The Commonwealth

Commonwealth Cyber Journal \ 161
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

Towards a Victim-Centred Approach? Reflections on Existing Cybercrime Instruments and the Draft United Nations Convention on Cybercrime

Brenda Mwale[1]

Abstract

In recent years, increasing attention to cybercrime and its impacts on society has led to an unprecedented focus on the prosecution of offenders. Indeed, anti-cybercrime conventions such as the Council of Europe Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data provide a good framework for addressing cybercrime by setting out provisions on substantive criminal law, procedural law and international co-operation, which are essential for prosecuting offenders. Yet, while these provide adequate frameworks, they barely focus on victims of cybercrime (those who suffer harm as a result of cybercrime). Unlike for traditional crimes, perpetrators of cybercrime do not require physical proximity to the victim, and they can anonymously reach a significant number of victims with limited detectability. As a result, the way in which cybercrimes occur and how their consequences manifest challenge the way we traditionally think about victims of crime.

This points to a need to specifically address the plight of victims of cybercrimes. Currently, negotiations on a binding international cybercrime treaty under the UN framework provide new hope for victims of cybercrime: the current draft not only recognises victims but also contains specific provisions relating to them. If adopted, the convention will be the first international cybercrime convention to adopt a victim-centred approach.

[1] Post-doctoral Fellow, Faculty of Law, University of Pretoria. Email: mwale17@gmail.com.

1. Introduction

As society continues to be digitalised, so too does the nature of crimes – and their victims. While the actual number of cybercrime victims is unknown, by the year 2020 alone it was estimated that the global cost of cybercrime was US$ 1 trillion per year, a 50 per cent increase on figures reported in 2018 (Scroxton, 2020). Estimates indicate that, in 2018, the global cost was as much as $600 billion per year (Lewis, 2018, p. 6). These figures are particularly concerning because it is generally known that the global scale of cybercrime is often underestimated, frequently because of underreporting.

Despite these worrying figures, the plight of victims of cybercrime (those who suffer harm as a result of cybercrime) has been ignored. Today, the primary focus of cybercrime instruments is to punish perpetrators by creating cyber-specific offences and imposing penalties on cybercrimes. While the needs of cybercrime victims may be partially met through the prosecution of cyber-offenders, their specific needs are often overlooked. As a result, their plight is often relegated to a secondary consideration. Vincent (2017, p. 27) highlights some of the reasons why criminal law overlooks victims of cybercrime:

> First, and perhaps most surprisingly to many..., victims and their harms are best of only marginal interest to... criminal law. Second, core features of criminal law doctrine are conceptually incompatible with recognizing and adjudicating cybercrime. Consequently, for largely doctrinal and conceptual reasons, criminal law makes a very poor ally for victims of cybercrime.

Besides, some forms of cybercrimes may be deemed victimless crimes. These could involve phishing offences, in which an unsuspecting victim unintentionally joins a criminal network (Halder, 2022, p. 6). In such cases, if victims' claims of victimhood are not supported by relevant facts, the criminal justice system may choose to dismiss them, place the responsibility on them or treat them like perpetrators.

These factors highlight the need for renewed reflection on how cybercrime instruments respond to the unique circumstances of victims of cybercrime. For a long time, there has been little scrutiny on this topic. However, since early 2022, UN member states have been negotiating a cybercrime treaty that has the potential to reshape the criminal justice approach to victims of cybercrime. This is because the current draft text of the convention (published in February 2024) contains specific provisions on victims, relating to the protection of victims who are witnesses, assistance to and protection of victims, mutual legal assistance, remedies such as recovery and return of proceeds of cybercrime, preventive measures and technical assistance. If adopted, the treaty has the potential to cement certain guarantees for cybercrime victims.

In this context, this article argues that legal measures aimed at addressing cybercrime, as provided in the draft text of the convention, should focus on a victim-centred approach that addresses the unique needs of cybercrime and its victims. Accordingly, as a preliminary matter, the article explains what cybercrime entails, who the victims are and

the impact of cybercrime on its victims, and highlights the specific needs of those victims. Building on this, the article analyses their legal position in the context of the current anti-cybercrime frameworks and the current draft text of the UN convention on cybercrime.

2. What is cybercrime?

A critical starting point in looking at the question of victims of cybercrime involves examining what cybercrime entails. This is because a clear definition of cybercrime has an impact on the definition of victims of cybercrime and measures to respond to their plight. That said, while cybercrime instruments aim to prevent, investigate and punish cybercrimes, there is no universally accepted definition of the term. Cybercrimes are conceptualised differently across different jurisdictions, with significant variations on what constitutes a criminal offence. Besides, most international and regional instruments shy away from defining cybercrime.

Nonetheless, at its broadest, it could be argued that the notion signifies illegal activities committed through information and communication technology (ICT). Based on this understanding, Thomas and Loader (2000, p. 3) conceptualise and define cybercrimes as 'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.' In addition, Brenner (2007, p. 386) notes that cybercrimes comprise 'the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order.'

