the 2021 innovations dialogue.

HIGHLIGHTS

- Increasingly powerful deep learning algorithms accompanied by the rapid advances in computing power have enabled the generation of **hyper-realistic synthetic media; malicious synthetic media is commonly referred to as 'deepfakes'**.
- **Deepfakes include all forms of digital content—video, text, images, and audio**—that have been either manipulated or created from scratch using deep learning algorithms to primarily mislead, deceive or influence audiences.
- By portraying someone doing something they never did or saying something they never said, increasingly sophisticated **deepfakes could challenge and influence perceptions of reality**.
- The fabrication and manipulation of digital content is not a new phenomenon. **The growing deepfake phenomenon however represents a significant leap forward** from what has come before primarily because: a) the fidelity of synthetic media is unmatched; b) along with manipulation, synthetic content that did not exist before can be fabricated; c) synthetic media technology allows the manipulation or fabrication of all forms of digital media, not just images; and d) sophisticated synthetic media generation is becoming increasingly accessible through the emergence of user-friendly software tools and services.
- **Synthetic media technology is not inherently malign**, it has many beneficial applications across social and economic sectors ranging from advertising and education to fashion and entertainment.
- **Deepfakes are however emerging against a backdrop of growing trends towards the deliberate spread of false information and declining trust** in institutions and among actors in the international system.
- **As hyper-realistic false, misleading or malicious content, deepfakes have the capacity to intensify the erosion of norms related to truth and trust** at an individual, organizational and societal scale.
- **Deepfakes perpetuate the 'liar's dividend'**—in the era of truth skepticism, the mere fact that deepfakes exist could undermine even what is in fact true or authentic.
- From an international security and stability perspective, **ready access to increasingly sophisticated deepfake technology could lower the barriers to weaponizing information and delivering tailored harm or disruption** in society as well as in the political and military spheres.
- **Many technical countermeasures and policy approaches at industry, national and regional levels are emerging** to respond to the multifaceted risks posed by deepfakes, including media provenance solutions, deepfake detection tools, regulation across the deepfake life cycle, and media literacy.
- **The key question for the international peace and security community is how it could leverage and bolster technical countermeasures and governance approaches** to effectively address the risks presented to international security and stability.