JOURNAL ENTRY 11

The article by (Beskow & Carley, 2019) emphasizes the need to understand manipulative social factors and network science that influences human behavior in cyberspace. Information has always been a crucial commodity, and it is the most important currency especially in an age where there is so much data and information circulating. The article highlights the growing importance and threats of cybersecurity. With the decentralization of information distribution, the responsibility of authentication and fact-checking falls on the receiver. The ease spread now gives the opportunity for malicious parties to sow discord and misinform indiscriminately.

This article focuses on the military use of information, particularly how state and non-state actors utilize it to misinform and sow discord. It emphasizes the importance of information quality, distribution speed, and their impacts on modern warfare strategies . Unlike in World war I or II, where spies had to be sent into enemy territory to either gather information or cause confusion among allies, today's decentralized information has made it easier and more concentrated. Misinformation can now happen on a personal, community-wide, or national level, turning individuals against a friend, subordinate against leader, or citizens against their government. This poses significant challenges. The article makes it clear that the US military should take a more active role in preventing this, not only to protect camps and bases but the nation as a whole from external manipulation. A divided nation is easy for outside actors to infiltrate, cause problems, or invade and destroy. It is believed that the best way to take down a nation is to initiate a civil war and turn the people against the government, a strategy that the US cannot permit, hence the need for a better security system.

Taking it out of a military context, the use of social media, and the introduction of bots, and social engineering hacking have made information gathering and sharing a rather tortuous undertaking. With so much information, especially in the media, there is a ton of wrong information. The introduction of bots worsens this by having non-human sources pass on wrong information. Social engineering exploits people's weaknesses using skills from many disciplines. This all ties into the need for a better security system, with the military at its center, but also building awareness among users (the populace) for better protection.

The threat of misinformation and misuse of information is very real and important to note. Keeping that in mind, all individuals should be taught to properly fact-check the information they receive from centralized, accountable sources before spreading or using it can help mitigate the threat of misinformation. This awareness will promote military and national security.

I fully agree with the authors of the article that information distribution is a sensitive subject and therefore should be given a closer look. All parties involved with receiving and sharing information should be sure of its credibility and authenticity so as to avoid discord or confusion. Therein comes the proactive step to information control but believe it should be on all levels.

References

Eddins, J. (n.d.). *Social Cybersecurity An Emerging National Security Requirement*. Army University Press. Retrieved July 11, 2024, from https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/