A popular distinction is drawn between two categories of cybercrimes based on the role that technology plays in committing a crime. The first category, computer-assisted crimes, involves crimes that occur because cyberspace allows them to be committed in new ways. Crimes that predate the internet, like fraud, hate speech and money laundering, can occur even without the internet, but the internet gives them a new life. In such cases, computer systems and networks merely facilitate the commission of existing crimes (Gillespie, 2016). On the other hand, computer-focused crimes – the second category – came into existence with the advent of computer technology and cannot be perpetrated without the use of computer systems and networks. A classic example of a computer-focused crime would be hacking.

The main criticism of this distinction is that 'technological advancements have... blurred the distinction between assisted and focused' (Gillespie, 2016, p. 9). Thus, it is argued that, while this classification is helpful, it may be limiting from a criminal law perspective as it focuses on the technology at the cost of the relationship between the perpetrator and the victim (Yar, 2006).

For these reasons, alternative approaches that are slightly more nuanced have been proposed. Some of these are broader and account for the role of technology in the perpetration of crime or specific types of offences (Phillips et al., 2022). For instance, Wall (2010, in ibid., p. 385) proposes a three-tier classification that distinguishes between:

1. Cyber-dependent crimes or true cybercrimes,
2. Cyber-enabled crimes or hybrid crimes; and
3. Cyber-assisted crimes or the use of computers in traditional crime.

It can be argued that this approach does not add new categories per se but extends the two-category system identified above. Other approaches focus on different categories of offences. For instance, the Council of Europe (COE) Convention on Cybercrime (2001) sets out four broad categories of cybercrime:

1. Offences against the confidentiality, integrity and availability of computer data and systems;
2. Computer-related offences such as fraud and forgery;
3. Content-related offences – such as child pornography; and
4. Offences related to infringements of copyright and related rights.

These categories focus on a range of online harms that can occur as a result of online conduct (e.g., hacking) or material (e.g., child pornographic material). Rather than explicit definitions of cybercrimes, the use of these broader categories and the above classification systems has gained popularity (Phillips et al., 2022). The problem, in the context of the topic at hand, is that lack of uniformity can pose challenges to determining who the victims of cybercrimes are across different jurisdictions.

3. Who are the victims of cybercrimes?

It follows from the above that defining victims of cybercrimes is not straightforward. Like with the concept of 'cybercrime,' there is no universally accepted definition of the term 'victim of cybercrime,' and it may be difficult to envisage an 'ideal' victim because of the breadth of prohibited acts that constitute 'cybercrime' across different legal instruments. However, as a point of departure, one can seek guidance from international instruments focusing on victims of crime. An oft-quoted reference point is the United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power (1985), which defines victims as:

> ... persons who, individually or collectively, have suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights, through acts or omissions that are in violation of criminal laws operative within Member States, including those proscribing criminal abuse of power (para. 1).

According to the Declaration, a person may be regarded as a victim irrespective of whether the perpetrator of the crime is identified, apprehended, prosecuted or convicted and whether there is a familial relationship between the perpetrator and the

victim (para. 2). Where appropriate, the definition extends to 'the immediate family or dependants of the direct victim and persons who have suffered harm in intervening to assist victims in distress or to prevent victimization' (ibid.).

Drawing on the above, two key points are critical. First, victims are defined by reference to the harm suffered. The focus on the harm suffered is emphasised by Suryanto et al. (2020, p. 155), who conceptualize victims as 'those who have been harmed both materially and non-materially as a result of cybercrime.' Second, two categories of victims can be identified: direct victims (those who suffered harm resulting from the cybercrime) and indirect victims (immediate family or dependants of the direct victim). In general, primacy is given to those who suffer harm as victims. However, where appropriate, there may be circumstances when immediate family or dependents are considered victims, as in the above definition.

It is noteworthy that, while the Declaration focuses on persons who individually or collectively suffer, 'victims of cybercrime [can] range from individuals and communities to entire businesses and governments' (Wilkinson, 2023). Thus, notwithstanding the difficulties in defining cybercrime and the lack of a common definition thereof, it can be concluded that a victim of a cybercrime is anyone who suffers harm resulting from a cybercrime. Such crime may be cyber-dependent or cyber-enabled, or arise from the list of cyber-offences in a cybercrime instrument.

4. What are the impacts of cybercrimes on their victims?

The focus on the harm suffered leads us to a discussion on the impact of cybercrimes on their victims. Generally, the negative impacts of cybercrimes are material and non-material and can fall into the categories highlighted below.

4.1 Financial impacts

Cybercrime can have devastating financial impacts on businesses and individuals. Even a single cyber-incident can result in significant financial losses. For instance, in 2017, the WannaCry ransomware cyberattack affected around 230,000 computers globally, causing a financial loss of US$4 billion across the globe (Kaspersky, nd). Besides, as noted earlier, the global financial cost of cybercrime scales up to $1 trillion a year. However, these estimates reflect the aggregate cost to countries, not to individuals or companies, and may not be reflective of the cost to individual victims (Lewis, 2018).

4.2 Reputational impact

In addition to causing financial losses, cybercrime can lead to reputational harm at different levels. For instance, at an organisational level, cybercrime can affect a company's image, erode customer trust, damage public perceptions and reduce

business opportunities (Agrafiotis et al., 2018). At the individual level, a cyber-incident that leaks personal information can have a negative reputational impact when the information leaked damages the individual's reputation.

