The BPF Cybersecurity is inviting Community feedback

To Whom It May Concern:

Please apologize for my late feedback, but I hope it will be still considered during the BPF workshop at the IGF meeting.

The following summarizes my feedback.

Artificial intelligence risks are largely absent in Cybersecurity Frameworks
Most of the reviewed international cybersecurity (CS) frameworks do not consider artificial intelligence (AI) as a new source of cybersecurity or cyberphysical threat. To combine both communities and debates, that of conventional cybersecurity and AI security, is important in order to increase security or best mitigate CS risks in the future. For AI will fundamentally change the cybersecurity risk landscape. AI will intensify existing methods of CS attacks, will cause new forms of cyberphysical attacks, and make attacks much more precise and economically viable for the attacker. AI will further complicate both the deterrence and attribution of cyberattacks due to the increasing complexity and interconnectedness of digital networks and methods of deterrence and attack. AI will cause longer term structural or transformational risks, which are usually not addressed in any of the cybersecurity frameworks. Structure risks relate to economic, governmental, societal, and military imbalances. Finally, one way to make networks more secure in the future is through the use of AI. At the same time, AI-based security technologies will introduce new forms of vulnerabilities. For example, hacker will induce or coerce non-person entities (NPEs) agent to gain privileged access to network or impersonate NPEs agents. National security agencies increasingly implement zero-trust architectures (ZTA), which should also be addressed by international CS frameworks.

Kind regards,
Thorsten Jelinek

Dr. Thorsten Jelinek
Director and Senior Fellow
Taihe Institute 太和智库
Website: http://www.taiheinstitute.org