Journal of Social Sciences Review (JSSR) DOI: https://doi.org/10.54183/jssr.v3i1.181

How to Cite This Article: Pervaiz, H. S., & Bhatti, S. H. (2023). Analyses of Cybercrime Regulations Falling behind New Technologies. *Journal of Social Sciences Review*, 3(1), 460-469. https://doi.org/10.54183/jssr.v3i1.181

Analyses of Cybercrime Regulations Falling behind New Technologies

Hafiz Shahzad Pervaiz	PhD Scholar, Times Institute Multan, Punjab, Pakistan.
Shaukat Hussain Bhatti	Assistant Professor, Department of Law, Times Institute, Multan, Punjab, Pakistan.

Vol. 3, **No.** 1 (Winter 2023)

Pages: 460 – 469

ISSN (Print): 2789-441X

ISSN (Online): 2789-4428

Key Words

Information and Communication Technology (ICT), Cyber Security, Cybercrime, Cyber Assets, Cyberspace, Cyberbullying, New Technologies, Social Network

Corresponding Author:

Hafiz Shahzad Pervaiz

Email: shahzadmirza9760@gmail.com

Abstract: *Information and communication technology (ICT) and digital systems have developed to the point that they are indispensable to all industries, including Europe. The extensive use of preventative measures reflects the growing concern regarding cyber security. Concerns regarding cyber security in light of new technology are the primary focus of this review paper, which also discusses the problem of out-of-date cybercrime regulations. New technological advancements in cyber security, together with ethical considerations and external factors, are highlighted. To prevent sensitive data from falling into the wrong hands and jeopardising the security of the financial industry, the industry must continually analyse and improve its systems. In this review article, we examine more than twenty unique scholarly evaluations. The abstract and introduction comprise the first section of this review. In this review article, we discussed a variety of scholarly opinions on the topic as reviews. Typically, the final paragraph of an article includes a concise summary of the main arguments and supporting evidence presented in the body of the article. Moreover, security threats and challenges, as well as the most recent developments and emerging trends in cyber security, are discussed.*

Introduction

What typically comes to mind when we consider the things we wish to do in connection to those that technology was designed to facilitate? Most people would say that the initial intent of the notion was to make our lives easier and more enjoyable, which is still true in many respects today. Unfortunately, technology has also made it simpler for criminals to conduct crimes from the safety and seclusion of their own homes (Velasco, 2022). The term "cybercrime" is used to refer to any illegal activity that occurs online and uses a computer or other electronic device to do harm to others. As human existence becomes increasingly computerized in healthcare, education, and industry, more information, particularly sensitive data, is being kept. This is the case in each of these fields. Security is the process of protecting digital data from unauthorized access, modification, destruction, and disclosure. However, the volume and sophistication of cybercrimes are increasing at the same rate as the development of technology (Brands & Van Doorn, 2022). This significant development in cybercrime has been fueled by a number of factors, including high rates of financial return, a lack of public knowledge, and others. These include the usage of obsolete or insufficient software, security tools, design faults, programming errors, and readily available online hacking tools. In order to test the target for vulnerabilities and launch an assault, technical attackers are developing more complex attack tools (Velasco, 2022). This is an intentional assault against the victim. As a result, new forms

of attack are being employed, each with its own nuances that make it difficult to detect (Saada et al., 2021). Several reasons have contributed to the development of effective security algorithms, including the ever-increasing usage of the internet in every aspect of life, the digital nature of the large volumes of data generated by online transactions, and the decentralization of data repositories. Since cybercrime is inherently fluid and continually evolving, it is a perpetual balancing act to stay up with and combat emerging threats (Chert, 2015). Since sophisticated dangers play such an active role in the process, protecting cyberspace is one of the most difficult and difficult tasks. Consequently, it is essential to understand the fundamentals of defensive security mechanisms, as well as the different tactics and current hot topics in the field of information security (Saada et al., 2021).

