

Hans Peterson

CYSE 201S

3/19/2024

### Journal Entry 10: Social Cybersecurity

Objective: Summarize response to article.

Social cybersecurity, now that the article effectively summarized it, is a crucial, growing, and non-traditional field of cybersecurity. I agree with the author's statements regarding the current "war" on the Internet and other mass media outlets. The information war is an effective and uncostly war that is happening throughout the Internet. There is no need to invade a country if the citizens of that country are revolting, destroying everything from the inside. If those citizens are able to be influenced, they are the cheapest, broadest, and efficient unit any nation can have. They can spread misinformation and disinformation, which can influence many facets of a nation and culture. Considering this article is from 2019, I can see how worse it got.

The article discussed techniques and bots that are used to spread disinformation. They're classic cases of manipulation. On information maneuvers, I've seen misdirection and hashtag latching be used; I've seen grizzly, unrelated images. For the network maneuvers, community building can easily lead to a dangerous echochamber that encourages extremism, which leads to terrorism. This reminds me of an extremist forum I've seen before, Stormfront. I've also seen this on other social media platforms (not to an echochamber extent), where they primarily discuss writing. For some reason, when one controversial guideline/rule when writing is discussed, everyone else decides to accept it and never question it. If a single

guideline/recommendation in writing is upheld without question, I would not be surprised if disinformation is spread and upheld easily.

Overall, the ability to recognize misinformation and disinformation is crucial. Every person must be able to recognize, as they are the targets.