4.3 Psychological and emotional impacts

At the individual level, cybercrime can result in psychological and emotional impacts on its victims. Often, victims have feelings ranging from anger, outrage, anxiety and fear to a total loss of trust in information technology. Victims can also feel ashamed, vulnerable and powerless, leading to depression. In many cases, victims of online abuse, such as cyberstalking, doxing, online harassment, non-consensual dissemination of intimate images and so on, often blame themselves for what happened.

4.4 Disruptive impacts

Cybercrimes, such as those aimed at causing data or system interference, can be disruptive, causing operational disruptions that result in downtime, loss of productivity, loss of access to critical services and delays in service delivery. For example, ransomware attacks can encrypt files on a computer system, rendering computer files inaccessible and unusable. As a result, victims may spend a lot of time trying to recover their data, which sometimes cannot be recovered.

4.5 Physical impacts

Cybercrimes can also result in physical damage to physical assets (such as computer hardware, infrastructure, etc.). There are 'targeted and specific intrusions capable of creating functional and even physical damage' (Rid and McBurney, 2012, p. 8). Damage to physical infrastructure can also have cascading effects on individuals, organisations and society as a whole (Agrafiotis et al., 2016).

5. What are the needs of victims of cybercrime?

By all accounts, victims' needs can be diverse, as the impacts of cybercrime on victims can range from material (e.g., financial loss) to non-material (e.g., reputational damage, psychological and emotional impacts). Some victims may have suffered financial loss and require compensation. When victims still feel the negative consequences of cybercrime, they may develop a more punitive stance and pursue prosecution of the offender (Pemberton and Vanfraechem, 2015). However, for others there can be more pressing matters than retribution. These may include an apology, assistance and protection, recognition and condemnation of the harm, guarantees of safety, restoration to the situation preceding the cyber-incident, prevention of the cybercrime's recurrence or participation in criminal proceedings.

Some may require immediate responses, such as removing illegal content posted online, while others may require responses that consider their particular vulnerabilities and needs. Thus, special consideration should be made of the fact that 'victimhood varies depending on a number of identified dimensions, including vulnerability aspects, psychological perspectives, [and] age-related differences' (Sikra et al., 2023, p. 28). This means that a wide range of measures are required to respond to the diverging needs of cybercrime victims.

6. The legal response: international responses to cybercrime and its victims

Despite the growing number of cybercrime victims, the impact of cybercrime on its victims and the specific needs of victims, the predominant focus of cybercrime instruments is on the prosecution of offenders by creating new cyber-offences or adapting existing offences to address the challenge of cybercrime. As the ensuing discussion demonstrates, the existing cybercrime instruments 'recognize' the harm to victims only when the crime is defined as a criminal offence (Vincent, 2017, p. 31). To further elaborate on the situation and the prospects of a victim-centred approach, this section analyses the relevant provisions of two multilateral cybercrime conventions (the COE Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection) and the draft text of the UN convention on cybercrime (published on 6 February 2024).

6.1 Council of Europe Convention on Cybercrime

In 2001, the COE Convention on Cybercrime (the Budapest Convention) was adopted as the first international convention to deal with cybercrimes. With the aim of establishing 'a common criminal policy aimed at the protection of society against cybercrime,' highlighted in its Preamble, the convention deals with issues of substantive criminal law, procedural law and international co-operation. It takes a retributive approach that focuses on prosecuting the following offences: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to infringements of copyright and related rights.

In terms of procedural law, Article 15 of the Convention provides that states parties should ensure that the establishment, implementation and application of the procedural powers are subject to the conditions and safeguards laid down in domestic laws. The Convention further provides in Article 15(3) that 'to the extent that it is consistent with the public interest, in particular the sound administration of justice, each state party shall consider the impact of [such] powers and procedures upon the rights, responsibilities and legitimate interests of third parties.' The Explanatory Report to the Convention notes that the initial consideration is given to the sound administration of justice and

other public interests, such as the interest of victims (COE, 2001a, para. 148). In this regard, victims' interests are implicitly recognised. Thus, while the Convention provides an adequate legal basis for prosecuting cybercrime, victims of cybercrime are considered to be of only secondary interest in terms of the conditions and safeguards that states should place while implementing procedural powers in the Convention.

Nonetheless, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (2022) recognises victims of cybercrime**.** It recognises in its Preamble 'the growing number of victims of cybercrime and the importance of obtaining justice for those victims.' The Second Protocol is one of the first examples of a cyber-convention recognising victims. However, although it constitutes a step forward, it is also worth noting that there are no detailed provisions on victims in the Protocol.

6.2 African Union Convention on Cyber Security and Personal Data Protection

In June 2014, the African Union Assembly adopted the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) as a regional instrument on cybersecurity, cybercrime and data protection. For many years after its adoption, the Convention did not receive the required number of ratifications to enter into force. It did so on 8 June 2023 following the deposit of the 15th Instrument of Ratification by Mauritania.

Similar to the Budapest Convention, the Malabo Convention sets out provisions on substantive criminal law, procedural law and international co-operation and takes a retributive approach. It lays down three broad categories of prohibited conduct that states should criminalise: (i) attacks on computer systems; (ii) computerised data breaches; and (iii) content-related offences. However, unlike the Budapest Convention and its Second Additional Protocol, the Malabo Convention does not refer to victims explicitly or impliedly. Save for setting out substantive offences, which could by implication cater to victims' needs through retribution, the Malabo Convention does not refer to victims in any way. Of course, victims can resort to instituting criminal proceedings against offenders. However, the assumption that punishing perpetrators alone will cater to victims' needs is flawed.

