Week 10 Journal Entry 10

Read this and write a journal entry summarizing your response to the article on social cybersecurity

https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/Links to an external site.

In reading through the article, I have some responses to different aspects, and some thoughts that come to mind. The information landscape has been evolving and changing rapidly over the course of the past 30 years. Russia recognized this early on and has used the space to their advantage in attacking other countries, especially the United States. Part of what makes information warfare so potent is that it's not just influencing soldiers like on a traditional battlefield, but that it sows distrust in the general population of a country, against each other, their government, and valuable institutions of society. This basically lays the groundwork for what could potentially become a grander scheme in the future, should such an elaborate plan ever be made. In looking at the information warfare space, the United States varies in many ways when compared to Russia, chiefly where it pertains to freedom and sovereignty. Attacking another countries' people in such a way is beneath the values we hold dear as a nation.

On the flip side, our hand may very well be forced at some point to engage in such warfare. Right now, we're trying to combat the spread of bots on the internet and especially on social media. It's easy to regulate laws for internet operations that happen within the country, and to control certain factors, but not so much outside the country. As AI starts to take on more of an active role in cyberspace, and as its capabilities are expanding and finding new uses, information warfare is certainly going to be among those uses. As it stands, AI models are already being trained to give out good information in a summarized format. The damage that can be done with a malicious AI model, where the AI is trained to give out bad information, could be catastrophic in relation to the damage being done in the information warfare space now.

Given the nature of information warfare, our society needs to be made more aware of methods to identify such misinformation and information warfare, much like how we train people on recognizing phishing attempts. This training can be a valuable tool in combatting information warfare and raise awareness. What such training and methods might look like, I do not know. Perhaps one indicator may involve the reliability of the source or the weblinks involved. Much of the bad information flowing through social media now points to external links with longer articles.