so giving discretionary power of granting many years as punishment. If the dissemination of malware with the intention to devise or execute any scheme or artifice to steal, defraud, deceive or extort or serious case of disseminating malware with bad intention the punishment would be 5 years rigorous imprisonment. Aggravated cases are also mentioned in the law, these are against the 'top secret' foreign or military computer data, systems or networks during times of emergency and punishment is 25 years of rigorous imprisonment [50]. However, here no provision is with regard to liability of writing a malicious code. Who created it? For reference making of malicious code is equally penalized as using of forged document. Making of forged currency is equally penalized as using of forged currency [51].

5.4. Punishments of malware use in China

In china, cybercrimes are under focus as these are recognized as a threat to national security [53]. In modern times, cyber crimes in China are increasing drastically that it is need of the time to rethink about the criminal law at basic theoretical level [54].

Interestingly China's legal system is using both target and consequence based approach. Article 286 of Criminal Law of the People's Republic of China states that;

1. Whoever violates states regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences, is to be sentenced to not more than five years of fixed-term imprisonment or criminal detention; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment.
2. Whoever violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences, is to be punished according to the preceding paragraph.
3. Whoever deliberately creates and propagates computer virus and other programs which sabotage the normal operation of the computer system and cause grave consequences is to be punished according to the first paragraph [55].

Here clause (iii) is referring to the propagation of computer virus which affects the normal operation of the computer system and causes grave consequence is punished upto maximum five years of fixed term punishment but more importantly this law recognizes the varied affects or consequences of the malware use and for appreciating it, same provision prescribes that not less than five years punishment if the consequences are serious. Although the term serious also needs clarification. This provision also penalizes the deliberate creation of the computer virus.

5.5. Punishments of malware use in UK

The UK Computer Misuse Act 1997 refers to misuse of computer and offenses committed while using medium of computers. This law criminalizes many of the malicious attacks or offenses against computer solutions, including hacking and ransoming [56]. Along with this law Fraud Act 2006, General Data Protection Regulation 2018, are dealing with related issues in UK.

The Computer Misuse Act defines the following as illegal and will prosecute:

- Unauthorised, or malicious, access to material stored on a computer.
- Intentional harm, or crime, using computer systems.
- Modifying, removing, or ransoming data.
- Aiding in computer misuses, such as supplying information.

This law penalizes the authorized access to information system and more importantly it significantly put importance on offenses effecting human life or national security and prescribing life imprisonment as punishment. The penalties vary in severity, from costly fines to prison sentences (Table 1).

But in recent times, many criticisms are made on the legislation that now technology evolved and new crimes emerged and a crime only done through computer to be dealt under this law might cause injustice as it might be only a civil wrong done through computer [57].

6. Comparative analysis of malware related laws in selected countries

The comparative analysis among various jurisdictions exhibits that there are considerable discrepancies in the magnitude of punishments for malware use. Fig. 2 provides a comparative analysis of malware related laws in UK, USA, China, Ethiopia & Pakistan.

In Pakistan there is ETO, 2002 and PECA, 2016 which criminalizes the use of malware. ETO, 2002 under Sec. 37 criminalizes the intentional use of malware for unauthorized access of information with the imprisonment of upto seven years or fine not exceeding one million Pakistani rupees or both. PECA, 2016 prescribes the punishment of two years or one million Pakistani rupees fine or both for writing or using malicious codes with mala fide intention under Sec. 23 and punishments upto three months or fine which may extend to fifty thousand Pakistani rupees for gaining unauthorized access to any information system under Sec. 3. Conversely, in the USA, Computer Fraud and Abused Act, 1984, as amended, maintains penalty of twenty years imprisonment for the commission of an offense targeting government or financial systems and ten years in other cases for first time offender. Ethiopia recognizes both intentional and unintentional use of malicious code, and the severity of the offense determines the range of punishments that is three months to 5 years. Criminal Law of China takes into account the resultant consequences of the activity, thereby resulting in more stringent penalties for severe outcomes ranging upto five years. UK, through Computer Misuse Act, 1997 has classified specific activities associated with malicious code as illegal imposing penalties ranging from three months to ten years; however, further elucidation is necessary. Use of same magnitude of punishments for crimes with varied seriousness is unjust and against the norms of Criminal Law and rule of law in general. There is a need to harmonize the punishments for use of malware with the severity of crime committed measured by the damages so resulted. The ever increasing frequency of cybercrimes through the use of malware requires the imposition of well rationed penalties for enhancing deterrence to meet the ends of administration of justice.

