Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Reconvened Concluding Session

29 July – 9 August 2024

Submission of DB Connect

Comprehensive Analysis and Recommendations for the Proposed United Nations Convention against Cybercrime

1. Introduction

DB Connect presents this analysis of key provisions found in the Updated Draft of the United Nations Convention against Cybercrime (Crimes Committed through the Use of an Information and Communications Technology System). This examination builds upon DB Connect’s previous contributions to the Ad Hoc Committee (AHC).

The Convention aims to establish a comprehensive framework for international cooperation in combating cybercrime while respecting national sovereignty and safeguarding human rights. It addresses a wide range of issues, including the criminalization of various cyber offenses, procedural measures for law enforcement, mechanisms for international cooperation, and protections for human rights.

This report focuses on the Updated Draft Text of the Convention (UDTC) and seeks to contribute to the refinement of this crucial international instrument. It is structured to explore key aspects of the Convention, encompassing criminalization, procedural measures, law enforcement practices, protection of children, emerging technologies, cross-border access to electronic evidence, data protection and privacy concerns, jurisdictional complexities, capacity building, collaboration with the private sector, and considerations of human rights.
2. Criminalization

2.1 Comprehensive Framework

Articles 7-17 (pages 6-12) provide a robust framework for criminalizing various forms of cybercrime.

2.2 Issue: Ambiguous Terminology

The use of the term "dishonest or criminal intent" in Articles 7, 8, and 12 may lead to inconsistent application across jurisdictions.

Argument: Ambiguous terminology such as "dishonest or criminal intent" could result in varied interpretations among different legal systems, potentially undermining the Convention's effectiveness. Clarity in defining these terms within Article 2 or through interpretative notes is crucial to ensure uniform application and strengthen legal certainty globally.

Supporting Explanation: The R v Ghosh case (1982) EWCA Crim 2 serves as a poignant illustration of the complexities inherent in defining terms such as "dishonesty" or "criminal intent." This case introduced a bifurcated test encompassing both subjective (what the defendant knew or believed) and objective (whether the defendant's conduct was dishonest according to the standards of reasonable and honest people) elements to assess dishonesty. However, the application of this test can vary significantly across different legal systems due to disparities in cultural, social, and legal contexts.

To navigate this complexity, a hybrid approach is proposed. This framework incorporates specific definitions for established cybercrimes, providing a foundation of legal certainty. Simultaneously, it accommodates emerging threats through broader, adaptable terms, ensuring the Convention's enduring relevance. Complementing this approach, clear interpretive guidelines and a mechanism for regular reassessment are essential to maintain the Convention's efficacy in combating the multifaceted landscape of cybercrime.

By harmonizing precision with balance through clear definitions and adaptable frameworks, the Convention can establish a robust foundation for effective international cooperation in the pursuit of justice in the digital realm. Uniform interpretation and application of these terms are paramount to ensuring the Convention’s efficacy and fostering a level playing field for all nations in the global fight against cybercrime.

Recommendation: Retain the provision in Article 16 addressing non-consensual dissemination of intimate images, as it addresses an important and growing form of cybercrime.
3. Procedural Measures and Law Enforcement

3.1 Conditions and Safeguards

Recommendation (page 13): Article 24 provides a robust framework for ensuring that procedural measures are implemented with appropriate safeguards. Retaining the non-exhaustive list of conditions and safeguards in paragraph 2 is essential as it balances flexibility with core protections.

Argument: Article 24’s comprehensive framework ensures procedural measures align with international standards, safeguarding rights while enabling effective law enforcement. The inclusion of specific conditions and safeguards fosters trust and cooperation among States Parties, crucial for the Convention's success.

3.2 Enhancing International Cooperation in Combating Cybercrime

24/7 Network

Real-Time Coordination: The establishment of a 24/7 network, as outlined in Article 41, is critical for facilitating real-time information sharing and operational coordination among States Parties. This network will enhance:

- **Rapid Response**: Enabling the swift identification, analysis, and response to emerging cyber threats.
- **Intelligence Exchange**: Promoting the sharing of critical information and best practices among law enforcement agencies.
- **Collaborative Efforts**: Supporting joint investigations and operations to dismantle transnational cybercrime networks.

