Fourth Session, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
Denise Bowen, Founder and CEO
DB Connect Digital Submission

January 2023

As the Founder and CEO of DB Connect, a start-up based in Manhattan, New York City, I am committed to finding innovative solutions to pressing issues facing our world today. In addition to serving as a judge for Grammy Award-winning Pharrell Williams' Black Ambition initiative, which is working towards closing the opportunity and wealth gap through entrepreneurship by investing in Black and Latinx founders, I am also an ambassador for Togetherband and the Sustainable Development Goal 10, "Reduced Inequality." Alongside other notable global ambassadors such as David Beckham, Billie Jean King, and Lewis Hamilton, I am working to address the issue of inequality and promote a more inclusive and equitable world. I hereby request to be listed as a "multi-stakeholder" under DB Connect within the framework of the relevant negotiations.

As the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC) continues its discussions, DB Connect is eager to contribute to the conversation on cybercrime and its impact on individuals and organizations. This document serves as a reference for Member States as they formulate their contributions and negotiate the fourth formal session of the AHC. Within it, I will provide a detailed analysis of the current state of cybercrime, including its predicted economic impact and trends we are seeing in 2023, as well as the particular impact on young girls and women. I will also propose solutions for effectively combating this growing problem.

DB Connect is committed to aligning global strategies against cybercrime and working with Member States to provide a unified response to the misuse of Information and Communications Technologies (ICT) for criminal purposes. I believe that by working together, we can create a safer and more secure online environment for everyone.

Recommendations for Removing Article 3(3) from the Convention on Cybercrime

I hereby request that Article 3(3) of the Convention be removed due to concerns that its inclusion may capture activity that is not necessarily harmful or malicious in nature, including acts undertaken by security researchers. This provision risks capturing activity that is beneficial to the public or done without malicious intent, and therefore should be deleted in order to clarify the scope and intent of the Convention and avoid unintended consequences.

It seems that the provision could potentially capture activity that is beneficial to the public or done without malicious intent, which could have unintended consequences for security researchers and others.

Recommendations for Removing Article 3(3) from the Convention on Cybercrime continued

The provision may not be necessary for the offenses set forth in the Convention, as it states that "it shall not be necessary, except as otherwise stated herein." Removing this provision could help to avoid confusion or uncertainty regarding its scope and application.

Deleting this provision could help to ensure that the Convention focuses on addressing harmful or malicious activity, rather than potentially capturing activity that is not necessarily harmful or malicious. Overall, I believe that deleting Article 3(3) is a reasonable approach that could help to clarify the scope and intent of the Convention, while also avoiding unintended consequences for security researchers and others.

Recommendations for Improving the Scope of Criminal Offences in Chapter II of the Consolidated Text

Regarding the scope of criminal offenses outlined in Chapter II of the consolidated text, many of these offenses are written in vague or overly broad language, which fails to comply with the permissible restrictions under international human rights law.

In order to address this issue, I recommend that the scope of criminal offenses in Chapter II be narrowed to include only those offenses listed in Cluster 1 of the consolidated text (Articles 6–10). These offenses reflect core cybercrimes, which are crimes that rely on information and communications technology (ICT) systems as both their direct objects and instruments. These types of crimes could not exist without the use of ICT systems. By limiting the scope of criminal offenses in this way, we can limit the scope of criminalization to core cybercrimes while still allowing for changes to be made in order to mitigate risks to human rights.

However, I also express concern that Articles 6 and 10 may capture the legitimate activities of journalists, whistleblowers, and security researchers. To address this issue, I recommend that these articles include a standard of malicious or fraudulent intent and harm, or provide a more clearly articulated and expansive public interest defense. This will help to ensure that the scope of these offenses remains narrow and specific, while also protecting the rights of individuals who may be engaged in legitimate activities.

Recommendations for Addressing Cybercrimes in the United Nations Treaty on Cybercrime

To achieve consensus on the language to use for cybercrimes, it may be helpful for the United Nations to draw on existing definitions and frameworks, such as the Council of Europe's Convention on Cybercrime (also known as the Budapest Convention). This convention provides a comprehensive definition of cybercrime that includes offenses such as illegal access, interception, data interference, system interference, computer-related forgery, computer-related fraud, and child pornography offenses.

The treaty could also address emerging types of cybercrime, such as cyber-enabled crimes against individuals (e.g., cyberstalking and technology-facilitated violence against women,) and crimes that target critical infrastructure or disrupt essential services.