It is important to mention that many criticisms are made on the legislation that now technology evolved and new crimes emerged and a crime only done through computer to be dealt under this law might cause injustice as it might be only a civil wrong done through computer [43]. Above discussion revealed that offense done through use of malicious codes may have different magnitude to be penalized. It should not be generalized punishment like in USA, UK and Pakistan but it should be as per the consequences done.

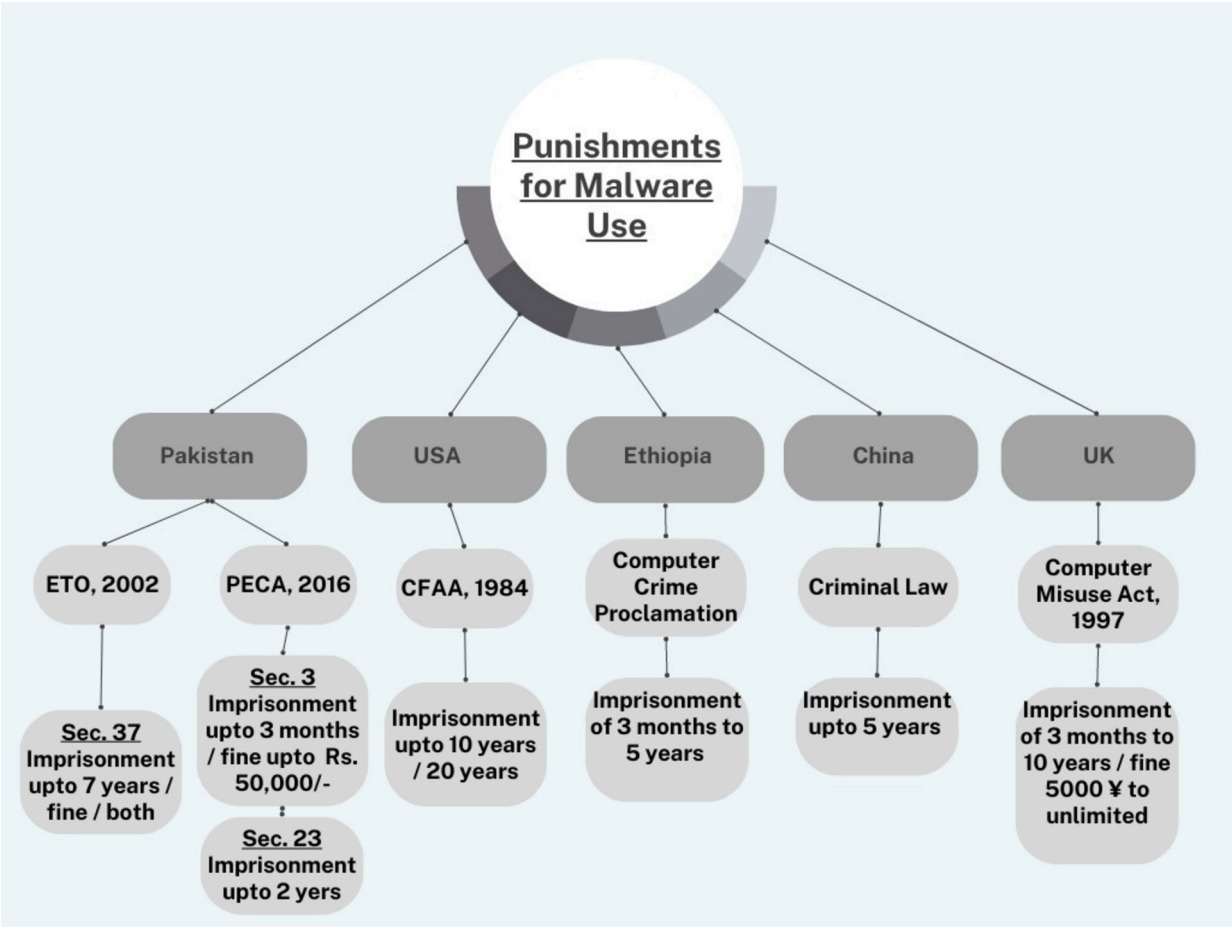


Fig. 2. Comparative analysis of malware related laws in selected countries.