6.3 Draft UN convention on cybercrime

For a long time, the Budapest Convention has been regarded as the most important international agreement on cybercrime and electronic evidence and the only international convention on the subject. Initially, it was open for signature only to the COE states and four observer states that participated in the negotiations. But today, any state prepared to implement its provisions and engage in co-operation can accede to it. Despite this, the lack of a UN convention on cybercrime (open to all member states) is still glaring.

In 1998, Russia introduced a draft resolution at the General Assembly that mentioned the need to prevent the misuse of information technology for criminal purposes. But progress towards adopting a UN treaty has been slow. It was only in 2019 that the General Assembly, pursuant to Resolution 74/247, decided to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes (para. 2).

In early 2022, UN member states convened their first session to negotiate a binding international cybercrime treaty draft pursuant to the work plan for the delivery of the mandate of the Ad Hoc Committee. Negotiations continued into early 2024; the concluding session was held in New York from 29 January to 9 February. The concluding session ended with no consensus on the scope of the convention, including on what crimes it should cover and on key provisions on criminalisation, international co-operation and human rights safeguards. As a result, a reconvened concluding session will be held at a future date. While proponents may view the lack of consensus as a dream deferred, it is an opportunity to reflect deeply on the provisions of the current draft text of the convention.

6.3.1 The scope of the draft text

During the first session of the Ad Hoc Committee, several member states submitted statements on what the scope of the convention should entail. South Africa captured the current state of affairs concerning the regulation of cybercrime by submitting that:

> The international system in its current form is not equipped to deal with the growing scourge of cybercrime, thus necessitating that the world unites in formulating a true international instrument that will protect the victims of crimes committed in cyberspace and guarantee maximum protection and legal remedies (South Africa, 2021, p. 1).

Several states agreed that the convention should focus primarily on substantive criminal law, criminal procedure and international co-operation. While these three areas are the main focus of existing cybercrime instruments, some states also drew attention to the need to focus on victims. For Switzerland, the convention should provide for a co-ordinated approach in the fight against cybercrime and create a common understanding of what cybercrime offences entail and a framework for international co-operation 'to protect ICT users and to obtain justice for the victims of cybercrime' (Switzerland, 2021, p. 2). In addition to provisions on criminalisation and co-operation, the EU and its member states stressed that the convention should also 'comply with international human rights standards and strive to fight cybercrime most effectively and thus protect victims' (EU, 2022, p. 2). Chile's view on the scope, objectives and structure (elements) of the convention focused on, among others, the preventive role of the convention. In Chile's view, the convention should 'promote victim-centered prevention strategies [that] deal with interpersonal cybercrimes' (Chile, 2021).

Prior to the concluding session, a draft text of the convention provided that the convention would apply to the prevention, investigation and prosecution of the offences set out therein, including the freezing, seizure, confiscation and return of the proceeds of such offences (UN General Assembly, 2023). It also provided that the convention would apply to the collecting, obtaining, preserving and sharing of evidence in electronic form. However, as noted above, no consensus was reached on the scope of the convention's application during the concluding session.

The current draft text, published on 6 February 2024 (UN General Assembly, 2024), while not addressing the scope of the convention, lists a number of prohibited conducts. These include illegal access, illegal interception, interference with electronic data, interference with an ICT system, misuse of devices, ICT system-related forgery, ICT system-related theft or fraud, offences related to online child sexual abuse or child sexual exploitation material, solicitation or grooming for the purpose of committing a sexual offence against a child, non-consensual dissemination of intimate images and laundering of proceeds of crime (Articles 6–16). While mirroring some of the offences laid down in the Budapest and Malabo Conventions, the proposed offences go beyond the list of core cybercrimes and may broaden the list of who victims of cybercrime are.

6.3.2 Recognition of victims in the Preamble

In the early stages of the treaty negotiations, the chair of the Ad Hoc Committee (2022a, p. 11) came up with guiding questions for invited delegations to consider and address in their interventions, including questions on victims. The following guiding questions were put across:

> Should the convention contain a provision on the assistance to and protection of victims? If yes, which factors of protection are important to include in such a provision, and what level of detail, in terms of definitions and description of related procedures, should be expected? What role should victims and reporting persons have? Would the committee like to follow the formulation of UNTOC [United Nations Convention Against Transnational Organized Crime] (article 25)?

These questions provided a useful framework for discussions on victims of cybercrime.

To begin with, the Preamble of the draft text emphasises the need to protect society against cybercrime. It also recognises 'the increasing number of victims of cybercrime, the importance of obtaining justice for those victims and the necessity to address the needs of persons in vulnerable situations in measures taken to prevent and combat the offences covered by [the] Convention.' This recognition represents a significant shift in how states view the objects and purposes of cybercrime instruments and has been welcomed by some stakeholders.

