The article I chose to review was Victimization by Deepfake in the Metaverse: Building a Practical Management Framework published in the International Journal of Cybersecurity Intelligence & Cybercrime. The articles' primary purpose was to discuss the proliferation of cybervictimization in the metaverse, briefly discuss theories on what may motivate a cyber offender, the use of deepfakes and how they are used to cyber victimize, and to discuss expert opinions on the matter and hypothesize a framework to best mitigate the deepfake cyber victimization in the metaverse. These authors utilized online open-source information, including various other studies on cybercrimes, cyber victimizations, the metaverse, deepfakes, etc., and sampled the opinions of 8 South Korean experts by way of snowball sampling and posing a series of questions. They stated that the primary reason for utilizing South Korean experts was the nations governmental active support for and use of the metaverse. The authors open the article by sharing a psychotherapists account of how she was targeted online in the metaverse, and later discuss how the experts believe that the *primary* targets of cybercrime in the metaverse are expected to include, children, elderly, and women. They even go on to state that in specific relation to deepfakes, women are the primary target of offenders. The majority of the experts state that the motivation for cybercrimes in the metaverse primarily stem from financial or sexual gain, while also commenting on what may motivation these offenders and lack of restrictions inside the metaverse (a lack of self-control). The article also briefly touches on the psychological factors that may play into the offenders, offending by citing Eysenck's theory of criminality, which states that metal illness and other psychological factors play into offending. The theory uses a questionnaire to measure the offender's personality. This theory along with the expert opinions on what may motivate these offenders leads me to believe that it is a more cognitive based theory on cyber offending and in regard to Eysenck's theory, a somewhat deterministic ideal. The article then goes onto discuss the current laws and policies in place to deal with cybercrime in the metaverse, and how they can be added too, changed, and/or improved to better protect people from deepfakes and cybercrime in the metaverse. The authors state that victims must be better supported psychologically because the psychological consequences of deepfakes and cybervictimization can be severe and lasting. They also discuss how metaverse ethics and user protection policies, helplines, Real ID verification, and stronger deepfake identification software must be developed and implemented in order to properly combat deepfake and cyber crime in the metaverse. The article remains objective when discussing the limitations of the study by disclosing the lack of previous knowledge in deepfake mitigations and the small pool of experts utilized.

References

Stavola, J., & Choi, K.-S. (2023). Victimization by Deepfake In the Metaverse: Building a Practical Management Framework. *International Journal of Cybersecurity Intelligence & Cybercrime*, 1-20.