Closing Statement by DB Connect at the Conclusion of the 6th Session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Dear Honorable General Secretariat, Member States, and Esteemed Colleagues,

Future-Proofing Against Cybercrime: Insights from 2024 Predictions

DB Connect welcomes the opportunity to submit its proposals in advance of the Sixth Session of the Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. As we embark on the critical task of drafting a comprehensive international convention on cybercrime, it's imperative to consider the rapid evolution of the cyber threat landscape. To that end, I would like to highlight pertinent cybersecurity predictions for 2024 compiled from Cybersixgill, closely aligned with our objectives:

Growth of AI as an Attack Tool and Target
The projected proliferation of AI-powered cyberattacks and the emerging use of AI systems as direct attack vectors warrant our attention. As generative AI enables sophisticated social engineering at scale, implementing safeguards against adversarial uses while encouraging responsible development is crucial. Addressing risks from AI-related threats and system vulnerabilities should be integral to our vision.

Elevated Geopolitical Threats
Predictions indicate that state-sponsored influence operations targeting critical infrastructure and essential services will intensify in times of global turmoil. Strengthening international cooperation and preventive capacities becomes paramount as non-financial motivations grow, potentially expanding targets and tactics. We must reinforce social cohesion against those seeking chaos.

Regulatory Pressures for Proactive Security
Cybersecurity regulatory requirements and executive accountability are tightening. Our guidelines can assist organizations in managing compliance through prioritized risk mitigation driven by cyber threat intelligence. Promoting data-based, context-aware, continuous security assessments would significantly improve baseline cyber hygiene.

The vision outlined in these projections closely mirrors the objectives we seek through the convention. I invite you to peruse the attached cybersecurity report in detail; its actionable insights can profoundly inform our way forward. Your feedback on pertinent areas of alignment would be invaluable.

Let us collaborate to future-proof global cybersecurity through an adaptable and far-sighted convention that withstands the test of time.

The Imminent Cost of Cybercrime: A Projected $10.5 Trillion by 2025

Cybersecurity Ventures projects a significant surge in global cybercrime expenses, expecting an annual growth rate of 15 percent over the ensuing five years. By 2025, these costs are anticipated to skyrocket to $10.5 trillion USD annually, a substantial increase from the $3 trillion USD recorded in 2015. This projection signifies an unprecedented transfer of economic wealth in history.

The ramifications of this exponential growth extend beyond mere monetary figures. It poses a substantial threat to incentives for innovation and investment, eclipsing the magnitude of damage inflicted by natural disasters in a single year. Astonishingly, it is projected to surpass the profitability of the global trade of all major illegal drugs combined.

This estimation is grounded in historical cybercrime data, accounting for recent year-over-year escalation and a marked surge in hostile nation-state sponsored and organized crime gang hacking activities. Additionally, the projected cyberattack surface for 2025 is expected to be exponentially larger than the present scenario, indicating an imminent and substantial threat landscape.

These figures underscore the urgent need for global attention and collaborative action to address the burgeoning threat of cybercrime. Failure to take decisive measures could lead to profound socio-economic repercussions worldwide.

United States' Perspective and Global Vision: Shaping an Inclusive Cybercrime Treaty Framework

As an esteemed member of the ad hoc committee and a multi-stakeholder based in the United States, my dedication to shaping global recommendations arises from a joint responsibility. It is vital, as representatives of diverse interests, to synthesize perspectives from the United States and worldwide viewpoints into a comprehensive framework. Acknowledging the analysis from the United States and integrating it with broader international perspectives, my recommendations aim to reconcile the language and implementation of the treaty, maintaining a balance between sovereignty and fundamental rights. Embracing the necessity for adaptability in the face of evolving threats, my suggested improvements aim to strengthen the treaty's resilience while preserving its original intent. Through deliberate dialogue to reconcile subtle differences, our collective endeavor focuses on constructing an adaptable and inclusive treaty framework that promotes collaboration and transcends ideological differences. This collaborative initiative, founded on empathetic reasoning and a shared commitment to international security, lays the groundwork for a progressive and cohesive approach, ready to tackle the intricacies of our digital age while upholding fundamental rights universally.

Leveraging Synergy: How Encode Justice New York and My Expertise Shaped the Draft Treaty's Framework

High school students associated with Encode Justice New York provided invaluable feedback on specific aspects of my draft treaty recommendations, focusing on crucial areas such as uniform terminology, multilingual resources, data requirements, and potential disproportionate impacts. While Encode Justice primarily focuses on human rights and AI governance, nonetheless, the students contributed general feedback through a civil liberties lens that assisted in strengthening related messaging.