To some extent laws of Ethiopia handled this issue but in that law still there are issues like the liability of the maker or generator of the malicious code.

7. Conclusion and future directions

The advancement of technology has brought both convenience and challenges to our lives, with one of the biggest challenges being the emergence of various advanced types of malware. It is difficult to find a one-size-fits-all solution to tackle this issue. Criminals take advantage of the absence of specific laws to protect themselves. Governments around the world are working towards combating cybercrimes by introducing laws with provisions that take into account the targets and consequences of such crimes to prevent them from happening. This study highlights the varying effects of using malicious codes in criminal activities, where the effects of targeting an individual's computer are different from those of targeting government systems or critical information infrastructures.

Our comparative analysis revealed that Pakistan imposes a penalty of 2 years for the use of malicious code with criminal intent. In the USA, if a malicious code affects the computer system of a government or financial institution, a penalty of 5 years is imposed. Ethiopia recognizes the use of malicious code without mens rea and provides lesser punishments for the said act. If the intention is to damage the system, the minimum punishment is 3 months, and for cases involving fraud or serious damage, the punishment is 5 years. China's laws take into account the severity of the consequences caused by the activity, with more severe punishments for grave consequences. In the UK, certain activities related to the use of malicious code are deemed illegal, but further definition and explanation are needed to effectively combat such activities.

Our analysis suggests that the same punishment for every kind of crime committed through malicious code is not equitable and undermines the principles of criminal law and the rule of law. A person should not be penalized for something they did not do, nor should they be exempted for a serious offense. Therefore, it is crucial for countries to consider the effects and consequences of a crime before assigning liability. Punishments must be proportionate to the magnitude of the offense, with lesser punishments for less severe offenses and more severe punishments for serious offenses. This approach would ensure justice and fairness in the handling of technology-related crimes, including the use of malicious code.

Role of funding source

This research received funding from King Saud University through Researchers Supporting Project Number (RSPD2023R1060), King Saud University, Riyadh, Saudi Arabia.

Ethical approval

This article does not contain any studies with human participants performed by any of the authors.

Informed consent

No clinical trials with human participations have been performed for this review study. However, for this review study, authors are responsible for correctness of the statements provided in the manuscript.

CRediT authorship contribution statement

Nadia Khadam: Conceptualization, Formal analysis, Investigation, Methodology, Writing – original draft, Writing – review & editing. **Nasreen Anjum:** Conceptualization, Formal analysis, Methodology, Software, Validation, Writing – original draft, Writing – review & editing. **Abu Alam:** Writing – review & editing. **Qublai Ali Mirza:** Writing – review & editing. **Muhammad Assam:** Writing – review & editing. **Emad A.A. Ismail:** Funding acquisition, Writing – review & editing. **Mohamed R. Abonazel:** Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No such data.

Acknowledgements

Researchers Supporting Project number (RSPD2023R1060), King Saud University, Riyadh, Saudi Arabia.

