G20 Conference on "Crime and Security in the Age of NFTs, AI and Metaverse"

Chair's Summary

13-14 July 2023, Gurugram, India

वसुधैव कुटुम्बकम् | ONE EARTH • ONE FAMILY • ONE FUTURE

G20 Conference on "Crime and Security in the Age of NFTs, AI and Metaverse"

Chair's Summary

The Chair's Summary is established under the responsibility of the Conference's Chair, with the purpose of reflecting key issues discussed during the Conference on Crime & Security in the age of NFTs, AI and Metaverse that took place in Gurugram, Haryana on 13-14 July 2023

In the context of India's G20 Presidency from December 2022 to November 2023, G20 delegates met in Gurugram on 13-14 July 2023 to deliberate on challenges of cybercrime and security in the era of new and emerging technologies like Non-Fungible Tokens (NFTs), Artificial Intelligence (AI) and Metaverse. The conference provided a platform for discussions to the distinguished delegates from the G20 countries, invitee countries, international organisations and multi-stakeholder participants on the following subjects;

- Internet Governance - National Responsibility and Global Commons.
- Securing Digital Public Infrastructure (DPI) - Amidst Unprecedented Scale of Digitalization: Design, Architecture, Policies and Preparedness.
- Extended Reality, Metaverse and Future of Digital Ownership - Legal and Regulatory Framework.
- Artificial Intelligence - Challenges, Opportunities and Responsible Use.
- Connecting the Dots on Dark Net: Challenges of Crypto currency and Dark Net.
- Criminal Use of Information and Communication Technologies (ICT) - Evolving a Framework for International Cooperation.

2. Today, the world is more digitally connected than ever before. Malicious online actors take advantage of vulnerabilities for attacking ICT systems. They are becoming increasingly agile and organized in exploiting new technologies, coordinating targeted attacks into the ICT infrastructure, causing serious harm to individuals, societies, businesses and governments. Malicious cyber activities transcend international boundaries. Due to its transnational nature, preservation and faster sharing of information and evidence for the purpose of investigation and prosecution is also becoming more challenging, due to lack of international cooperation frameworks. As victims of such crimes and ICT infrastructure used in such crimes span multiple jurisdictions, any response will need to be closely synchronized between countries.

3. As dependence on use of ICTs increases globally, the risks of crimes using new and emerging technologies like NFTs, AI and Metaverse will also increase. For example, with lines blurring between physical and virtual world, malicious actors have been innovative with the use of the Metaverse for a variety of purposes, including but not limited to identity theft, fraud, technology facilitated gender based violence, and malicious attacks on other users. It is imperative to be cognizant of the security risks including to privacy, fraud, key management loopholes, marketplace security and other cyber risks, in order to plan and tackle them holistically with the right control levers across the ecosystem.

4. The misuse of ICTs along with new and emerging technologies and advanced ICT tools by State and non-State actors for terrorist purposes is a serious concern for global security and stability, economic and social development, as well as the safety and well-being of individuals. The importance of deterring, preventing and combating the use of ICTs for terrorist purposes and strengthening of international cooperation, through exchange of best practices, sharing of information and effective and efficient mutual legal assistance, was underscored.

5. ICT environment is an increasingly complex and dynamic environment and the increased use of ICTs in day-to-day individual, social, political and economic activities post the COVID-19 pandemic has resulted in an increased number of malicious actors targeting ICT vulnerabilities to steal data, breach privacy, disrupt critical ICT infrastructure and commit financial fraud. While emerging technologies such as AI, Big Data, Cloud Computing and others have high potential for creating economic opportunities, and are neutral in nature, these could increase vulnerabilities and expand attack vectors and hence there is an urgent need that these advanced technologies are used ethically, in ways that respect international law, with malicious actors being prevented from exploiting them for criminal and terrorist purposes. It is critical to strengthen and develop capacities of individual states, international organizations and relevant stakeholders to better respond to traditional, non-traditional and new and emerging challenges, including terrorism and its financing, money laundering, misinformation and disinformation.