Multiple state actors with diverse legal and cultural perspectives and strategic objectives will seek to exert influence across overlapping and overlapping domains of authority due to the broad nature of cyberspace. These domains of influence are the result of the varied strategic agendas of national actors. Since nations rely on the internet for communication and physical world supremacy, severing ties with it is impossible (Chert, 2015). As a result, cyberspace has an ever-increasing impact on the functions and obligations of international and national security agencies. Due to the global nature of software and hardware development, it is impossible to provide guarantees across the whole supply chain. The scalability of the cyber realm is what distinguishes it from other domains. Even under extreme conditions, a bomb's range is limited, whereas cyber threats can have far-reaching effects. As a result, we now have a mechanism to govern real-world actions. Similar to the majority of other fields of competence, cyberspace operations are primarily controlled by a small handful of individuals. Users have little control over the setup or functionality of the gadgets they employ. It is well-known that only a small number of individuals possess the skills necessary to efficiently control or manage cyber warfare (Rani et al., 2021). The cyber realm is too enormous to be mastered by a single person or organization, even if they devote their entire life and acquire unfathomable amounts of specialized knowledge. Due to the constant evolution of computing and communication technology, cyberspace is undergoing a fast transformation.

Cyber cohesion contributes to this acceleration. Every innovation introduces an entirely new period of vulnerability and adaptability. Cyberspace is incredibly dynamic and unlike any actual location (Chert, 2015). Cyber assets are widely scattered over a vast array of organizations, ranging from those that are closed and governed by the government to those that are privately owned and run. Each of these types of organizations possesses a distinct set of resources and facilities, as well as various capacities and concerns, all of which are present. The primary concerns posed by cyberspace include external threats, internal threats, supply chain risks, and low operational competency of local forces. Foreign intelligence organizations frequently employ cyber capabilities in their spying and information-gathering operations. Terrorists pose a threat to national security because they may target vital infrastructure in an attempt to cause widespread harm, cripple the economy, and undermine public faith. In a digital environment that is increasingly permeating every aspect of our public and private lives, it is vital that we have adequate levels of security. Without stability, the world as we know it will disintegrate.

Importance of the Study

Many parties are interested in the findings of this study since it will provide a novel perspective on social media users. Numerous businesses will profit from the research, particularly those that have had difficulty forming partnerships using cutting-edge technologies in the past.

Methodology

To learn more about the background of the previously published investigations, a literature review was conducted. Experts in qualitative research use a wide range of methods to analyse collected data, such as assessing, classifying, tabulating, and recombining information.

On the other hand, this study aims to learn more about the many sources, articles, and journals that are utilised throughout the data extraction and analysis phases, as well as the inferences and conclusions that are drawn from these activities.

Literature Review

The purpose of this section is to create a solid foundation for the subsequent analyses and interpretations of the study's findings by reviewing the current research of researchers.

According to Parker's article written in 2022 (Parker, 2022), more crimes have been perpetrated due to the widespread adoption, use, and growth of information and communication technologies. This has resulted in cybercrime becoming a significant issue for the international community. Cybercrime is merely one type of transnational crime affected by the globalisation of information and communication technologies (Parker, 2022). Four characteristics distinguish cybercrimes from their terrestrial counterparts: the ability to learn how to commit them quickly and easily, the low resource requirements relative to the potential damage they cause, the possibility of commission in a given jurisdiction without the offender's actual presence there, and the fact that, in many cases, no actual laws are broken. From this vantage point, the evolving nature of cybercrime presents governments and law enforcement agencies around the globe with new challenges. For this reason, it is essential to have strong domestic and international procedures in place to monitor how individuals misuse ICTs for illegal objectives online (Parker, 2022).

According to Doorn, Cybercrime is on the rise, and the majority of young people report becoming victims of it. Offline disruption or actual psychological issues are at the heart of cybercrime victimization, and it is vital to recognise the probable mental impacts on the younger generation as they blend their online and offline lives (Brands & Van Doorn, 2022). E-shopping, web publishing, virtual interaction, and digital downloading are among the most common Internet uses among college and university students. Expectedly, these behaviours were found to be connected with concerns about several types of cybercrime, such as malware with digital downloading, digital piracy with web publishing, cyberbullying with virtual involvement, and online scams with online purchasing.