References

[1] J. Fang, Z. Yang, N. Anjum, Y. Hu, H. Asgari, M. Shikh-Bahaei, Secure intelligent reflecting surface assisted UAV communication networks, in: 2021 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2021, pp. 1–6.
[2] K. Imran, N. Anjum, A. Alghamdi, A. Shaikh, M. Hamdi, S. Mahfooz, A secure and efficient cluster-based authentication scheme for Internet of Things (IoTs), Comput. Mater. Continua 70 (1) (2022) 1033–1052.
[3] F.S. Alabbadi, E.M. Al Amaren, S.I. Aletein, International responsibility arising from cyberattacks in the light of the contemporary international law, Int. J. Cyber Criminol. 16 (1) (2022) 156–169.
[4] A not-so-common cold: malware statistics in 2022, https://dataprot.net/statistics/malware-statistics/.
[5] P.H. Meland, Y.F.F. Bayoumy, G. Sindre, The ransomware-as-a-service economy within the darknet, Comput. Secur. 92 (2020) 101762.
[6] T. McIntosh, A. Kayes, Y.-P.P. Chen, A. Ng, P. Watters, Ransomware mitigation in the modern era: a comprehensive review, research challenges, and future directions, ACM Comput. Surv. 54 (9) (2021) 1–36.
[7] Revealed: the supermarkets that will sell you malware for $50, https://www.forbes.com/sites/daveywinder/2020/04/28/revealed-the-supermarkets-that-will-sell-you-malware-for-50/?sh=4111710d30ae.
[8] How much malware tools sell for on the dark web, https://www.techrepublic.com/article/how-much-malware-tools-sell-for-on-the-dark-web/.
[9] How many cyber attacks happen per day in 2022? https://techjury.net/blog/how-many-cyber-attacks-per-day/gref.
[10] 600% increase in Covid-19 related phishing attacks, https://www.itsecurityguru.org/2020/04/16/600-increase-in-covid-19-related-phishing-attacks/.
[11] Interpol report shows alarming rate of cyberattacks during Covid-19, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
[12] Google blocking 18m coronavirus scam emails every day, https://www.bbc.co.uk/news/technology-52319093.
[13] Cybersecurity: a global priority and career opportunity, https://ung.edu/continuing-education/news-and-media/cybersecurity.php#:~:text=A%20Clark%20School%20study%20at,give%20attackers%20more%20chance%20of.
[14] N. Anjum, Z. Yang, H. Saki, M. Kiran, M. Shikh-Bahaei, Device-to-device (D2D) communication as a bootstrapping system in a wireless cellular network, IEEE Access 7 (2019) 6661–6678.
[15] N. Alhalafi, P. Veeraraghavan, Cybersecurity policy framework in Saudi Arabia: literature review, Front. Comput. Sci. 3 (2021) 736874.
[16] Punishment and state's criminal law, https://pakistanlaw.pk/articles/1096/punishment-and-state-s-criminal-law.
[17] N. Anjum, D. Karamshuk, M. Shikh-Bahaei, N. Sastry, Survey on peer-assisted content delivery networks, Comput. Netw. 116 (2017) 79–95.
[18] B.A. Jacobs, Deterrence and deterrability, Criminology 48 (2) (2010) 417–441.
[19] G. Duus-Otterström, Do offenders deserve proportionate punishments?, Crim. Law Philos. 15 (3) (2021) 463–480.
[20] A. Abusitta, M.Q. Li, B.C. Fung, Malware classification and composition analysis: a survey of recent developments, J. Inf. Secur. Appl. 59 (2021) 102828.
[21] D. Aboshady, N. Ghannam, E. Elsayed, L. Diab, The malware detection approach in the design of mobile applications, Symmetry 14 (5) (2022) 839.