The CyberPeace Institute, for instance, noted in its submission to the Ad Hoc Committee that the recognition of victims was a 'key statement as the main purpose of a new international treaty on cybercrime should be to protect and bring remedy to its victims

through evidence-led accountability, allowing those affected by cybercrime to seek redress and for measures to prevent their re-victimisation'. However, the Institute argued that the Preamble should consider the various types of harm that cybercrime can cause by highlighting the distinct impacts of cybercrime that may be felt by those disproportionately targeted or affected in cyberspace. This article argues that, although the Preamble does not provide for the various types of harm, it acknowledges the needs of persons in vulnerable situations in measures taken to prevent and combat the offences covered by the convention.

6.4 Specific provisions relating to victims

In addition to recognising victims in the Preamble, the draft text contains provisions relating to victims. It specifically provides for the protection of victims who are witnesses, assistance to and protection of victims, mutual legal assistance, remedies such as recovery and return of proceeds of cybercrime, preventive measures and technical assistance in relation to victims.

6.4.1 Protection of victims who are witnesses

First, the draft text provides for the protection of victims who are witnesses. Article 33 requires states parties to establish measures to protect witnesses who give testimony, provide information concerning offences established in the convention or co-operate with investigative or judicial authorities. Protective measures may include establishing physical protection procedures and evidentiary rules to ensure the witness' safety when testifying. States parties should also consider entering into agreements or arrangements with other states for the relocation of witnesses. Article 33(4) states that these measures also apply to victims insofar as they are witnesses and are based on Article 32 of the United Nations Convention Against Corruption (UNCAC).

Practically speaking, the idea of victims who are witnesses of cybercrimes sounds complex. When someone thinks of a 'witness,' what comes to mind is someone who saw a crime take place. Thus, in the context of cybercrimes, it may be difficult to envision a victim who is a witness given that cybercrimes occur via computers and computer systems and can result in online harms. As Wilkinson and Swali (2022) put it, a 'witness' in cyberspace is more ambiguous than a 'victim.' Nonetheless, while Article 33 does not define who 'witnesses' are, it limits its scope to witnesses who give testimony or provide information concerning offences established in the convention. Although not definitive in describing cybercrime witnesses, international conventions such as the UNCAC may be 'a productive starting point, demonstrating the merit of adapting language that enjoys international consensus in existing anti-crime frameworks' (ibid.).

On the other hand, states may need to consider the specific realities of cybercrime witnesses and victims. Most importantly, protective measures should go beyond physical protection procedures and evidentiary rules to ensure the safety of witnesses when

testifying. This is because there are many ways in which victims and witnesses can be intimidated in a digital environment that require cyber-specific measures. For instance, victims who are witnesses of cybercrimes may require an assurance that their data will be protected while giving digital evidence.

6.4.2 Assistance to and protection of victims

Second, Article 34 of the draft text makes provision for the assistance and protection of victims. To begin with, states parties are required to take appropriate measures to provide assistance and protection to victims of cybercrime, especially in cases of threat of retaliation or intimidation. States parties are also required to establish appropriate procedures to provide access to compensation and restitution for those victims, subject to their domestic laws. Indeed, compensation and restitution are key pillars of victim assistance as they acknowledge victims' losses by providing financial relief. In practice, however, particular difficulties may arise from the fact that a single cyber-incident can result in multiple victims spread across different jurisdictions, and multiple claims for compensation instituted in several states could raise jurisdictional issues. Therefore, it would be helpful if the provision on compensation and restitution is tied to a requirement for states to co-operate in cases where cybercrimes traverse borders.

On criminal justice matters, states parties are required, subject to domestic laws, to consider the views and concerns of victims at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence. This provision gives wide discretion to domestic courts to determine the appropriate stage at which victims can participate in criminal proceedings. It must be noted, however, that expressing 'views and concerns' is not the same as giving evidence. Although the views and concerns of victims may assist courts in approaching evidence, they do not form part of trial evidence (ICC, 2014). Thus, unless victims are witnesses, as provided for under Article 33, their participation in criminal proceedings is limited to expressing their views and concerns.

Special provision is also made for the assistance and protection of children. Article 34 covers victims of offences related to online child sexual abuse or child sexual exploitation material; solicitation or grooming for the purpose of committing a sexual offence against a child; and non-consensual dissemination of intimate images. States parties are required to take appropriate measures to assist such victims, including their 'physical and psychological recovery, in cooperation with relevant international organizations, non-governmental organizations, and other elements of civil society' (Article 34(4)). Many would argue that it is important that these actions are undertaken in collaboration with relevant stakeholders such as international organisations, non-governmental organisations and civil society because these are leading providers of services to victims of various crimes. Even so, including other stakeholders, such as technology companies, is crucial, given their technical expertise.

It is also important to note that the protection of child victims of sexual abuse and sexual exploitation can be improved by aligning the relevant provisions of the draft text with the minimum standards for the protection of children outlined in the UN Convention on the Rights of the Child (UNCRC) 1989. Specifically, Article 39 provides that:

> States Parties shall take all appropriate measures to promote physical and psychological recovery and social reintegration of a child victim of: any form of neglect, exploitation, or abuse; torture or any other form of cruel, inhuman or degrading treatment or punishment; or armed conflicts. Such recovery and reintegration shall take place in an environment which fosters the health, self-respect and dignity of the child.

