# Cyber-Crime and Cyber-Security are Two Sides of the Same Coin. A Critical Discussion on these Concepts based on Practical Examples which Happened in Zimbabwe Over the Past 6 Years.

**Ladislous Mutambanashe**

**DOI: https://dx.doi.org/10.47772/IJRISS.2023.70701**

**Received: 06 June 2023; Revised: 20 June 2023; Accepted: 26 June 2023; Published: 24 July 2023**

## INTRODUCTION

Cyber-crime and cyber-security are contemporary broad areas that handle issues to deal with computers and networks. Many people suggest that "cyber-crime and cyber-security are two sides of the same coin" and this paper intends to dissect and give informed comments concerning this statement. Cybercrime is a 21st criminal behaviour, an anti-social behaviour that manifests itself in the cyberspace where as the cyber security is a concerted effort to combat the cybercrime. The concepts are divergent in the sense that when cybercrime is on the increase it entails failure on the part of cybersecurity. On the other hand, cybersecurity effectiveness can be seen through decrease in cybercrime. This write up will deliberate on the relationship between cyber-crime and cyber-security mentioning areas where they converge as well as outlining their main differences. This stems from the fact that global connectedness requires in-depth understanding of the consequences of cybercrimes, this will trigger attention to detail in respect of mechanisms that should be put in place to improve cybersecurity. Cybersecurity is one of the major contemporary facets in the world that has to be providing high end solutions to the ever changing technological and cyberspace. The paper provides the key definitions, provides overview of the concept of cybercrime and cybersecurity. It will then provide a discussion on the cybersecurity and cybercrime, highlighting their divergence as well as providing relevant examples. The paper then provides a comprehensive conclusion and provides recommendations as predicted by the discussion.

## DEFINITION OF KEY TERMS

**Cyber** relating to or characteristic of the culture of computers, information technology, and virtual reality.

**Cyber-crime** is a crime where a computer is the object of the crime or is used as a tool to commit an offense (Humphrey, 2012).

**Cyber-security** is the protection of internet-connected systems such as hardware, software and data from cyber threats (Lee, 2017).

## OVERVIEW OF THE CONCEPTS

### Cyber-crime concept overview

Cybercrime is vastly growing in the world of technology today. Criminals of the World Wide Web exploit internet users' personal information for their own gain. Criminals use dark web to buy and sell illegal products and services. Cybercrimes are costing companies and individuals billions of dollars annually. The evolution of technology and increasing accessibility of smart tech opened multiple access points within users' homes for hackers to exploit. While law enforcement attempts to tackle the growing issue, criminal numbers continue to grow, taking advantage of the anonymity of the internet.

**Major types of cybercrimes perpetrated in Zimbabwe**

Cybercriminals use a variety of techniques to defraud individuals and businesses, including card cloning, identity theft, cyberwar fare, WhatsApp hacks, social media prepayment scams, corporate account hacks, phishing scams, and hot airtime charge scams. Sitemere (2022) also correctly mentioned that the international remittance sector faces several significant risks, including money laundering, fraud, terrorist financing and sexual exploitation. Cyberbullying is also a cybercrime that harasses people through electronic means. Zimbabwe's celebrities, business owners and executives have long been victims of cyberbullying, cyber-harassment and revenge porn. Most cyberbullying takes place on media sites such as Facebook, Instagram, Twitter, and WhatsApp. Cyberbullying occurs through devices such as mobile phones, computers, and tablets. This includes posting, transmitting or sharing harmful, false or hateful content about others to extent of damaging an entity's reputation, poising a financial risk.

Social media also remains a favoured target of scammers, as criminals seek to leverage the trust people have in their own social circles. Social media is quickly becoming a daily part of life in Zimbabwe; following a global trend. In social media generated cyber-crimes, criminals take advantage of the sharing facilities and present fake products, video links and "like" buttons which they use to spread their scams. Users are also lured into clicking fake website buttons that install malware with some posting updates on a user's newsfeed, spreading the attack. This may end up in identity theft or denial of service.

**Cyber-security concept overview**

The cybersecurity field include application security, information or data security, network security, disaster recovery/business continuity planning, operational security, cloud security, critical infrastructure security, physical security and end-user education (Lee, 2017). Maintaining cybersecurity in a constantly evolving threat landscape is a serious challenge. Traditional reactive approaches, in which resources were put toward protecting systems against the biggest known threats, while lesser known threats were undefended, is no longer a sufficient tactic. To keep up with changing security risks, a more proactive and adaptive approach is necessary.