[22] S.A. Roseline, S. Geetha, A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks, Comput. Electr. Eng. 92 (2021) 107143.
[23] Z. Almahmoud, P.D. Yoo, O. Alhussein, I. Farhat, E. Damiani, A holistic and proactive approach to forecasting cyber threats, Sci. Rep. 13 (1) (2023) 8049.
[24] A. Muhammad, I. Murtza, A. Saadia, K. Kifayat, Cortex-inspired ensemble based network intrusion detection system, Neural Comput. Appl. (2023) 1–14.
[25] G. Renjith, P. Vinod, S. Aji, Evading machine-learning-based Android malware detector for IoT devices, IEEE Syst. J. (2022).
[26] E.C. Cheng, T. Wang, Institutional strategies for cybersecurity in higher education institutions, Information 13 (4) (2022) 192.
[27] J. Hruska, 5.1 Virus types, in: Practical Data Security, 2019.
[28] S. Gupta, A.K. Cherukuri, C.M. Subramanian, A. Ahmad, Comparison, analysis and analogy of biological and computer viruses, in: Intelligent Interactive Multimedia Systems for e-Healthcare Applications, Springer, 2022, pp. 3–34.
[29] C.C. Zou, W. Gong, D. Towsley, L. Gao, The monitoring and early detection of Internet worms, IEEE/ACM Trans. Netw. 13 (5) (2005) 961–974.
[30] The top 10 worst computer viruses in history, https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history.
[31] R. Langner, Stuxnet: dissecting a cyberwarfare weapon, IEEE Secur. Priv. 9 (3) (2011) 49–51.
[32] Global ransomware damage costs predicted to exceed 265 dollar billion by 2031, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[33] Ransomware: the true cost to business, https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business.
[34] K. Anumula, J. Raymond, Adware and spyware detection using classification and association, in: Proceedings of International Conference on Deep Learning, Computing and Intelligence, Springer, 2022, pp. 355–361.
[35] What is adware? The 5 examples you need to know, https://softwarelab.org/what-is-adware/.
[36] H.-W. Lee, Taking deterrence seriously: the wide-scope deterrence theory of punishment, Crim. Justice Ethics 36 (1) (2017) 2–24.
[37] T.S. Nixon, J. Barnes, Calibrating student perceptions of punishment: a specific test of general deterrence, Am. J. Crim. Justice 44 (3) (2019) 430–456.
[38] K.R. Reitz, Zimring, Hawkins, and the macro problems of imprisonment (Review of Franklin Zimring & Gordon Hawkins, The Scale of Imprisonment), J. Crim. Law Criminol. 87 (1997) 604, http://www.heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jclc87&id=614.
[39] G. Kleck, B. Sever, S. Li, M. Gertz, The missing link in general deterrence research, Criminology 43 (3) (2005) 623–660.
[40] M. Menegatti, Variability in punishment, risk preferences and crime deterrence, Int. Rev. Law Econ. 75 (2023) 106140.
[41] K. Kittichaisaree, K. Kittichaisaree, Future prospects of public international law of cyberspace, in: Public International Law of Cyberspace, 2017, pp. 335–356.
[42] J.X. Li, Cyber crime and legal countermeasures: a historical analysis, Int. J. Crim. Justice Sci. 12 (2) (2017).
[43] V. Adewopo, Exploring open source intelligence for cyber threat prediction, Ph.D. thesis, University of Cincinnati, 2021.
[44] The prevention of electronic crimes act, http://nasirlawsite.com/laws/peca1.htm, 2016.
[45] The prevention of electronic crimes act, https://na.gov.pk/PDF, 2016.
[46] Network access to Pakistan's top fed agency FBR sold on Russian forum, https://www.hackread.com/network-access-pakistans-top-fbr-russian-forum/.
[47] Computer Fraud and Abuse Act, 1866 (18 U.S.C. section 1030), https://www.law.cornell.edu/uscode/text/18/1030.
[48] K.M. Yilma, Developments in cybercrime law and practice in Ethiopia, Comput. Law Secur. Rev. 30 (6) (2014) 720–735.
[49] Egypt: president ratifies anti-cybercrime law, https://www.loc.gov/item/global-legal-monitor/2018-10-05/egypt-president-ratifies-anti-cybercrime-law/.
[50] K.M. Yilma, Ethiopia's new cybercrime legislation: some reflections, Comput. Law Secur. Rev. 33 (2) (2017) 250–255.
[51] Dagne Jembere, Alemu Meheretu, Implications of the Ethiopian computer crime proclamation on freedom of expression, Jimma Univ. J. Law 10 (2018), https://doi.org/10.46404/jlaw.v10i0.989.
[52] A guide to UK cybercrime legislation, https://www.ramsac.com/blog/cybercrime-legislation-uk/.
[53] L. Ivanova, Criminal liability for cybercrimes in the BRICS countries, BRICS Law J. 10 (1) (2023) 59–87.
[54] G. Wang, Criminal law regulation of countering cybercrime in China: state, trends and shortcomings, Vestn. Saint Petersburg Univ. Law (2022) 661.
[55] Criminal law of the People's Republic of China, https://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm.
[56] Computer Misuse Act 1990, Chapter 18, https://www.legislation.gov.uk/ukpga/1990/18/enacted.
[57] K. Wilson, Computer (MIS) use and the law: what's wrong with the CMA?, Ph.D. thesis, University of Oxford, 2019.