Drawing from my extensive experience as a member of the ad hoc committee, specializing in cybercrime policy and legislative frameworks, I carefully assessed how to integrate their feedback effectively. This led to targeted revisions in the draft, incorporating some of their suggestions through nuanced adjustments to language and content.

While acknowledging Encode Justice New York's valuable perspective from a youth rights standpoint, the primary responsibility for formulating expert recommendations aligned with the goals of the treaty committee rested with me. I applied my specialized expertise to translate pertinent suggestions into meaningful enhancements. The final iteration of the draft reflects my deep technical understanding of cybercrime.

Scope of Application (Article 3)

It is recommended to clarify that the Convention's scope encompasses cyber-enabled crimes, including online fraud, identity theft, threats, extortion, and intrusions into computer systems.

Moreover, suggesting the addition of language emphasizing the obligations of States Parties to uphold sovereignty and refrain from engaging in activities that could harm the critical infrastructure of other States.

Protection of Sovereignty (Article 4)

Proposing to bolster the sovereignty provision by explicitly prohibiting cyber operations that contravene the domestic laws of the target State or qualify as internationally wrongful acts.

Additionally, recommending language that affirms the commitment of States Parties to resolve disputes through peaceful means.

Respect for Human Rights (Article 5)

It is advisable to fortify the language to mandate that States Parties ensure the consistent implementation of the treaty in accordance with their obligations under international human rights law. This includes, but is not limited to, the realms of privacy, due process, and non-discrimination. It is recommended to

explicitly outline fundamental principles such as legality, necessity, and proportionality, alongside provisions for effective remedies and impartial oversight.

Additionally, there is a need to emphasize the imperative of safeguarding vulnerable groups and advocate for gender-sensitive approaches in the execution of the treaty.

Criminalization Provisions (Articles 6-16)

There is a discernible necessity to enhance the differentiation between provisions aimed at addressing crimes that result in harm to individuals, economic interests, or critical infrastructure and those targeting intrusive surveillance or censorship. Certain articles within this domain appear to possess an overarching scope.

It is proposed to precisely define the outcomes deemed harmful to uphold the principles of legality and fair notice. Furthermore, it is recommended to specify protections for legitimate cybersecurity research, encryption practices, anonymity, and whistleblowing.

Criminal Liability and Sanctions (Article 21)

Suggesting the inclusion of language mandating States Parties to establish accessible procedures and effective remedies for individuals wrongly accused or subjected to improper surveillance based on erroneous digital evidence or unlawful cyber tactics.

Further, recommending the explicit requirement for sanctions regimes to adhere to international human rights standards.

Procedural Measures (Articles 23-30)

There is a pressing need to bolster safeguards pertaining to oversight mechanisms, privacy impact assessments, data security protocols, and limitations on data retention. It is suggested to introduce additional protections for sensitive data, such as safeguarding journalist sources, doctor-patient communications, and religious confessions.

To enhance clarity, it is advised to distinctly outline the criteria and procedures necessary for compelled assistance as opposed to voluntary cooperation by service providers. Incorporating independent checks before granting permits is also proposed.

International Cooperation (Articles 35-40)

It is recommended to strengthen the criteria for refusing cooperation in instances where human rights concerns, notably pertaining to privacy, fair trial, non-discrimination, and humanitarian protections, are evident. Suggesting an explicit prohibition on the transfer of data that could facilitate human rights violations is also advocated.

In summary, it is advised to bolster human rights protections comprehensively throughout the treaty. This entails enhancing clarity concerning definitions and standards of liability, enumerating checks and balances, and distinctly delineating between voluntary and compulsory requirements for both entities and security researchers.

General Principles of International Cooperation (Article 40)

It is advisable to introduce language that enables States Parties to reject cooperation requests that might undermine crucial rights such as privacy and fair trial guarantees.

Furthermore, it is suggested to explicitly authorize States Parties to engage in cooperation concerning cybercrime matters through regional conventions or bilateral mutual legal assistance treaties.

Illustrating Operational Guidelines

1. Privacy Protection: States Parties should have the authority to reject cooperation requests that demand the disclosure of personal data without adequate safeguards. For instance, if a request entails the release of sensitive user information from a digital platform without proper legal procedures or protections, States Parties should reserve the right to decline such requests to safeguard individual privacy rights.

2. Fair Trial Guarantees: It's crucial for States Parties to retain the ability to reject cooperation requests that might compromise fair trial guarantees. For example, if a request requires sharing evidence obtained through illegal means or without proper judicial oversight, States Parties should have the discretion to deny such cooperation to uphold the integrity of fair trial principles and prevent the use of unlawfully obtained information in legal proceedings.

24/7 Network (Article 41)

Recommendations entail mandating that points of contact possess relevant expertise in human rights and civil liberties protections while handling international requests.

