Regulatory and Legal Implications of AI in Security:

Esteemed delegates, as we witness the increasing integration of artificial intelligence into cybersecurity operations, the Russian Federation acknowledges the importance of addressing regulatory and legal implications to ensure the responsible and ethical use of AI technologies.

Russia advocates for the development of clear and comprehensive regulatory frameworks that govern the deployment and operation of AI-driven security solutions. These frameworks should encompass issues such as data privacy, liability, transparency, and accountability to uphold the rule of law and protect the rights of individuals and organizations.

In our commitment to promoting a safe and secure digital environment, the Russian Federation is actively investing in cybersecurity measures as well as artificial intelligence (AI) technology to improve its cyber capabilities. Our cybersecurity strategy involves a multi-layered approach that includes preventative measures such as network security, firewalls, and antivirus software, as well as reactive measures in the event of a cyber-attack.

In terms of AI, Russia is using the technology for a variety of cybersecurity purposes including threat detection, intrusion prevention, and cyber-attack response. We also have established cybersecurity centres and cooperation programs with other countries to develop and implement emerging technologies to protect us from cyber threats.