IGF 2023 High Level Session I: Understanding
8 October 2023 | 09:30 - 11:00 JST | Kyoto, Japan
Summary Document

Speakers

Mr. Taro Kono, Minister for Digital Transformation, Japan; Ms. Courtney Gregoire, Chief Digital Safety Officer, Microsoft; Mr. Junhua Li, UN Under-Secretary-General for Economic and Social Affairs; Ms. Leonida Mutuku, AI Research and Strategy Lead, Local Development Research Institute; and Ms. Shivanee Thapa, Senior News Editor & Presenter, Nepal Television (moderator).

Summary

Digital Risk in Emerging Technologies

As emerging technologies like artificial intelligence (AI), the Internet of Things (IoT), and blockchain become more integrated into the global economy, they introduce both unprecedented potential and a wide range of new risks. The digital risk terrain is constantly evolving, with new vulnerabilities emerging as more industries adopt these technologies. Key risks include cybersecurity threats, such as data breaches, ransomware attacks, and the malicious use of AI, all of which can compromise the integrity of digital systems. Privacy concerns also loom large, particularly in areas like biometric data and the increasing volume of personal data processed by automated systems. These risks highlight the need for robust digital resilience, which is essential to safeguard public trust in these technologies.

The Role of Cyber Resilience

Building resilience to address these risks requires a comprehensive approach that combines technological defenses with cross-sector collaboration. Cyber resilience not only involves developing cutting-edge cybersecurity solutions but also fostering a culture of continuous risk assessment and incident response preparedness. To stay ahead of evolving threats, organizations must adopt adaptive governance models, incorporate AI-driven security measures, and engage in cross-industry partnerships to share best practices. Moreover, improving the digital literacy of both public and private sector actors is critical to empowering stakeholders to identify and address emerging risks in real time.

Proactive Regulation and Global Cooperation

In addition to internal security measures, the role of proactive regulation is essential for managing the growing complexity of digital risks. Global cooperation is necessary to develop international standards that can support seamless cross-border data flows while ensuring that security and privacy are maintained. Key challenges include aligning national regulations to avoid fragmentation and ensuring that regulatory frameworks are flexible enough to adapt to future technologies. An inclusive multistakeholder approach that brings together governments, private companies, and civil society is vital in shaping regulations that protect users without hindering innovation. Effective regulations should focus not only on data security but also on ethical considerations, especially as AI and machine learning continue to evolve.

Addressing the Digital Divide

One critical aspect of digital resilience is ensuring that all regions, including developing countries, can keep pace with technological advancements. The digital divide poses a significant risk, as regions with limited access to cutting-edge technologies are more vulnerable to cyberattacks and data privacy issues. Governments and international organizations need to invest in infrastructure and capacity-building programs to promote digital inclusion, ensuring that vulnerable populations are not left behind in terms of both access and security.

Ensuring digital resilience is not only about addressing immediate risks but also about laying the groundwork for a safe and trustworthy digital future. As the digital landscape continues to evolve, fostering global cooperation and maintaining flexibility in both governance and technology will be key to mitigating risks and ensuring that technological advancements benefit all.