Refining Mutual Legal Assistance

Clarify Grounds for Refusal

While acknowledging the importance of national sovereignty, we propose refining Article 40, paragraph 21 as follows:

- **Human Rights Violations**: Expand grounds for refusal to include cases where there are reasonable grounds to believe that cooperation could result in human rights violations.
- **Clear Criteria**: Establish specific, objective criteria for applying each ground for refusal to ensure a consistent and equitable process.
• **Review Mechanism:** Implement a robust, independent review mechanism involving a multilateral panel of legal experts to adjudicate disputes over mutual legal assistance requests.

• **Encourage Partial Assistance:** Explore the feasibility of partial assistance, such as redacted information or access to specific data sets, to balance cooperation with national interests and data protection concerns.

• **Regular Review:** Commit to periodic evaluations of mutual legal assistance provisions to ensure their continued relevance and effectiveness in addressing both cybercrime and human rights concerns.

**Upholding Human Rights**

Human Rights Safeguards: Integrate explicit human rights considerations into mutual legal assistance frameworks. This includes:

• **Expanding Grounds for Refusal:** Ensuring that mutual legal assistance is refused if there are reasonable grounds to believe that it will lead to human rights violations, such as unfair political prosecution or discrimination.

• **Review Mechanism:** The proposed review mechanism should incorporate a strong human rights component to:
  ○ Ensure Transparency and Accountability: Provide a transparent process for resolving disputes related to human rights concerns.

• **Capacity Building:** Support capacity building in developing countries to enhance their ability to participate effectively in international cooperation and protect human rights.

**Recommendation**

To establish a balanced and effective framework for international cybercrime cooperation, we recommend:

• **Adopting Proposed Refinements:** Integrate the suggested refinements to Article 40, paragraph 21, ensuring that grounds for refusal are clear, consistent, and include human rights considerations.

• **Strengthening the 24/7 Network:** Enhance the operational capacity of the 24/7 network established under Article 41 to facilitate real-time coordination and rapid response.

• **Implementing Regular Reviews:** Establish a mechanism for periodic, independent evaluations of mutual legal assistance provisions to adapt to evolving cybercrime challenges and human rights standards.
- **Promoting Human Rights Safeguards**: Ensure that all mutual legal assistance aligns with international human rights standards and build capacity in developing countries to foster equitable and effective participation.

- **Exploring Additional Cooperation Mechanisms**: Consider developing platforms for joint investigations, information sharing, and capacity building to strengthen cross-border collaboration.

By adopting these recommendations, we can build a robust international framework that effectively combats cybercrime while upholding human rights and respecting state sovereignty. This approach will foster trust, strengthen global partnerships, and enhance overall security.

4. **Protection of Children**

4.1 **Criminalization**

**Recommendation (pages 8-9)**: Maintain the uniform age threshold of 18 years for child sexual abuse or child sexual exploitation material (CSAEM) as proposed in Article 14, aligning with established international legal norms.

**Argument**: Article 14's proposed uniform age threshold provides clarity and consistency in combating CSAEM globally, reflecting a collective commitment to protecting vulnerable children online. Maintaining this standard strengthens legal frameworks, enhancing accountability and deterrence against child exploitation.

4.2 **Protection of Vulnerable Populations in Legal Proceedings**

**Recommendation (page 16)**: Retain Article 40, paragraph 18, allowing for remote hearings of child victims via videoconference, ensuring equitable access to justice and safeguarding their well-being.

**Argument**: Article 40, paragraph 18's provision facilitates child victims' participation in legal proceedings without physical presence, mitigating trauma and ensuring their rights are upheld. This innovative approach underscores the Convention's responsiveness to evolving challenges in child protection, prioritizing their welfare in digital environments.

4.3 **Technical Assistance and Information Exchange**

**Recommendation (page 18)**: Maintain Article 53, paragraph 3(i), emphasizing expedited removal of child sexual abuse material, crucial in safeguarding children from online exploitation.

**Argument**: Article 53, paragraph 3(i)'s swift removal provision is indispensable in minimizing harm and protecting children from the psychological and emotional impact of CSAEM. Strengthening this measure
underscores the Convention's commitment to proactive intervention, reinforcing global efforts to create safer digital spaces for young people.

**Issue:** The current language "ensure the swift removal" in Article 53, paragraph 3(i) may not adequately emphasize the urgency of removing CSAEM.

**Argument:** Strengthening Article 53, paragraph 3(i) to "ensure the immediate removal" of CSAEM underscores the imperative nature of action against child exploitation. This revision enhances operational effectiveness, demonstrating a robust commitment to child protection within the Convention's framework.