According to the article (S. look, 2022) Cybercrime victims written by S. cook, Cybercrime victims were more likely to fit specific demographic features, such as being male, younger, urban-dwelling, unemployed, and having fewer offline social contacts. Invasion of privacy, sexual harassment, eve-teasing, molestation, cyberstalking, and the spreading of rumours and gossip about the girl child via social media with the goal of embarrassing and humiliating her are among the concerns associated with adolescent girls' usage of digital media (S. look, 2022).

Cybercrime is defined in an article by Reddy as "offences committed by individuals and groups against the individuals, groups, and organizations with criminal intent to intentionally damage, i.e. physical or mental harm to the victim directly or indirectly, who uses telecommunication networks such as chat rooms, emails, notice boards and groups, and mobile phones for SMS/MMS." Cybercrime, or crimes committed using computers, can be subdivided into various categories, including but not limited to: computer as a target; attacking other computers by infecting them with viruses and spreading malware; etc. The second category

of computer use involves the commission of more traditional offences, such as fraud or underground gaming (Reddy et al., 2022Reddy). Thirdly, a computer can be utilised as an accessory, which is a euphemism for the storage of material gained through illegal means

Julian Jang-Jaccard outlines the phenomenon in her article. Enhancing a nation's cyber defences and taking safeguards to safeguard its vital information infrastructure is essential to the stability and growth of the nation as a whole. Protecting Internet users and making the Internet a more secure environment have been crucial to the development of new services and government regulation (jang, 2020). According to one concept of the crime triangle, an approach to defining cybercrime, these are the three factors that must coexist for cybercrime to occur: a victim, a motive, and a window of opportunity (Jang, 2020). The victim is the intended receiver of the criminal's violent actions, and the opportunity is the window of time within which the criminal can actually commit the assault. A criminal act's motive is known as a motive (e.g., it can be an innate vulnerability in the system or an unprotected device). Even while attacks today are increasingly sophisticated and targeted at specific victims based on the attacker's goal, such as financial gain, espionage, coercion, or retaliation, opportunistic assaults that do not target anyone in particular are still rather common (Jang 2020). As their name suggests, opportunistic attacks are those that specifically target victims based on a perceived weakness.

This study recommends the use of Camellia, a block cypher with 128 bits of encryption. Camellia stands out not just for the security it offers but also for the speed with which it can be deployed on various computer systems (Saada et al., 2021). Camellia has been demonstrated to be an effective countermeasure against differential and linear cryptanalysis. Camellia provides a multi-step technique for undertaking experimental risk evaluations. Software and hardware encryption speeds are at least as quick as those of AES. Injuries can manifest themselves in a person's life in five primary ways: their capacity to function, their access to basic requirements, their ability to maintain a sense of dignity and pride, their loss of control over their own lives, and their damage to their public image. In addition, they explore the domino effect of harm by analysing actual crimes that had a significant impact on society, and they create a five-level scale for the different types of harm (Saada et al., 2021).

In his article, Chertoff examines the present state of Internet jurisdiction law and the challenge of allocating jurisdiction to a single venue when numerous jurisdictions are involved in a dispute (Chert, 2015). They present four distinct formulations for finding the dominant jurisdiction in a given circumstance in a transparent and equitable manner. The location, the nationality of the data producer, the nationality of the data holder or custodian, or some combination thereof, determines which set of laws applies to a given piece of information, data, or system (Chert, 2015).

According to Mathieu and Guy, a high-quality literature review undertaken by an individual provides credible information and insights on previous research, allowing other researchers to follow new routes on relevant subjects of interest. In addition, the results of this study could be used as a reference in related fields or as a beginning point for other research. The author asserts that hacker-activist organizations have attacked internet security with the intent of inflicting harm on web services in a particular context. The author discussed a method for conducting sentiment analysis with Twitter posts. The author's technique was based on a compilation of tweets produced daily by persons who discuss current events and distribute links to cyberattack-related content. The acquired data were transformed into information that could be statistically analyzed to determine the possibility of an assault. The latter was made possible by studies on how users and hacktivist organisations

reacted to a global event. In his study, Edwards uses a Bayesian Generalized Linear Model to analyse a publicly accessible dataset of data breaches. The ultimate objective of this study is to uncover common patterns in security events. Despite the fact that the total number and frequency of data breaches have remained relatively stable over the past few years, the damage caused by each event is growing. The volume of electronic financial transactions is increasing, and threat actors are becoming more adept at converting stolen personal information into cash. In a survey study, it is asserted that a comprehensive literature analysis of machine learning and data mining approaches to cyber analytics in support of intrusion detection has been conducted.