Cyber resilience and end-to-end protection in the financial services ecosystem cannot be overemphasized. Cybersecurity is now more than a powerhouse to understand many of the tricks and techniques behind the most popular scams. Zimbabwe's increased use of mobile money, online banking and shopping during the COVID-19 lockdown has increased the need for cybersecurity. Cybercrime and computer crime are on the rise in the country due to cyber incidents related to money fraud, card duplication and identity fraud.

Furthermore, according to the 2020 National Risk Assessment (NRA) report, cyber risks, primarily through digital financial channels, have resulted in an estimated US$900 million in illegal proceeds from criminal activity in Zimbabwe annually. To combat cyber-attacks and ensure better data protection, the Government of Zimbabwe implemented a Cyber Security and Security Policy in 2021 aimed at providing minimum requirements that institutions shall build upon in the development and implementation of strategies, policies, procedures and related activities aimed at mitigating cyber risk in developing digital economy. The government also passed the Data Protection Act (Chapter 11:22) Number 5/2021 (Fintech, 2022). Cybersecurity is known as a set of guidelines and conduct to prevent crime (Lee, 2017). There are various forms of cyber security breaches that leads to the perpetration of cyber-crime. This paper touches on the following cybersecurity breaches.

**Ransomware**

Ransomware is a type of ill-disposed software that is used by cybercriminals to block victims from accessing their data (Wazid, Zeadally & Das., 2019). These digital variety extortionists encrypt victim's files and add extensions to victim's data and then hold it hostage until the ransom is paid. Ransomware is illegal because the user captures victim's data and demands a ransom fee.

Malware attacks against educational and corporate websites have been reported in Zimbabwe, inclusive of the Herald Newspaper, government, NUST and Harare Institute of Technology. This reflects the reality of the threats on Zimbabwe's doorstep. Businesses and banking systems have also also fallen victim to hacking (breaking into and using computer systems), allowing individuals to steal large sums of money. The case of a Chitungwiza man who hacked OK Zimbabwe Money Wave system and subsequently stole US$70,000 is a good example of such cybercriminal activity (Chindaro, 2017). For example, in 2017 the National University of Science and Technology's website was hijacked by hackers who demanded a ransomware of $6 billion United State dollars. This revealed that the cyber security of this University are not watertight.

**Viruses**

Viruses are the most common method of breaching cyber security (Lee, 2017). By the use of viruses cyber criminals may take control of an account by sending email attachments or even through a flash drive. For example, there has been an increase on the number of hackers who are using coronavirus to spread a computer virus. The emails from such hackers contain an attached document that include new developments on the coronavirus spread.

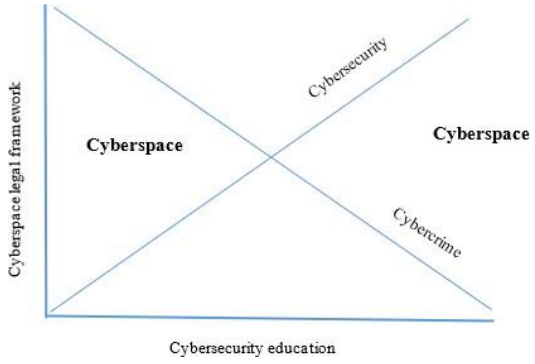
**SQL Injection**

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (Wazid et al., 2019). A Chinhoyi University of Technology student was arrested after hacking into the University's results portal and altering grades for himself and other students. The students used a technique called SQL Map which is an SQL injection technique to hack into the institution's database.

**Distributed Denial of Service Attacks**

For several days, starting on Monday 14 January 2019, Zimbabweans went without Internet access. This was as a result of the Southern African country's government, under rumoured instructions from the responsible authorities that decided to threaten and ordered all four of the country's telecommunications to shut off the internet completely. The Zimbabwean internet shutdown followed a week of protests by Zimbabweans against the rise in fuel price and the high cost of living in the country.

**Diagramatic presentation on the relationship between cybercrime and cybersecurity**




The Figure 1 indicates that as the availability of cyberspace legal framework and cybersecurity education improves, it bears fruits of reduction in cybercrime and also enhances overall cybersecurity. This entails that there is need to foster robustness in the promulgation of responsive legal framework in the cyberspace and promoting appropriate cybersecurity awareness and education. The diagram also reveals the relationship cyber-crime and cyber-security as two sides of the same coin, a head and tail situation. They do not move in same direction, factors that enhances cybersecurity have an negative impact on cyber criminals. On the other hand, factors that promotes cybercrime on the other hand affects effectiveness of cybersecurity.