In cases where children are victims of sexual abuse and sexual exploitation, Article 34 of the UNCRC provides that states parties undertake to take measures to prevent (i) the inducement of a child to engage in unlawful sexual activity and (ii) the exploitative use of a child in prostitution, other unlawful sexual practices or pornographic performances. These protective measures should be guaranteed both offline and online (UN Committee on the Rights of the Child, 2021). To further assist and protect child victims, the United Nations Children's Fund argues that the proposed cybercrime convention can be used to further strengthen the protection of children by adopting special measures such as child-friendly practices in the criminal justice system and different forms of platforms for compensating child victims (UNICEF, 2022).

In applying the above measures, the draft text provides that states parties should take appropriate measures that consider the age, gender, particular circumstances and needs of victims, including the particular circumstances and needs of children. Further, states parties should take steps, in accordance with domestic laws, to ensure compliance with requests to take down such content relating to online child sexual abuse or child sexual exploitation material; solicitation or grooming for the purpose of committing a sexual offence against a child; and non-consensual dissemination of intimate images, or render them inaccessible. On that basis, the proposed treaty should also include specific provisions for online platforms and service providers to remove such content on their platforms without delay.

6.4.3 General principles and procedures relating to mutual legal assistance

Third, Article 40 of the draft text contains a lengthy provision on general principles and procedures relating to mutual legal assistance in (i) investigations, prosecutions and judicial proceedings relating to offences laid down in the convention and (ii) with the aim of collecting evidence in electronic form. While victims do not take centre stage in Article 40, they are mentioned in subparagraph 18 alongside witnesses or experts in relation to hearings in court proceedings. Article 40 (18) reads as follows:

> Wherever possible and consistent with fundamental principles of domestic law, when an individual is in the territory of a State Party and has to be heard as a

> witness, victim or expert by the judicial authorities of another State Party, the first State Party may, at the request of the other, permit the hearing to take place by videoconference if it is not possible or desirable for the individual in question to appear in person in the territory of the requesting State Party. States Parties may agree that the hearing shall be conducted by a judicial authority of the requesting State Party and attended by a judicial authority of the requested State Party. If the requested State Party does not have access to the technical means necessary for holding a videoconference, such means may be provided by the requesting State Party, upon mutual agreement.

Noting that cybercrimes can traverse multiple jurisdictions and hearings can occur outside the jurisdiction where the cybercrime occurred, special measures for hearings to take place by videoconference are highly welcomed.

6.4.4 Recovery and return of proceeds of cybercrime

Fourth, Article 52 provides for the recovery and return of proceeds of cybercrime. It provides that the disposal of confiscated shall be in accordance with its domestic law and administrative procedures. Here, primacy is given to the victims of cybercrime and prior legitimate owners in the return of such proceeds. Article 52 (2) provides that:

> When acting on a request made by another State Party [...] States Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give *compensation to the victims* of the crime or return such proceeds of crime or property to their prior legitimate owners. [Emphasis added.]

This means that a victim can be compensated for loss or damage arising from a cybercrime. Indeed, this is a positive step in recognising victims by allowing them to benefit from the prosecution of cybercrimes, particularly in the context of compensation or return of confiscated proceeds of crime or property. The challenge, however, is that compensation in this regard is dependent on domestic law and the confiscation and return of the proceeds of crime. In cases where a state does not have domestic legal redress measures or mechanisms, the guarantees that they may offer to victims are weakened. Commenting on Article 52 of the draft text, Microsoft calls on states to 'enable victims to initiate civil action in courts of other states to protect their property rights violated by cybercriminals' (Microsoft Corporation, 2023).

6.4.5 Preventive measures, technical assistance and capacity-building

Earlier draft texts of the convention did not provide for preventive measures, technical assistance and capacity-building in relation to victims. This might have led the CyberPeace Institute to call for the 'mainstreaming [of] victims' perspectives throughout the chapters on preventive measures and technical assistance.' Perhaps in realising the need to do so, the negotiations towards the current draft text led to the inclusion of

Article 53(3), which provides for preventive measures, including a requirement for states to develop or strengthen support programmes for victims. It also includes provisions on technical assistance and capacity-building in relation to victims.

Specifically, Article 54 requires states parties to afford one another the widest measure of technical assistance and capacity-building, including training, exchange of expertise and, where possible, transfer of technology for the purposes of preventing, detecting, investigating and prosecuting offences under the convention. States parties should also establish, implement or improve specific training programmes for those involved in preventing, detecting, investigating and prosecuting offences under the convention. To the extent permitted by domestic law, these measures may deal with methods 'used in the protection of victims and witnesses who cooperate with judicial authorities' (Article 54(3)(h)).

Capacity-building is particularly important to help criminal justice authorities deal with cybercrimes. Given that evidence relating to cybercrime may be stored in computer systems and networks, those involved in preventing, detecting, investigating and prosecuting cybercrimes should be trained to handle electronic evidence. In addition, this article argues that special training programmes should be made available to relevant stakeholders who provide services to victims of crime. In so doing, technical assistance and capacity-building measures become valuable tools in responding to the specific needs of cybercrime victims.

7. Towards a victim-centred approach?

As demonstrated above, the draft text to the UN convention on cybercrime constitutes the first time since the adoption of the Budapest Convention that states have attempted to respond to the plight of victims of cybercrime by coming up with draft provisions on victims. From the outset of the negotiations, many state and multistakeholder groups agreed that a future cybercrime treaty needed to include provisions for victims of cybercrime. One of the arguments in favour of recognising victims is the need for victims to obtain justice.

