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 7TH, 2024)

Confidence-Building Measures

Kazakhstan fully supports the use of Confidence-Building Measures. Facilitating a common understanding of ICT security terminology among participating states serves as a foundational step to enhance trust, communication, and cooperation in effectively addressing the complex landscape of cybersecurity challenges.

We consider it important to indicate the creation of a list of ICT terminology as one of the CBMs. Including ICT terminology in Confidence-Building Measures is crucial, as this terminology resource helps in understanding key concepts in the field of ICT. The glossary is needed not only for participating states but also for all who would like to familiarize themselves with the text of the annual reports for a more understandable text and with the content of abbreviations in it.

Furthermore, we should highlight the institute of raising awareness as a key component of the CBMs, prioritizing this effort. This initiative not only encourages a broad understanding of cyber threats but also encourages active participation from all stakeholders in preventive measures. On that note, it would be beneficial to compile a list outlining potential approaches to raising awareness, drawing from the collective experiences of all participating States willing to share their best practices. The proposed awareness-raising measures can be made as a questionnaire and posted on the PoC portal, making it more informative and increasing its importance.

It is also necessary to focus on highlighting capacity building as one of the CBMs, by providing states with the necessary skills and knowledge to effectively counter cyber threats and manage cyber incidents. On that note, we consider that participating states should develop capacity-building initiatives aimed at enhancing their capabilities in ICT threats and vulnerabilities, promoting ICT security, and developing the skills necessary to effectively respond to cyber incidents.

As for points of contact, we support the work of the PoC as it helps improve coordination, expedite the resolution of concerns, and overall strengthen cybersecurity measures. Like many countries, Kazakhstan is currently in the process of appointing points of contact. In our part working with the CBMs, Kazakhstan is the only country in Central Asia within the framework of OSCE co-curating one of the confidence-building measures together with Canada, related to ensuring the open, interoperable, secure, and reliable Internet. As part of the CBM work, we organized sub-regional training sessions in our state last year, related to the use of CBM and ways to counter cyber threats. Furthermore, we also actively support the OSCE's work on Points of Contact, and to date, Kazakhstan is actively applying this in practice. For instance, we already had a case where through the OSCE's communities portal for PoC, we were able to contact representatives of another State

to request information on a cyber attack. This approach contributes to quick coordination and active cooperation.

Finally, we support highlighting the role of public-private partnerships. We propose reflecting on the work of white hat hackers as they play an important role in this sector as a strategic mechanism for cultivating trust, enhancing communication channels, and significantly improving response capabilities in the face of evolving threats.