5. **Artificial Intelligence and Emerging Technologies**

**Issue:** The Convention's omission of explicit provisions on artificial intelligence and emerging technologies may render it inadequate in addressing future cyber threats comprehensively.

**Argument:** Incorporating a dedicated article on artificial intelligence within Article 57 ensures the Convention remains adaptive and responsive to technological advancements. This proactive approach facilitates ongoing dialogue and adaptation, enhancing its efficacy in combating evolving cyber threats globally.

**Recommendation:** Integrate specific provisions addressing artificial intelligence's dual role in cybercrime prevention and criminal exploitation. This includes leveraging AI capabilities for proactive detection and mitigation, reinforcing the Convention's resilience in an increasingly digital landscape.

6. **Cross-border Access to Electronic Evidence**

**Recommendation (page 16):** Retain the semi-mandatory language "shall endeavor to" in Articles 45 and 46, ensuring flexible yet proactive approaches to real-time data collection and interception.

**Argument:** Article 45 and 46's semi-mandatory language balances operational imperatives with legal safeguards, fostering collaborative efforts in accessing electronic evidence across borders. This approach underscores the Convention's adaptability to diverse legal systems, essential in addressing transnational cyber threats effectively.

**Issue:** Article 42's procedures for expedited preservation of electronic data may lack sufficient rapidity, potentially compromising evidence integrity in time-sensitive investigations.

**Argument:** Implementing a fast-track procedure for urgent cases under Article 42 ensures timely preservation of electronic evidence, critical in preventing data loss and enhancing investigative outcomes. This streamlined approach reinforces operational efficiency, safeguarding evidentiary integrity and supporting robust cybercrime prosecutions.
7. Data Protection and Privacy

**Issue:** Balancing effective cybercrime prevention with individual privacy rights poses significant challenges under the Convention's current framework.

**Argument:** Strengthening Article 24 to explicitly mandate procedural measures' compliance with privacy and data protection principles ensures alignment with international standards. This enhancement reinforces trust in law enforcement practices while upholding fundamental rights, essential for sustainable global cooperation against cyber threats.

**Recommendation:** Introduce a dedicated article detailing data protection principles integral to implementing the Convention. This includes requirements for lawful, proportionate, and transparent data handling practices, fostering accountability and public confidence in cybercrime investigations.

8. Jurisdictional Challenges in Article 39

**Issue:** Article 39 of the Convention focuses primarily on facilitating the transfer of criminal proceedings between States Parties, a crucial element of international cybercrime cooperation. However, the Convention's silence on concurrent jurisdiction creates significant challenges in cases involving multiple jurisdictions. This gap can hinder effective investigation, prosecution, and adjudication of cross-border cybercrimes.

**Argument:** While the transfer of criminal proceedings is essential, it is insufficient to address the complexities of concurrent jurisdiction in cybercrime cases. Multiple jurisdictions often assert authority over the same offense, leading to potential conflicts, inefficiencies, and even immunity for offenders. Without clear guidelines for resolving these conflicts, international cooperation is hampered, and the prospect of successful prosecutions is diminished. For instance, imagine a cyberattack originating in Country A targeting a server located in Country B, while the victim resides in Country C. In such a scenario, all three countries might claim jurisdiction, leading to confusion, delays, and potentially jeopardizing the investigation.

**Recommendation:** To enhance the effectiveness of the Convention, Article 39 should be expanded to include specific provisions addressing concurrent jurisdiction. These provisions could establish criteria for determining primary jurisdiction, such as the location of the server attacked, the nationality of the victim, or the habitual residence of the perpetrator. Additionally, the framework could outline mechanisms for cooperation and information sharing between involved jurisdictions, including designated points of contact and standardized procedures for evidence exchange. Finally, provisions for resolving jurisdictional disputes could be established, potentially involving neutral third-party arbitration or pre-trial agreements between relevant States. By adopting a comprehensive approach that encompasses both the
transfer of proceedings and the resolution of jurisdictional conflicts, the Convention can become a more robust tool for combating cybercrime and ensuring justice for victims.

9. Capacity Building

**Recommendation:** Enhance Article 53's provisions for technical assistance and capacity building, prioritizing tailored support for developing countries. This includes knowledge transfer, training programs, and resource sharing to bolster cybercrime prevention and enforcement capabilities globally.

**Argument:** Article 53's expanded provisions foster inclusive participation in cybercrime mitigation efforts, promoting equitable access to technical expertise and operational resources. This inclusive approach enhances international solidarity, empowering all States Parties to effectively combat cyber threats and safeguard digital ecosystems.