Cybersecurity is the practice of defending government or corporate computers, servers, networks from malicious attacks and threats and keeping information like data safe and secure from unauthorized access. While cyber-crime is about exploiting human or security weaknesses in systems to steal data, money or passwords or engage in fraud schemes.

**Discussion on cyber-crime and cyber-security**

In order to reveal that cyber-crime and cyber-security are issues that are found in the same environment but operating differently, there is need to highlight their main differences.

**The Victims**

Cybercrimes and cyber security both have victims. These victims differ based on what crime was committed. With cyber-crimes, it is generally individual or group of individuals. With cyber security, the most concerned parties are government or corporate. Individuals can suffer substantial financial loss from cyber-crime. The greatest impact being theft including theft of intellectual property. Average people are on their own when it comes to securing computers and devices (Yar, 2012). These personal attacks cause chaos and computer distress. It is proven that large corporations can recover from an attack much easier than that of an individual.

For instance individuals who had their debit cards cloned by Chinyemba suffered a loss they failed to recover. Chinyemba and his company “cloned” POSB debit cards and managed to steal Z$3 million. These thieves stole card data including the name, along with the credit card number and expiration date through skimming and shimming. Skimming frequently happens at ATMs and it also can occur when a person hand a card over for payment especially out of sight. In that brief moment, the cashier skims card data with a handheld device.

On the other hand, cybersecurity is vital to a corporation because it comprises everything relevant to the protection of their sensitive data. Cybersecurity is primarily interested in preventing damage and theft that is attempted by cyber criminals. Government and corporation leaders must educate themselves and staff on scams like phishing and ransomware attacks since it causes irreversible reputational damage. Therefore cyber security practitioners concentrate on building capacity to defend against cyber-attacks and providingcyber security tools, incident response services, and assessment capabilities to safeguard and enhance the confidentiality, integrity and availability of data. This entails that organisations should have valuable, rare, inimitable and non-substitutable capabilities so as copy up with rapid development in new technologies such as the Internet of Things and Artificial Intelligence that could produce new security threats.

**The Principles**

The founding principle of cyber-crime law is to punish criminals who have unauthorized access to computer systems with a delinquent intent. This is to prevent damage and change of systems as well as the data on the electronic environment. For instance, the Cyber and Data Protection Act (Chapter 12:07) amended section 163 of the Criminal Law (Codification and Reform) Act (Chapter 9: 23) and now provides offence for hacking in that a person who (a) knowing or suspecting that he or she must obtain prior authority to access the data, computer programme, computer data storage medium, or the whole or any part of a computer system in question; and

(b) intentionally, unlawfully and without such authority, secures access to such data, programme, medium or system; shall be guilty of hacking and liable (c) in any of the aggravating circumstances to a fine not exceeding level 14 or to imprisonment for a period not exceeding ten years or both such fine and such imprisonment.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS |Volume VII Issue VI June 2023

On the other hand, cybersecurity explains the high-tech advance to securing systems from attack or failure. Acceptable cyber security principles are identified with the fact that all computer systems contain a certain level of susceptibility and address the root causes of insecurity, by computing then identifying and fixing those susceptibilities. For instance, the Cyber and Data Protection Act (Chapter 12:07)'s long title provides that it was enacted to establish a Cyber Security Centre; a Data Protection Authority and to provide for their functions as well as to create a technology driven business environment and encourage technological development and the lawful use of technology. This is an eloquent testimony on the need to have cybersecurity measures in place.

**Human Rights**

Cybercrime and cyber security both value human rights, though they express it in different ways. In cyber-crime they use cyber-crime laws to build legislation with human rights protection and defence. Cybercrime law should align to a country's constitution and line up with international responsibilities to protect human rights. The Cyber and Data Protection (Chapter 12:07) was also established as an Act to provide for data protection with due regard to the Declaration of Rights under the Constitution of Zimbabwe. It is also however, important to mention that the perpertrators of cybercrimes infringes the victims' human rights. These rights can only be protected if there is in existence adequate laws that punishes deviant behaviour in the most appropriate manner.

While cybersecurity arranges, protects, and safeguards individuals, networks and devices, such policies must have individuals and their rights at the heart of its operations. These policies must pursue to protect and strengthen human rights rather than make them less significant.

**The Framework**

The framework, or the basic structure underlying within a system, is existent in both cyber-crime and cyber security. They are firmly established in their structural beliefs. With cybercrime laws, they lay the foundation for far-reaching legal frameworks around "cyber-enabled crime" (Ibrahim, 2016). This is referring to entrenched crimes committed in a new way by using technology such as the distribution of child pornography. As an example, the distribution of child pornography is a crime no matter the criminal is using a computer or not, it will be supported by the exhaustive efforts of child protection legal framework.