6. The Darknet has gained popularity among cyber criminals due to its perceived anonymity and the ability to conduct various activities generally outside the reach of law enforcement agencies. Within the Darknet, one prominent trend is the increasing criminal misuse of crypto assets as a medium of financial transaction. Collaboration between law enforcement agencies, financial institutions, technology companies, and cryptocurrency exchanges can lead to better intelligence and coordinated efforts to combat illegal

activities. By addressing the challenges, implementing robust solutions, and exploring future directions, stakeholders can strive to connect the dots in the Darknet and create a safer digital environment for all users.

7. The use of AI, Metaverse, NFTs, Dark Net, Deep fakes, Internet of Things (IoTs) and other technologies by malicious actors is increasing rapidly. There is concern about AI generated cyber-attacks, malware, highly convincing information manipulation, and scams that can be deployed cheaply and at formidable scale using these tools. There is also a need for analysis of capabilities and applications of AI technologies of malicious actors that can be exploited for malicious purposes. Focussed discussions on the need for transparent and accountable AI governance frameworks to ensure the responsible use of AI technologies is necessary considering the recent developments in this field. The emerging challenges and risks associated with the misuse of Non-Fungible Tokens (NFTs) needs to be explored. In-depth discussions, knowledge exchange, and the formulation of strategies to address this evolving threat landscape is necessary. The Conference also shed light on the challenges in tackling illicit activities associated with Metaverse technologies by facilitating discussions and presenting recommendations and insights during the discussions. The ideas generated in the conference will contribute to the development of effective strategies, policies, and collaborations to mitigate the threats posed by Metaverse-related concerns.

8. The promotion of an open, secure, stable, accessible, peaceful and accountable ICT environment was emphasized, as was the need for a comprehensive and balanced approach to ICTs development and security, including technical advancement, business development, safeguarding the security of States and public interests and respecting privacy right of individuals. Concerns were raised over the increasing challenge to protect individuals, particularly women and children, from online sexual exploitation and from other content harmful to their health and well-being. Stakeholders are looking forward to strengthen cooperation to develop initiatives aimed at ensuring safety of users, especially children and women on the Internet.

9. Concern was expressed over malicious cyber activities contrary to established norms, principles and rules of responsible State behaviour in cyberspace and international law. It was stressed that co-ordination on prevention and mitigation strategies against Advanced Persistent Threats (APTs) is needed. All States need to work together to achieve a comprehensive international convention on countering the use by ICTs for criminal purposes under the UN framework, taking into account the existing international frameworks. This would promote effective and efficient international cooperation on

preventing, deterring, detecting, mitigating, investigating and prosecuting crimes and the malicious online actors while ensuring speedy justice for the victims of new age crimes. It would also respond to the need for appropriate safeguards including data protection while balancing the needs of Law Enforcement Authorities (LEAs) to enable them combat these crimes.

10. Working in partnership with a whole-of-society approach increases mutual cyber resilience and security. Furthermore, working closely with industry and through international organisations would also be key to ensuring that the new and emerging technologies are 'secure by design' and are deployed under consistent and cohesive frameworks and standards. Support to efforts to increase the availability of cyber skills in workforce and promoting people-to-people and educational links enhances awareness and preparedness in the domain of cyberspace.

11. Capacities to secure information systems, develop resilience, protect critical information infrastructure, identify threats and respond to them in a timely manner vary from one country to another. These differences in capacities and resources related to the use of ICTs, unequal awareness and access to existing cooperative measures available to mitigate, recover and investigate such malicious ICT activity need to be addressed. It is crucial to promote capacity building, technical assistance, public-private partnership, awareness and education to bridge these gaps.

12. In the light of the ever-increasing importance of crime and security, dialogue on these matters would be continued at mutually agreed fora and periodically, in order to foster strong and inclusive international cooperation to deal with these challenges effectively and comprehensively.

13. The Chair thanked delegates from G20, invited countries and international organisations, including INTERPOL and UNODC, as well as the Speakers at the thematic sessions, for their participation and contributions. Delegates recognized that India's G20 Presidency has established a valuable platform for discussions on the challenges of crime and security in the age of NFTs, AI and Metaverse.