Compendium of Representative Cyber Offenses and Their Terminology

1. Hacking: unauthorized access to or control over computer systems, networks, or devices.
2. Phishing: the use of fake websites, emails, or other online communications to trick individuals into disclosing sensitive information, such as passwords or financial data.
3. Malware: software that is designed to harm or exploit computer systems, such as viruses, worms, or Trojans.
4. Cyberstalking: the use of electronic communications to harass, intimidate, or threaten an individual.
5. Identity theft: the unauthorized use of someone's personal information, such as their name, address, or financial data, to commit fraud or other crimes.
6. Distribution of child pornography: the possession, distribution, or creation of sexually explicit images of minors.
7. Fraud: the use of false or misleading information to deceive individuals or organizations for financial gain or other purposes.
8. Denial of service attacks: attempts to make an online service or website unavailable by overwhelming it with traffic or other means.
9. Technology-facilitated violence against women, also known as cyber violence against women or online violence against women, refers to the use of technology, such as the internet, social media, or mobile phones, to harass, stalk, or abuse women. This can include a range of behaviors, such as sending threatening or abusive messages, sharing intimate or embarrassing photos or videos without consent (also known as "revenge porn"), or using GPS tracking to monitor a person's movements. Technology-facilitated violence against women can have serious consequences for the victims, including emotional distress, loss of privacy, and damage to reputation. It can also contribute to a broader culture of violence against women and undermine efforts to promote gender equality. **The inclusion of technology-facilitated violence against women in Chapter II is necessary to address the increasing use of technology in perpetrating violence against women and to ensure that such behaviors are properly criminalized**.

Source: Council of Europe Convention on Cybercrime, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008897d

Global Cybercrime Damage Prediction

According to Cybersecurity Ventures, global cybercrime damages are predicted to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history and risks the incentives for innovation and investment. In 2023 alone, it is estimated that cybercrime will inflict damages totaling $8 trillion globally, making it the third-largest economy in the world after the United States and China. The costs of cybercrime include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

Trends in Cybercrime

One of the most significant trends in cybercrime in 2023 is the continued rise of ransomware attacks. According to Cybersecurity Ventures, a business falls victim to a ransomware attack every 11 seconds, a rate that is expected to increase to every two seconds by 2031. The economic impact of these attacks is staggering, with global ransomware damage costs predicted to exceed $265 billion by 2031, up from $325 million in 2015.

Another trend we are seeing is the increasing sophistication of cyber attacks, with hackers using more advanced techniques to evade detection and maximize their profits. This includes the use of machine learning and artificial intelligence to automate the hacking process and target specific individuals or organizations.

There are several ways to ensure that human rights are placed front and center in treaty negotiations:

1. Involve human rights experts and civil society organizations in the negotiation process: By including human rights experts and civil society organizations in the negotiation process, states can ensure that the human rights implications of the treaty are thoroughly examined and taken into account.
2. Conduct human rights impact assessments: States can conduct human rights impact assessments to assess the potential impact of the treaty on the enjoyment of human rights. These assessments can help identify any negative impacts and provide recommendations for how to mitigate them.
3. Engage in transparent and inclusive negotiations: States can ensure that the negotiation process is transparent and inclusive, allowing for the participation of a wide range of stakeholders and the airing of diverse perspectives. This can help to ensure that the treaty reflects the needs and concerns of all relevant parties.
4. Incorporate human rights safeguards into the treaty: States can include specific human rights safeguards in the treaty to ensure that human rights are protected. For example, the treaty could include provisions on the protection of freedom of expression or the prohibition of discrimination.
5. Monitor implementation and compliance with human rights obligations: States can establish mechanisms to monitor the implementation and compliance of the treaty with human rights obligations, such as the establishment of independent bodies or the inclusion of reporting requirements.

Overall, it is crucial that states take a proactive approach to ensure that human rights are placed front and center in treaty negotiations. By taking these and other steps, states can help to ensure that the treaty reflects the values and principles of human rights and that it is implemented in a way that respects and protects the rights of all individuals.

Impact on Young Girls and Women

The impact of cybercrime extends far beyond financial losses, with victims often experiencing significant emotional and psychological trauma as well. This is particularly true for young girls and women, who are often targeted by cyberbullying and online harassment. According to the United Nations, one in three women and girls experience physical or sexual violence in their lifetime, and the internet has become a new platform for this abuse. A survey conducted by the Pew Research Center found that 73% of adult internet users have witnessed someone being harassed online, with young women aged 18-24 being particularly vulnerable. It is crucial that we take steps to protect young girls and women from these harmful and often traumatic experiences.

Cryptocurrency

Cryptocurrency has been linked to cybercrime in several ways. For example, cybercriminals may use cryptocurrency to facilitate illegal activities, such as buying and selling stolen goods or services on the dark web. Cryptocurrency may also be used to launder money or evade detection by law enforcement, as it allows for anonymous and untraceable financial transactions.

According to a report by CipherTrace, a cybersecurity firm that tracks illicit cryptocurrency activity, the amount of cryptocurrency lost to scams, hacks, and fraud reached $1.9 billion in the first half of 2020. This represents a significant increase from the previous year, and suggests that cybercriminals are increasingly turning to cryptocurrency as a means of committing crimes.

To prevent the use of cryptocurrency for cybercrime in 2023, it will be important for law enforcement and regulatory agencies to continue monitoring and tracking illicit activity, and for businesses and individuals to adopt best practices for securing their cryptocurrency holdings. This could include using strong and unique passwords, enabling two-factor authentication, and using reputable and secure exchanges and wallets. It may also be helpful for businesses and individuals to educate themselves about the risks and potential red flags associated with cryptocurrency, such as phishing scams or unauthorized transactions.