In contrary, cyber security builds a cyber-security "framework" rather than one law in seclusion (Ibrahim, 2016). Cybersecurity is comprised of different approving actions and approaching legislation, as one of the elements to it. Most elements of cyber security depend on non-legal structures. They have minimum guidelines of security, assets in security, research, and security audits of public bodies and key industries. Government policy in this field can make a true difference in elevating the standard of security.

**The Interpretations**

Cybercrime and cyber security both interpret this form of cyber activity on different levels, however, they are both straightforward with how they come to classify these cyber activities. In cyber-crime, this is used to narrowly interpret cyber-crime. The founding principle is that of punishing unauthorized access such as breaking into the computer system (Ibrahim, 2016). Whereas in cyber security they interpret by placing the efforts in a suitable threat assessment. A threat assessment acknowledges possible weaknesses such as outdated infrastructure that make a country more accessible to an attack and they aid in setting up and decision making.

**The Infrastructure**

Another form of attack is an attack organized by one nation against another nation's institutions and

infrastructure. A form of cyber warfare. This is where one country infiltrates another country's computers and networks to cause harm, cause disruption, or obtain sensitive security information. In such attacks, nation states seek to disrupt the activities of organizations or other nation states for strategic or military purposes and cyber espionage. Cyberspace and its fundamental infrastructure are exposed to a wide variety of risks. Cybercrime and cyber security both do their part to protect it. Cyber intrusions are becoming more common place, more dangerous, and more sophisticated. The nation's vital infrastructure regarding both private and public sector networks are targeted by antagonists. The Ministry of Defence and Security is transforming itself to address universal and growing cyber threats. The Zimbabwe Republic Police's Cyber Division investigative dimensions are being enhanced to strengthen its focus on intrusions into private and government computer networks. The key priorities include computer and network intrusions, ransomware, identity theft, and online predators.

In relation to cyber security, practitioners identify and engage in fault finding infrastructure. This refers to the important systems by which their loss or damage would have a considerable impact on the performance of the state as well as the safety of the people. Some examples would include banking, health, digital, financial market and energy infrastructure. For instance, imagine the effect that has been felt whenever there an EcoCash mobile banking infrastructure disruption which disables all associated services such as mobile money transfers even just for a day or disrupts Econet, Telecel or TelOne mobile communication. The disruption usually results in a substantial damage to the economy. Hence, we witnessed the outcry that accompanied the disruption of WhatsApp services for a few hours on 25 October 2022 whereby over 2 billion users who rely on WhatsApp for communication and payments were affected around the world. This is a taster of the potential effect of cybercrime on everyday life on on the cyberspace and importance of cybersecurity.

Terror groups which fall in the terrorism financing cybercrime have also been taking advantage of social media to further their goals and spread their message presenting governments with another frontier for cybersecurity. Investigations into such cybercrime and attacks, like the one witnessed in Kenya Westgate Mall revealed the use of social media and computer networks in planning and co-ordinating the terrorism attacks.

In December 2016, Ukraine experienced a blackout as a result of cyber-attacks on electric power distribution companies. Most recently, and still ongoing are allegations of Russian interference in the USA elections through cyber activities. The WikiLeaks case which also affected Zimbabwe is a typical highlight of another form of cyber-espionage. These incidents have brought into light, situations which used to be viewed as science fiction.

**How They Establish Response**

Cybercrime and cyber security have their way of handling and responding to the issues that go twisted from a cyber- attack. Cyber-crime investigators understand that a cyber-attack could go on completely undetected for a long time hence it is important to routinely perform monitoring and diagnostics to support early detection and resolution (Humphrey, 2012). In case of an incident there is need to prioritize by secluding the incident and discovering its impacts. It is critical to know of the enterprise network environment so as to decide if the correct response should include a full investigation, following the cyber-crime response plan. The investigation needs to be started and conducted in a secure environment with the utmost urgency. There is also need to eliminate repetitive crimes through putting plans that are organized and conducted with speed being precise because the attacker may try to infiltrate again (Vito and Maahs., 2015). There will be also need to provide a report giving resolutions on things such as insurance claims, litigation threats, intelligence and customer notification.

On the other hand, cyber security establishes incident response teams. This team contains experts on the battlefield. They can detect when security is threatened. They deal with devices that have been jeopardized and even services that are allowing cyber-attacks to transpire.