In their study titled "cybercrime attacks," H. Lee, Lee, and colleagues discuss cyberattacks. Key loggers are a prevalent form of attack weapon; they record every keystroke a user makes and can be downloaded for free from the Internet. As the prevalence of key loggers has increased, numerous new attachment mechanisms have evolved. The report's author said that defending key human and commercial systems demands the most up-to-date knowledge of cyber security's threats and weaknesses (Rani et al., 2021). There are numerous open and hidden sources of information regarding these threats, including the National Vulnerability Database, CERT alerts, blog posts, social media, and black websites. Other attempts concentrate on risk framework creation and modelling business system resilience. By analysing the interconnectedness of diverse assets, researchers can utilise these models to study the topic of how natural disasters might disrupt essential services on a worldwide scale. Each danger is connected with its own destructive process, its own vulnerability, and its own set of challenges to the system's overall resilience, and this information is utilised to construct a threat-based model. To make any progress, it is necessary to devise strategies for tackling such a formidable obstacle.

Nguyen presents a new strategy based on the "top-down" paradigm described in criminology. Customers may be ready to pay "premiums" to prevent malicious software from endangering their assets. Our current understanding of cyber security is mostly dependent on information derived from commercial threat reporting and media sources. This information, however, only portrays a restricted and skewed image of the activities around cyber dangers, as it is frequently politicized and controlled by the needs of influential clients and the interests of competent suppliers.

Mellado, D.; Mouratidis Protection has not been thoroughly explored. The majority of strategies concentrate on extending the SPL to include additional safety-related elements and conditions. In the early stages of the production process for the product line, several distinct approaches were utilised to manage variability and define safety standards. Cyberattacks can jeopardise patients in many ways, including by compromising data or interfering with the performance of medical devices. Recent examples include the Wanna Cry and Not Petya ransomware attacks and the flaws discovered in the software used to operate implanted cardiac devices by Medtronic.

According to many article reviews, although hacking is not expressly covered, there are numerous other potential hazards to the safety of the elderly that are not addressed in this article. The elderly and adolescents are particularly vulnerable since they are the least likely to be aware of the existence of criminals. Traditional solutions, as well as the use of analytical models, machine learning, and big data, could be improved, according to the article's author, by giving pertinent knowledge to mitigate or restrict the effects of risks.

Cyberbullying and online harassment are typical examples of cyber-enabled crimes,

whereas computer security issues such as malware infections, infestations, and the theft and exploitation of personal data are examples of cyber-dependent crimes. Cyberbullying and online harassment are two types of cybercrime. A paper describes a method for monitoring social media data and presenting it in a format that can be utilized to carry out cyberattacks.

Mohsin, M.; Anwar, A., et al. Cyber security professionals face the difficulty of determining whether the tried and true approaches of feature models can be adapted for use in cyber security. Here, we describe a strategy to improve the generation of secure software product families and their progeny (SPLs). This research provides a bird's-eye view of the cyber security concerns that have emerged as a result of recent technological and inventive advances, to quote MdLiakat Ali. In addition to focusing on new ideas, advances, and ethical considerations in cyber security, this presentation's primary emphasis is on these topics.

K.T., Kutub Thakur In the past, cybersecurity and knowledge security were used interchangeably. In the past, humans were viewed as an additional element in the safety process; however, this is no longer the case in cyber security. The moral fabric of a society is reflected in a debate with far-reaching effects on cyber security. Numerous approaches and options have been developed to address cyber security.

