7TH OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF INFORMATION AND TELECOMMUNICATIONS TECHNOLOGIES 2021-2025 (NEW YORK)

STATEMENT BY THE REPUBLIC OF KAZAKHSTAN (MARCH 4TH, 2024)

Existing and Potential Threats

Kazakhstan expresses its full support for the work of Open-ended Working Group in facilitating consensus on key international ICT agenda items.

In the realm of digital world, the emergence of AI and machine learning technologies presenting challenges despite significant advantages in ICT security.

The potential for the abuse of AI within the critical infrastructure by malicious actors is a concern. While security experts use AI to counter cyber threats, cybercriminals can employ this technology to devise new forms of attacks.

It also being used to create and spread misinformation and disinformation by generating vast amount of content quickly and convincingly, making it difficult for users to identify fact from fiction.

On our side, Kazakhstan recently finalized its AI Development Concept for 2024-2029, set for approval this year.

It underscores the potential of AI systems to analyze extensive data and make decisions based on identified patterns, aiming to enhance service quality and improve overall user experience with guideline for AIs safe using.

Furthermore, it is crucial to highlight the significance of data breaches.

States should comprehend that protection of sensitive data, is paramount. Cybersecurity measures as encryption and authorized access are essential to protect against online threats.

With the continuous development of technology, the landscape of cybersecurity is constantly changing, making data breaches, ransomware attacks, and hacking incidents more commonplace.

As a result, we should prioritize cybersecurity initiatives, implement protective measures, and stay aware against emerging cyber threats to uphold the integrity and security of personal data.

As of today, our government is taking additional measures to prevent data leaks. On that, the secondary law signed last year, which is directed, towards the protection of personal data and ensuring cybersecurity in general.

Finally, we consider it important to emphasize the significance of Internet of Things (IoT) and cloud computing technologies security in the era of 5G. The development of 5G networks introduces unique challenges in the realm of ICT security. The expanded attack surface of IoT devices and cloud computing increase the risk of cyber threats.

Within this framework, the use of 5G also introduces new possibilities for DDoS attacks.

Ensuring security in networks and managing safety in use of critical infrastructure with many devices demands cautious application of protective measures and raising awareness in creating cyber resilience.