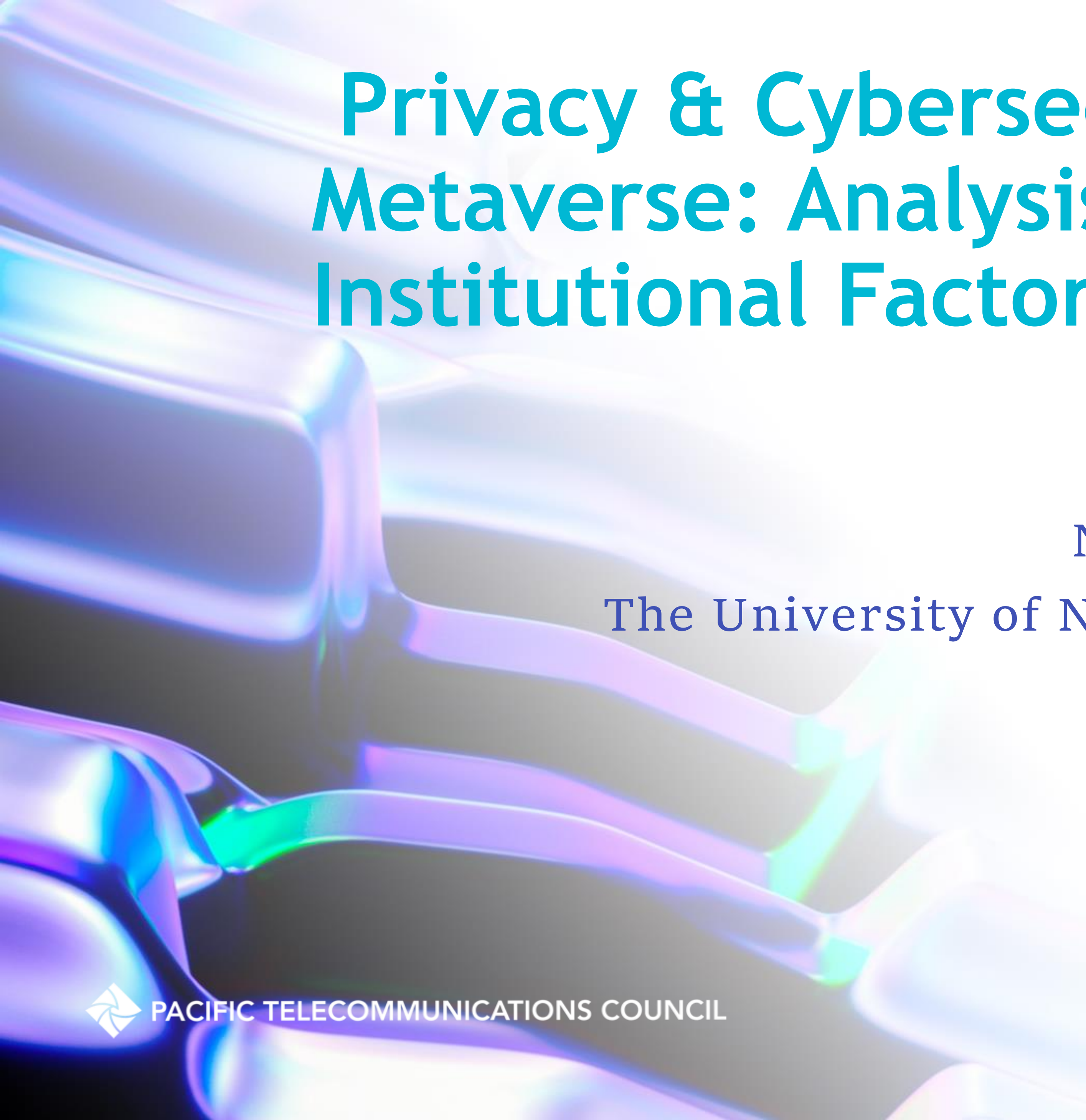

# Privacy & Cybersecurity Issues Facing Metaverse: Analysis of Technological & Institutional Factors

Nir Kshetri

The University of North Carolina at Greensboro, USA

PACIFIC TELECOMMUNICATIONS COUNCIL

PTC'24

21-24 JANUARY 2024 | HONOLULU, HAWAII

@PTCOUNCIL #PTC24

# The metaverse as an attractive cybercrime target

- Metaverse companies:  40% increase bot-driven as well as human-driven attacks during 2021 Q4.
    - Likely to increase as more people join the metaverse and more data are created.
- Serious concerns about data privacy in the metaverse.
    - Multi-sensory experiences: sensitive data such as those related to emotion as well as  biometric, and physiological data.

# Technological and institutional environment affecting nature and extent of threats and effects on victims

| | Nature and extent of threats | Effects on victims |
|---|---|---|
| **Technological environment** | • More and richer data involved: higher incentives to engage in privacy violations and security breaches<br>• Newness and novelty of technologies: cybercriminals' victimization attempts are more likely to be successful<br>• Greater number of and more varied privacy and cybersecurity threats | • More likely to be victimized<br>• More serious harms<br>• Immediate harm |
| **Institutional environment** | • Less developed formal constraining institutions: legitimate as well as illegitimate actors' tendency to engage in privacy violations and security breaches | • Less likely to get legal recourses |

# Technological environment: Data intensiveness

- Credit Suisse: the average data usage worldwide : Up 20 times by 2032.
- 20 minutes of VR use: 2 million unique data elements related to the way the user breathes, walks, thinks, moves or stare (wirewheel.io, 2021).
- New data related to NFTs, cryptocurrency transactions, avatars, experiences and other aspects

# Technological environment: Newness and novelty of technologies involved

- Rare enemy syndrome (Dawkins, 1982; de Jong, 2001).
- The metaverse and AI: perpetrators can effectively deceive and victimize users.
- AI is playing an increasingly important role in Web3 and the metaverse.
- The goal of VR and AR: to fool the senses by making computer-generated content seem like real-world experiences.
- Alan Turing: a human-level AI's ultimate test would be to successfully fool consumers into believing that the AI is human.