In Pawlak et al., the evolution of threats and government security are analysed and compared (2013). They conclude, after much discussion, that governments everywhere must do more to bolster the fundamental capabilities of their populations to protect themselves and their nations from external dangers. The results of their inquiry led to this conclusion. Concern exists that governments may lag significantly behind in terms of cyber security. In addition, based on the findings of a second study, they emphasize the significance of eight changes that will impact the future evolution of cyber security risks. Examples include cloud computing, large data storage, IoT, mobile internet, neural interface, contactless payments, mobile robots, quantum computing, and cyberspace weaponization. In conclusion, they propose the development of a model depicting the future relationship between the public and private sectors.

Franke et al. (2014) examine 102 publications from IEEE Xplore, Scopus, Springer link, and Web of Science to build a cyber situational awareness research agenda. Topics span from game theory and cognitive science to detecting weaknesses and attacks, as well as more fundamental introductions. In addition, they include multiple works on "visualisation" for cyber situational awareness; certain conceptions of emergency management; various tools, architectures, and algorithms on a vast array of topics, including attribution; etc. Despite the widespread interest in cyber situational awareness among policymakers, in collaboration (in multiple senses), in information exchange, and in military strategy, researchers have observed a paucity of publications in areas such as national or other high-level cyber situational awareness. The study of ICSs is advancing rapidly, and this has obvious implications for the advancement of cyber situational awareness.

Thus, "computer crime" comprises not only illegal use of the Internet but also any criminal activity involving the use of computers and networks. Cybercrime consists of activities such as fraud, theft, extortion, forgery, and embezzlement, and its genesis is often a computer or computer network. Cybercrime is extraordinarily difficult to identify and punish because of its technical complexity and the fact that its offenders are sometimes unnoticed and located thousands of kilometres away. The nature of cybercrime and its capacity to change with technology means that new dangers are emerging with alarming frequency, making it more difficult for users to cooperate with one

another, which may undermine the security and financial health of a nation (Kulshrestha et al., 2022).

Discussion

Cybercrime Legislation in the Modern Era

The majority of contemporary economic, commercial, cultural, social, and governmental activities and contacts between nations at all levels occur in cyberspace. This covers the work of people, non-governmental organizations, and government and government agencies. Economic, commercial, cultural, social, and governmental are the seven broad categories into which these processes and exchanges can be sorted (Nguyen, 2023). Cyber-attacks and the hazards of wireless communication have recently become major concerns for a vast array of private businesses and government agencies throughout the globe. Due to the dependence of modern civilization on electronic technology, security against malicious cyber-attacks is a primary concern. Companies are targeted in cyber-attacks because hackers want to lose money on the venture. In other instances, cyber-attacks may be conducted for political or military reasons (Nguyen, 2023). These damages can be caused by a wide range of risks, such as computer viruses, knowledge breaches, the data distribution service (DDS), and other attack vectors (Parker, 2022).

Many various types of organisations and organisations utilise many different kinds of safeguards to get the job done. When it comes to cyber security, nothing beats up-to-the-minute data and information. Researchers from around the world have created a wide variety of solutions to prevent or lessen the impacts of cyberattacks. Some of the solutions have been implemented, while others are currently undergoing testing and development (Nishnianidze, 2022).

Investment in cybersecurity is increasingly vital for enterprises to maintain the availability, integrity, and secrecy of their digital assets and the survival of the business in the face of such a risky climate. This gives a background for why such investments are now an important decision for all businesses. However, anecdotal evidence and field practitioners indicate that an inadequate level of cybersecurity exposes an organization to a higher risk of a successful attack and higher overall costs, so it is uncertain whether the rising costs due to cyberattacks are dependent on investments in countermeasures.

The Cyber-attack Impact Assessment Technique

It, presented in detail by Genge, has the potential to function as a flexible tool for analysing the effects of cyber-physical system attacks. This discovery would have far-reaching implications for the safety of cities and countries, even if the study did not specify how it may be implemented. Examples of major forms of cyberattacks include "denial of service," "logical bomb," "abuse tools," "sniffer," "trojan horse," "virus," "worm," "send spam," and "botnet."