During the second session of the Ad Hoc Committee (2022b), held in Vienna between 30 May and 10 June 2022, Mexico proposed the following clause: 'In all actions aimed at the implementation of the present Convention, the best interests of the victims -individuals and institutions and organizations- of the crimes recognized in the present Convention shall be a primary consideration' (Ad Hoc Committee (2022b, p. 6). Although not included in the draft text, Mexico's proposal captured the crux of a victim-centred approach that puts the best interests of victims at the forefront of efforts to implement the convention. Similarly, as the CyberPeace Institute (2023) puts it, 'mainstreaming the victims' perspectives throughout the chapters on preventive measures and technical assistance can support the development of targeted, needs-driven, and context-specific responses to mitigating and preventing cybercrime.'

As noted above, the draft text focuses on measures related to the protection of victims who are witnesses, the assistance and protection of victims, mutual legal assistance provisions, effective remedies, preventive measures and technical assistance measures. While these provisions can guide states on how to address victims of cybercrime, certain shortcomings in the relevant provisions are likely to present challenges. First, the relevant provisions do not require these specific measures to be taken in conformity with international human rights standards. States could therefore define how to implement the provisions, subject to their domestic laws, in ways that disregard their human rights obligations. If the cybercrime instrument is to be effective, human rights standards must be included to guarantee fundamental rights and freedoms.

Second, many of the measures listed in the draft text are to be taken subject to domestic laws. The challenge at the domestic level is threefold: (i) victims of cybercrime are often marginalised by national cybercrime laws; (ii) some states have not adopted adequate cybercrime laws, let alone specific provisions that address victims of cybercrime; and (iii) in the absence of legal safeguards, states could use domestic laws as a tool for arbitrary abuse of power. These challenges may be a stumbling block to the implementation of a victim-centred approach in addressing cybercrime.

Third, little is done to address the unique needs of victims in the cyber context. It must be pointed out that using technology as a means, medium or target of crime creates a wide range of cyber-specific needs. It is therefore imperative that special consideration is given to the nature of online harm and the specific impact of cybercrime on its victims, while also bearing in mind the fact that victimhood depends on a number of aspects such as vulnerability, psychological aspect and age-related differences (Sikra, 2023). These issues should be addressed in future treaty negotiations.

8. Conclusion

While the recognition of victims' needs can be implied through existing cybercrime conventions' retributive approaches, such approaches do not put the needs of victims centre stage. Prosecution is only one aspect of addressing cybercrime and its victims. An appropriate response to the plight of cybercrime victims should be holistic, involving much more than bringing perpetrators to justice. Although, as of the time of writing this article, no consensus had been reached to adopt the draft text to the convention, the proposed treaty has the potential to transform how states view and address victims of cybercrimes. If adopted, it will mark a significant step towards realising specific guarantees for cybercrime victims. However, if it is to make a valuable contribution, the problematic areas on the specific criminal justice needs of cybercrime victims, human rights guarantees and adequate safeguards to protect victims should be resolved by addressing the gaps in the current draft text.

References

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (2022a) 'Guiding Questions'. Second Session, 30 May–10 June. www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/Letter_from_AHC_Chair_-_2nd_session_methodology_and_guiding_questions4115.pdf

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (2022b) 'Compilation of Draft Provisions Submitted by Member States on Criminalization, General Provisions and Procedural Measures and Law Enforcement'. Note by the Secretariat, Vienna, UN Doc A/AC.291/CRP, 30 May–10 June. www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/CRP11.pdf

Agrafiotis, I., M. Bada, P. Cornish et al. (2016) 'Cyber Harm: Concepts, Taxonomy and Measurement'. Saïd Business School Research Papers 2016–23. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828646

Agrafiotis, I., J. Nurse, M. Goldsmith et al. (2018) 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate'. *Journal of Cybersecurity* 4(1): yy006.

African Union (2014) 'Convention on Cyber Security and Personal Data Protection'. Adopted on 27 June 2014, entered into force on 8 June 2023.

Brenner, S.W. (2007) 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare'. *Journal of Criminal Law & Criminology* 97(2): 379–475.

Chile (2021) 'Submissions from Member States Related to the First Session of the Ad Hoc Committee: Chile's Views on the Scope, Objectives, and Structure (Elements) of the New Convention, Regarding the Implementation of UN General Assembly Resolutions 74/247 and 75/282'. www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/CHILE_national_views_AHC_05.11.2021.pdf

COE (Council of Europe) (2001a) 'Convention on Cybercrime'. European Treaty Series 185, adopted in Budapest on 23 November 2001 and entered into force on 1 July 2004.

COE (2001b) 'Explanatory Report to the Convention on Cybercrime'. Budapest, 23 November. https://rm.coe.int/16800cce5b

COE (2022) 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence'.

CyberPeace Institute (2023) 'CyberPeace Institute's Submission to the Fifth Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes'. https://cyberpeaceinstitute.org/news/submission-to-ad-hoc-committee-on-cybercrime/

EU (2022) 'Contribution from the European Union and Its Member States: Preparation for the First Session of the United Nations Ad Hoc Committee to Elaborate a Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Taking Place from 17–28 January 2022 in New York'. www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Cwomments/EU_Position_for_AHC_first_session.pdf

Gillespie, A.A. (2016) *Cybercrime: Key Issues and Debates*. New York: Routledge.