Proposal for the Inclusion of Cryptocurrency in Article 33 of the Convention on Cybercrime

I propose that cryptocurrency be included in Article 33 of the Convention on Cybercrime, specifically in paragraphs 1(a)(i) and (ii) and paragraphs 1(b)(i) and (ii). The inclusion of cryptocurrency in these provisions will allow for the criminalization of the conversion or transfer of cryptocurrency, knowing that it is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offense to evade the legal consequences of their actions, as well as the concealment or disguise of the true nature, source, location, disposition, movement, or ownership of or rights with respect to cryptocurrency, knowing that it is the proceeds of crime. It will also allow for the criminalization of the acquisition, possession, or use of cryptocurrency, knowing that it is the proceeds of crime, and participation in, association with, or conspiracy to commit, attempts to commit, and aiding, abetting, facilitating, and counseling the commission of any of the offenses established in accordance with this article.

The inclusion of cryptocurrency in Article 33 is necessary due to the increasing use of cryptocurrency by cybercriminals for illicit purposes. A report by CipherTrace, a cybersecurity firm that tracks illicit cryptocurrency activity, found that the amount of cryptocurrency lost to scams, hacks, and fraud reached $1.9 billion in the first half of 2020, representing a significant increase from the previous year. This suggests that cybercriminals are increasingly turning to cryptocurrency as a means of committing crimes.
In addition to the findings of CipherTrace, cryptocurrency has been linked to cybercrime in several other ways. For example, cybercriminals may use cryptocurrency to facilitate illegal activities, such as buying and selling stolen goods or services on the dark web. Cryptocurrency may also be used to launder money or evade detection by law enforcement, as it allows for anonymous and untraceable financial transactions.
I believe that the inclusion of cryptocurrency in Article 33 will help to deter and prosecute cybercrimes involving the use of cryptocurrency, and will strengthen the efforts of law enforcement to combat this growing threat.

Conclusion

Cybercrime is a complex and rapidly evolving threat that poses significant risks to individuals, organizations, and society as a whole. It is a global problem that requires a multifaceted approach to effectively combat it, involving collaboration between government agencies, international organizations, and legal authorities.

One solution to address cybercrime is to increase funding for cybersecurity research and development, which will allow us to stay ahead of evolving threats and develop new technologies and strategies for defense. Artificial intelligence (AI) and machine learning are already showing great promise in improving cybersecurity, and the global AI cybersecurity market is expected to grow significantly in the coming years.

Another solution is to improve cybersecurity education and awareness, particularly among young people who are at higher risk of falling victim to cyber attacks. This could include creating educational materials and programs specifically tailored to young girls and women, as well as providing resources for victims of cyberbullying and online harassment.

To effectively combat cybercrime on a global scale, it is also essential that we work to strengthen international cooperation and coordination. This could include sharing information and resources among law enforcement agencies and collaborating on efforts to bring perpetrators to justice. Working with global organizations such as Interpol and the International Telecommunication Union (ITU), as well as implementing legal frameworks to facilitate cooperation and extraditions across borders, can help to effectively address cybercrime.

While AI and machine learning can be powerful tools in the fight against cybercrime, there have been instances where facial recognition technology has failed, resulting in inaccurate or biased results. This can have serious consequences for individuals who are misidentified or wrongly accused as a result of these failures.

According to a study published in the Journal of Big Data in 2020, facial recognition technology has been found to be less accurate for individuals with darker skin tones, as well as for women and younger people. The study analyzed data from a number of different sources, including government reports, academic papers, and media articles, and found that facial recognition technology had higher rates of error for these groups.

In addition, a report from the Georgetown Law Center on Privacy and Technology found that facial recognition technology has been used in a number of high-profile cases where it has resulted in false positives or other errors. For example, in one case, a man was falsely identified as a suspect in a crime due to an error in the facial recognition software used by the police department.

Conclusion continued

To address these concerns, it is important to ensure that facial recognition technology is thoroughly tested and evaluated to ensure its accuracy and fairness. This should involve collecting and analyzing data on the performance of the technology under a variety of conditions, including different lighting conditions, angles, and facial expressions. In addition, it is important to establish clear guidelines and protocols for the use of facial recognition technology to ensure that it is used in an ethical and transparent manner. This should include measures to protect the privacy and civil liberties of individuals, as well as procedures for correcting errors and addressing any negative impacts of the technology.

Furthermore, it is important to involve a diverse range of stakeholders in the development and oversight of facial recognition technology, including representatives from affected communities, civil liberties organizations, and technical experts. This will help to ensure that the technology is developed and used in a way that is fair and responsible, and that any negative impacts are minimized. Ultimately, facial recognition technology must be used ethically and effectively to combat cybercrime in order to ensure accuracy and fairness.

Sources:

- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In Proceedings of the 1st Conference on Fairness, Accountability and Transparency (pp. 77-91).
- Garvie, C., & Bedoya, A. (2016). The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy and Technology.