In a denial-of-service attack, access is blocked to legitimate users while malevolent users get access. In actuality, the attacker bombards the targeted machines with messages before ultimately obstructing the data that should be allowed to pass (Li & Liu, 2021). As a result, no system can access the Internet or communicate effectively with other computers (Nishnianidze, 2022). Widespread denial of service is another methodology, which differs from the traditional method in that, rather than launching an attack from a single place, attackers employ a large number of geographically dispersed systems to launch an attack simultaneously (Kulshrestha et al., 2022). Worms, which propagate to other computers before executing an assault, are frequently deployed in this context. The public has access to abuse tools that can scan for security weaknesses and get varying degrees of access to networks. Logic bombs are another type of cyberattack; they are pieces of code put into a programmer with the goal that it will execute harmful code if a certain circumstance is met. Sniffer is a

programme that not only spies on data in transit but also analyses each packet in the data stream in search of specific data, such as passwords (Guryanov et al., 2022). Trojan horses are a type of malicious software that disguises themselves as useful programmes in order to trick users into installing and running them (Li & Liu, 2021). A virus may also infect your system by embedding a duplicate of itself within a system file.

Knowledge of Cybercrime and Experience with Legacy Computer Systems

Cybercrime is one of the most pressing issues in the Internet Age. Understanding the many types of cybercrime and being prepared to defend against them in the future is vital.

May & Bhardwa, 2018 utilised a software (not actual) installation test to measure the students' level of cybercrime knowledge in their article. Surprisingly, the majority of pupils were interested in computer technology, and over 80 per cent of students agreed to instal a harmful application on their computers. In addition, the vast majority of pupils identified with computer science (May & Bhardwa, 2018). In addition, there is a widespread lack of awareness and irresponsibility among young internet users regarding the security of the information they store on their portable electronic devices. It is hardly surprising that inattentive computer users leave themselves vulnerable to hacking attempts by hackers; carelessness is a characteristic of the human condition (Nguyen, 2023).

Conclusion

Cyberspace and its closely connected technologies are one of the most significant sources of energy in the 21st century. Cyberspace's characteristics, such as accessibility, anonymity, vulnerability, and asymmetry, contribute to the dissipation of power. Other parties, including private businesses, organised terrorist and criminal groups, and individuals, must now play a larger role in the power game than governments have up to this point. This occurrence is unlikely to threaten the security of any nation, at least not significantly. Cyberattacks can do a great deal of harm since they occur without warning, have multiple layers, and target important systems and networks. Fourth, traditional measures, such as the military and the police, are insufficient to combat these dangers, as are sovereign states acting alone. Instead, governments and corporations must collaborate successfully because they have a vested interest in avoiding or mitigating the effects of these dangers. He threatens you if you do not comply with his requests. As demonstrated in the previous paragraph, the effects of cyber hazards are not confined to governments; individuals, corporations, and other organisations are also in danger. In addition, it is easy to overlook or misunderstand the numerous theoretical approaches to international relations whose foundations are mostly centred on governments because security in the digital age is not just the responsibility of governments. Institutions such as schools and courts must undergo a period of adaptation whenever a new piece of technology reaches the mainstream. Both the government and our educational system must implement the appropriate cybercrime protection tactics and procedures.

Youth and regular Internet users should engage in safe and conscientious work practises, enhance their level of awareness, and cultivate their cognitive talents and perceptual acuity to lower their chance of being victims of crime. Administrators or owners are ultimately responsible for maintaining the security of their sites. This can be achieved by using measures such as raising password strength and installing additional monitoring equipment. Numerous research findings have been analysed, and it has been determined that cybercrime can be prevented by raising the awareness of young people through the educational system, bolstering the government's policing apparatus, and punishing those who disobey the law. Our

literature review revealed that the lack of a good educational foundation, the small number of formalised research approaches, and the emphasis on cryptography all pose challenges for the cybersecurity industry as a whole. Its consequences are not limited to the academic realm or the economy it supports; they are felt globally. Using research methodologies and instructional practises to define a problem of this nature is, to put it mildly, tough. There are, however, steps that can be taken to accelerate and enhance the quality of a study. Standardizing academic language is one of a number of measures made to enhance communication between scholars. Raising the standard of research is another possible strategy. Beyond the sphere of technical competence, there is almost no consensus on a standard vocabulary for expressing cyber security challenges. Despite being the most formalised aspect of cyber security, certain practical implementations of private key encryption, such as AES, rely on public consensus rather than precise mathematical proofs