  - AI-driven avatars: more and more likely to look, sound, and act like humans,
  - Consumers will not be able to tell the difference between actual people and virtual people.

# Technological environment: Complexity and weak architectural security

- Being built on many advanced technologies
  - Blockchain, VR, AR, AI/ML, NLP, 3D graphics and sensors of various types.
- Many of these technologies have been in use for many years.
  - They are being used together for the first time.
- Different organizations built these technologies: No understanding of the end use
  - Increase the security risk

# Technological environment: Amplified impact on victims

- Multisensory environment.
- Complex and sophisticated features: more graphic, 3D design, immersive visual and auditory experience,
- Unwanted and privacy-invasive content: felt as more intrusive
- Greater negative impact on the users/victims.
- Perpetrators target financial data, crypto-assets, sensitive personal data.
- Privacy violations and security breaches: more severe consequences
- Rare enemy syndrome: poison itself is more deadly + the victims lack  a counter poison for providing protection against and destroying the poison,

# Technological environment: Immediate harms to victims

- Web3 metaverses:  Decentraland, the Sandbox, and Voxels are bult on blockchain.
- Traditional environments: nefarious actors: no clear or immediate monetary benefits.
- Hackers can monetize only a small proportion of stolen bank passwords.
- Most passwords stolen from nonbank institutions are virtually worthless .
- Web3 environment: cybercriminals easily monetize stolen data.
- In blockchain applications, significant value is often encoded directly into the software.

# Institutional environment

- Weak and underdeveloped regulatory environment
  - Avatar’s data processed: how the location is determined?.
- Lack of preparedness at the industry level
- Lack of intra-organizational rules and norms
- Formal constraining institutions governing privacy and security issues in the metaverse are less developed compared to the non-metaverse environment.
- Less developed formal constraining institutions governing privacy and security issues: increase legitimate as well as illegitimate actors' tendency to engage in privacy violations and security breaches in this environment.

# Thank you!

Email: nbkshetr@uncg.edu