Additionally, proposing language that steers 24/7 Network cooperation towards established international channels, like INTERPOL, while maintaining stringent privacy and data security measures.

Preventive Measures (Article 53)

It is recommended to instruct States Parties to collaborate with national human rights institutions, privacy advocates, and technology experts in crafting preventive measures and raising public awareness. Additionally, prioritizing the development of multilingual curriculums for workshops and prevention programs is paramount. This approach ensures accessibility across diverse linguistic communities, empowering a larger segment of the population to comprehend and actively engage in safeguarding against cyber threats. By offering materials in multiple languages, we not only break language barriers but also democratize access to crucial information, fostering a more inclusive and informed society in countering cybercrime.

Statistics on Cybercrime (Article 55)

Furthermore, it is pivotal to advocate for language that not only encourages research into the underlying causes facilitating cyber violence but also emphasizes understanding the specific communities and groups most impacted by these acts. This inclusive approach will illuminate not just the circumstances enabling cybercrime but also shed light on the disproportionate effects on certain demographics. By comprehensively studying these societal factors and their differential impacts, we can craft more informed and targeted preventive measures. This nuanced understanding is crucial in developing strategies that address the root causes and provide tailored support to the most vulnerable communities, ultimately fostering a more effective and inclusive approach in countering cyber violence.

Conference of the States Parties (Article 57)

Suggesting language that promotes the active involvement of human rights organizations, digital rights groups, and pertinent stakeholders in Conference of States Parties meetings.

Further recommendation is to direct the Conference to deliberate on the impact of cybercrime policies on the security and privacy of communications, encompassing cryptography, browsing anonymity, and digital journalism.

In-Depth Assessment of Proposed Treaty Recommendations by the United States

Applicability of Articles 6-16 to Modern Cybercrime

Areas of Agreement

I agree with the United States's analysis that the consensus within articles 6-16 utilizes technology-neutral language effectively, thereby criminalizing prevalent cyber-dependent and cyber-enabled offenses. These include ransomware attacks, intrusions into critical infrastructure and government systems, malicious data interference, illegal surveillance leading to privacy violations, trafficking in stolen credentials, fraudulent schemes, and identity theft. The examples provided vividly illustrate the draft treaty's robustness against current and emergent threats.

Potential Risks and Unintended Consequences

The United States rightly emphasizes Member States' freedom to interpret certain acts as "without right" within their domestic systems, acknowledging the balance between respecting sovereignty and making complex determinations. However, a thorough examination of implementing legislation, whether formal or informal, in subsequent expert reviews would ensure that fundamental rights remain central, aligning with the treaty's intended purpose.

We acknowledge the necessity for agile instruments adaptable to unforeseen developments. My recommendations aim to strengthen this aspect rather than undermine it, fostering continued dialogue. While our approaches align in substance, nuanced differences in treaty language may exist. Further discussions could uncover innovative compromises.

Building Bridges Beyond Differences: A Call for Collaborative Evolution in Treaty Development

This comprehensive review underscores our substantial agreement and identifies areas where differing perspectives provide opportunities for nuanced formulations. Constructive discussions, accounting for technical and social evolution, will allow us to shape a flexible framework that also upholds fundamental rights.

Our focus now should address unresolved treaty areas impeded by ideological differences. By spreading our aligned vision, breakthroughs across divisions become plausible through sustained empathetic reasoning. I eagerly anticipate further collaboration to build upon this foundation.

Ad hoc committee members, amidst the diversity in our approaches, I wholeheartedly acknowledge our shared commitment to crafting an impactful cybercrime treaty that harmoniously balances security and individual rights. The expansive overlap in our agreement areas forms a robust foundation, providing us with a solid platform for progress.

By emphasizing our common treaty objectives, we have the opportunity to collaboratively enhance this collective groundwork in a spirit of trust and cooperation. Initiating discussions with a positive mindset opens the door to resolving nuanced disputes through collective efforts. I am confident that our unified purpose, deeply rooted in global well-being, will catalyze the ongoing and constructive evolution of this pivotal accord. Together, let us propel this treaty toward new heights of effectiveness and relevance.

Kind regards,

Denise Bowen
Chief Executive Officer, DB Connect
Committee Member, United Nations Universal Health Coverage and Cybercrime
Committee Member, Regional Cyber Crime Consultation for the Americas (UNODC-NGO Unit)
Advisory Council Member, EmblemHealth
Local Advisory Council Member, ForbesBLK|Forbes
Mentor, Techstars
Mentor, Black Girls in Cyber
Mentor, Verizon Small Business Digital Ready
Coach and Mentor, WomenTech Network

denise@dbconnectus.com