Halder, D. (2022) *Cyber Victimology: Decoding Cyber-Crime Victimisation*. New York: Routledge.

ICC (International Criminal Court) (2014) 'Representing Victims before the International Criminal Court: A Manual for Legal Representatives'. Office of Public Counsel for Victims.

Kaspersky (nd) 'What Is WannaCry Ransomware?' www.kaspersky.com/resource-center/threats/ransomware-wannacry (accessed 1 March 2024).

Lewis, J. (2018) *Economic Impact of Cybercrime—No Slowing Down Report*. Washington, DC: CSIS.

Microsoft Corporation (2023) 'Microsoft's Submission to the Sixth Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes'. www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/Microsoft_Submission_-_AHC_Sixth_Substantive_Session.pdf

Pemberton, A. and I. Vanfraechem (2015) 'Victims' Victimization Experiences and Their Need for Justice'. In Vanfraechem, I., D.B. Fernández and I. Aertsen (eds) *Victims and Restorative Justice*, pp.15–47. New York: Routledge.

Phillips, K., J.C Davidson, R. Farr et al. (2022) 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies'. *Forensic Science* (2(2): 379–398.

Rid, T. and P. McBurney (2012) 'Cyber-Weapons'. *The RUSI Journal* 157(1): 6–13.

Scroxton, A. (2020) 'A Trillion Dollars Lost to Cyber Crime Every Year'. *Computer Weekly*, 7 December. www.computerweekly.com/news/252493157/A-trillion-dollars-lost-to-cyber-crime-every-year

Sikra, J., K.V. Renaud and D.R. Thomas (2023) 'UK Cybercrime, Victims and Reporting: A Systematic Review'. *Commonwealth Cybercrime Journal* 1(1): 28–59.

South Africa (2021) 'Submissions from Member States Related to the First Session of the Ad Hoc Committee: South Africa's Views on Scope, Objectives and Structure (Elements) of the Envisaged International Convention on Countering the use of Information and Communications Technologies for Criminal Purposes'. www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/SOUTH_AFRICA_SUBMISSION_ON_SCOPE_OBJECTIVES_AND_STRUCTURE_17_DECEMBER_202171.pdf

Suryanto, T., H. Hamzah, S. Wahab et al. (eds.) (2020) ICETLAWBE 2020: Proceedings of the International *Conference on Environmental and Technology of Law, Business and Education on Post Covid 19*. European Alliance for Innovation Publishing.

Switzerland (2021) 'Elaboration of a Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes: Switzerland's View on the Objectives, Scope and Structure'. www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Cybercrime_input_Switzerland_102021.pdf

Thomas, D. and B.D. Loader (2000) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. Abingdon: Routledge.

UN Committee on the Rights of the Child (2021) 'General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment'. UN Doc CRC/C/GC/25, 2 March.

UN General Assembly (1989) 'Convention on the Rights of the Child'. *Treaty Series*, 1577, 3.

UN General Assembly (2019) 'Countering the Use of Information and Communications Technologies for Criminal Purposes'. UN Doc A/RES/74/247, 27 December.

UN General Assembly (2023) 'Revised Draft Text to the Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes'. UN Doc A/AC.291/22/Rev.1, 6 November.

UN General Assembly (2024) 'Further Revised Draft Text of the United Nations Convention against Cybercrime'. UN Doc A/AC.291/22/Rev.2, 6 February.

UNICEF (United Nations Children's Fund) (2022) 'Renewed Opportunities: The Convention on Countering the Use of ICTs for Criminal Purposes to Further Strengthen the Protection of Children'. www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_intersessional_consultation/Presentations/Panel_2_Afrooz_Kaviani_Johnson_UNICEF.pdf

Vincent, A.N. (2017) 'Victims of Cybercrime: Definitions and Challenges'. In Martellozzo, E. and E.A. Jane (eds) *Cybercrime and Its Victims*, pp. 27–42. London & New York: Routledge.

Wilkinson, I. and A. Swali (2022) 'Cybercrime Convention Could Help and Harm Victims: The Proposed UN Cybercrime Convention Has Risks and Opportunities for Defining and Protecting Vulnerable Groups'. Chatham House, 19 July. www.chathamhouse.org/2022/07/cybercrime-convention-could-help-and-harm-victims

Wilkinson, I. (2023) 'What is the UN Cybercrime Treaty?' Chatham House, 2 August. www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter

Yar, M. 2006. *Cyber Crime and Society*. London: SAGE Publications.

About the author

Brenda Mwale is a postdoctoral fellow under the South African Research Chair in International Constitutional Law, University of Pretoria. She holds an LLD from the University of Pretoria, and her LLD thesis is titled 'The Prevention and Repression of Cyber Terrorism in Africa: An Analysis of the Applicable Legal Regimes'. She also holds an LLM in transnational criminal justice from the University of the Western Cape in conjunction with Humboldt-Universität zu Berlin, a postgraduate diploma in law from the Kenya School of Law, and an LLB from Kenyatta University. She is an Advocate of the High Court of Kenya with experience in teaching and legal research. Her research interests lie in public international law, criminal justice and cyber law.