**Academic programs to start a career in these fields**

To begin a career in cyber-crime or cyber security, one must invest their education into certain areas of study (Vito and Maahs., 2015). It is important to possess a degree in these associated fields to become a cyber-crime investigator or to become a cyber-security practitioner. To start a career in cyber-crime, a person must study in the areas of criminology, psychology and sociology. Within the field of criminology, they use theories to explain delinquent behaviour. The use theories such as social learning theory and low self-control theory. The psychology aspect of learning is invested in profiling cyber criminals (Yar, 2012). By looking back and applying psychological research to study people's behaviour and observing the predetermined factors that lead an individual to commit a cyber-crime.

The academic programs for a career in cyber security are Computer Science, Computer Engineering and Information Technology (Yar, 2012). With Computer Science, the focus is on building new features and software. A cyber security specialist would include auditing security systems, setting up firewalls, reporting data breaches and analysing networks. Cybersecurity is a critical part of the broad field of Computer Science. Computer Engineering provides the importance of learning about the hardware and software of the computer (Yar, 2012). They learn to protect sensitive data of businesses from hackers and cybercriminals alike. Information Technology involves the security and protection of computer systems as well as the prevention of changes or unauthorized use. These studies are used to maintain confidentiality and integrity.

## CONCLUSION

From the discussion that ensued it was indeed discovered that cybercrime and cyber security are two sides of the same coin. While the terms 'cybersecurity' and 'cybercrime' are interrelated and their interests often intersect, their meanings are not identical, and the scope of what constitutes 'cybersecurity' and 'cybercrime' varies from technical, legal and political perspectives. It was clear that cybercrime perpetrators and investigators operate in the same cyber space with the cyber security practitioners. Cyber security practitioners aspire to have a cyber space that continues to inspire confidence on people whilst cyber criminals wish to use their skills to exploit the cyber space so as to commit complex crimes that are difficult to adduce sufficient and appropriate evidence. It is therefore evident that cyber security personnel are on a precarious position since cyber criminals continue to take advantage of rampant technology advancement to create new tools to commit more complex cyber-crimes. Cybercrime not only affects technological progress, but is also an attack on the economic, social and political progress of society. It is therefore important that relevant ministries put in place stronger awareness-raising and capacity-building programs to promote cyber resilience in the future while ensuring proper governance and respect for human rights.

## RECOMMENDATIONS

It is therefore recommended that;

- A culture of cybersecurity among stakeholders, especially governments, businesses, cooperatives, academia, civil society organizations and international organizations operating within the country developed. and developing information systems to manage and use them. Governments also need to mobilize resources to develop cybersecurity skills.
- Government should raise public awareness and provide education and training. Law enforcement agencies need training to carry out their cybersecurity missions while upholding the rule of law and meeting human rights requirements.
- To enable international cooperation, Zimbabwe's laws must be compatible with those of other countries. Over-criminalizing social media content should be avoided to curb the stigma associated with the new laws.

- Governments must ensure that critical information infrastructure is protected in order to protect data and sensitive information in terms of the promulgated data protection laws (this is crucial given the contemporary biometric systems that collects sensitive personal data such as fingerprints).
- Stakeholders and citizens of all countries must work together to change the mindset and public perception of cybersecurity issues.
- Cyber security practitioners should ensure that they are robust and agile to remain ahead of criminal sophistry
- Cyber criminals should be given tough sentences when convicted
- Cyber-crime investigators and court official should be kept updated on cyber space issues

## REFERENCES

1. Chindaru, S. (2017). TechZim: We underestimated Cybercrime in Zimbabwe, it's time to be woke now… Insights and Security
2. Humphrey, J. (2012). Cyber Warfare and The Crime of Aggression: The need for Individual Accountability on Tomorrow's Battlefield. [Online] Available at: http://www.law.duke.edu [accessed: 20 November 2021]
3. Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. International Journal of Law, Crime and Justice, 47, 44-57.
4. Jahankhani, H., & Al-Nemrat, A. (2011). Cybercrime profiling and trend analysis. In Intelligence Management (pp. 181-197).
5. Lee, H. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity and risky cybersecurity behaviours.
6. Sitemere, S. (2022). Country Manager, Zimbabwe, and South Africa, WorldRemit on Fintech. Zimbabwe
7. Vito, F.G., and Maahs J. (2015). Criminology: theory, research, and policy of cybercrime for social media usage. Journal of Information Technology, 33–67.
8. Wazid, M., Zeadally, S., & Das, A. K. (2019). Mobile banking: evolution and threats: malware threats and security solutions. IEEE Consumer Electronics Magazine, 8(2), 56-60
9. Yar, M. (2012). The criminological landscape of new social media. Information and Communications Technology Law, 21, 207-219.