10. Private Sector Cooperation

**Issue:** Insufficient clarity on private sector roles and responsibilities in cybercrime prevention may hinder collaborative efforts with law enforcement agencies.

**Argument:** Introducing a dedicated article on public-private partnerships within the Convention establishes clear frameworks for information sharing and technical cooperation. This collaborative approach enhances proactive threat detection and mitigation capabilities, reinforcing collective resilience against cybercrime globally.

**Recommendation:** Outline specific obligations for private sector entities in preserving and providing access to electronic evidence under Article 57. This includes guidelines on data security standards and lawful cooperation with law enforcement, fostering trust and operational synergy in combating cyber threats.

11. Emerging Cyber Threats

**Issue:** The Convention's current framework may not sufficiently address emerging cyber threats, including ransomware and IoT-based attacks.

**Argument:** Incorporating periodic reviews of emerging cyber threats within Article 57 enhances the Convention's adaptive capacity. This proactive approach facilitates ongoing risk assessment and mitigation strategies, ensuring continued relevance and effectiveness in combating evolving cybercrime challenges.

**Recommendation:** Expand existing provisions or introduce new articles within the Convention to address emerging cyber threats comprehensively.
This includes specific measures for ransomware mitigation, IoT security protocols, and adaptive response frameworks, reinforcing global resilience against dynamic cyber risks.

12. Human Rights

12.1 Balancing Cybercrime Prevention with Human Rights Protection

Reference: Article 6, paragraphs 1-2

Argument: Article 6's mandate to consider human rights in all Convention actions ensures lawful and proportionate responses to cybercrime threats. Upholding individual freedoms while combating criminal exploitation fosters public trust and adherence to international legal norms, essential for sustainable global cooperation against cyber threats.

Recommendation: Retain and expand Article 6's human rights provisions to encompass diverse international human rights instruments. This inclusive approach reinforces universal values and ethical standards in cybercrime prevention, promoting equitable justice and respect for fundamental freedoms worldwide.

12.2 Human Rights Safeguards in Procedural Measures

Reference: Article 24, paragraph 1

Argument: Amending Article 24 to explicitly mandate procedural measures' compliance with human rights safeguards ensures equitable justice and legal accountability. Upholding privacy rights and due process principles enhances public confidence in law enforcement practices, essential for effective cybercrime prevention and prosecution.

Recommendation: Introduce detailed guidelines within Article 24 on lawful, proportionate, and transparent procedural measures. This includes judicial oversight requirements and accountability mechanisms, reinforcing human rights protections while combating cybercrime globally.

12.3 Protection of Freedom of Expression

Reference: Article 53, paragraph 3(e)

Argument: Expanding Article 53, paragraph 3(e) to include explicit protections for freedom of expression promotes digital inclusivity and democratic values. Safeguarding journalistic integrity and academic discourse enhances public discourse while deterring cybercrime, essential for sustaining open societies and global cybersecurity.
**Recommendation:** Strengthen Article 53, paragraph 3(e) to uphold freedom of expression principles across digital platforms. This includes safeguards against censorship and undue restrictions on lawful online activities, reinforcing democratic values in cybercrime prevention efforts.

**13. Conclusion**

To conclude, the proposed United Nations Convention against Cybercrime marks a substantial step forward in global cybersecurity governance. By establishing robust legal frameworks, fostering international cooperation, and prioritizing human rights, the Convention provides a critical foundation for addressing the evolving challenges of the digital age. Effective implementation of the recommendations outlined in this report will be instrumental in ensuring the Convention's adaptability and resilience.

As the cyber threat landscape continues to evolve, ongoing collaboration, innovation, and a steadfast commitment to human rights are essential. By prioritizing legal clarity, operational efficiency, and inclusive dialogue, States Parties can create a secure digital future for all. A united and proactive approach is imperative to harness the full potential of the Convention and protect global digital ecosystems for generations to come.

Kind regards,

**Denise Bowen**

CEO, DB Connect

- Advisor & Committee Member, UN Universal Health Coverage and Cybercrime
- Advisory Council Member, EmblemHealth
- Judge, Pharrell Williams' Black Ambition
- Mentor: Techstars, Black Girls in Cyber, Verizon Small Business Digital Ready
- Local Advisory Council Member, ForbesBLK|Forbes
- Coach and Mentor, WomenTech Network

edenise@dbconnectus.com | ☎️ (347) 573-0517