Availability of Information Explanation

Every author associated with the featured studies is strongly encouraged to offer researchers free access to their data. Through Google Scholar, we have access to the datasets we utilised or developed for this study, as well as any other pertinent material that could be used to validate the study's conclusions. Write "the authors declare no conflict of interest" if there is no chance for a conflict of interest to occur. The author is responsible for ensuring that their responsibilities are met. The extent of the sponsors' participation in the study's inception, processes, data interpretation, writing, and publication decision must be made absolutely clear.

References

Brands, J., & Van Doorn, J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior*, *127*, 107082. https://doi.org/10.1016/j.chb.2021.107082

Chert. (2015). *Revitalizing the Rule of Law: Examining the Success of the Arab Spring - ProQuest*. Www.proquest.com. https://search.proquest.com/openview/e00b725291c1b8e8002c120f93048528/1?pq-origsite=gscholar&cbl=32013

Cook, S., Giommoni, L., Pareja, N. T., Levi, M., & Williams, M. L. (2022). OUP accepted manuscript. *British Journal of Criminology*, *63*(2), 384–406. https://doi.org/10.1093/bjc/azac021

Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in "real world" policing and law enforcement. *The Police Journal: Theory, Practice and Principles*, 0032258X2211075. https://doi.org/10.1177/0032258x221107584

Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law & Security Review*, *41*, 105528. https://doi.org/10.1016/j.clsr.2021.105528

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*, *2*(1), 1–18. https://doi.org/10.3390/jcp2010001

Jang. (2020). *Julian Jang-Jaccard*. Scholar.google.com.au. https://scholar.google.com/citations?hl=en&user=AsTWD0UAAAAJ

Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *PLOS ONE*, *15*(1), e0227800. https://doi.org/10.1371/journal.pone.0227800

Kundi, G., Nawaz, A., & Akhtar, R. (2020). *Digital Revolution, Cyber-Crimes And Cyber Legislation:*

A Challenge To Governments In Developing Countries. 4(4). https://core.ac.uk/download/pdf/234677092.pdf

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7(7), 8176–8186. ScienceDirect. https://doi.org/10.1016/j.egyr.2021.08.126

Narasimhan, P. (2023, January). *Most Extensive Cyber Security Challenges & Solutions in 2023*. Www.knowledgehut.com. https://www.knowledgehut.com/blog/security/cyber-security-challenges

Parker, S. T. (2022). Measuring gun violence in police data sources: transitioning to NIBRS. *Injury Epidemiology*, 9(1). https://doi.org/10.1186/s40621-022-00376-8

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, 2(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Rand. (2021). *Technology and the future of cybercrime*. Www.rand.org. https://www.rand.org/randeurope/research/projects/technological-developments-and-the-future-of-cybercrime.html

Rani, S., Kataria, A., Sharma, V., Ghosh, S., Karar, V., Lee, K., & Choi, C. (2021, April 28). *Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey*. Wireless Communications and Mobile Computing. https://www.hindawi.com/journals/wcmc/2021/5579148/

Reddy, K. C., Divya. B, & M, V. (2022). Cyber Crime against Women in India. *European Journal of Humanities and Educational Advancements*, 64–69. https://www.scholarzest.com/index.php/ejhea/article/view/2492

Saada, A., Abdel-Kader, H., & Ali, A. (2021). Enhanced Security System of Internet of Things data streaming. *IJCI. International Journal of Computers and Information*, 8(2), 144–150. https://doi.org/10.21608/ijci.2021.207860

Velasco, C. (2022). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the applicable international instruments. *ERA Forum*. https://doi.org/10.1007/s12027-022-00702-z

Vuggumudi, S., Wang, Y., Ragothaman, K., Noteboom, C., & Liu, J. (2022). Improving the Effectiveness of Security Controls to Prevent APT Attacks. *Faculty Research & Publications*. https://scholar.dsu.edu/bispapers/305/