James Applegate

3/27/24

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

This article, tailored for national security professionals, policymakers, and individuals interested in cybersecurity and modern warfare, provides a comprehensive overview of social cybersecurity's emergence as a critical component of national security, particularly in contemporary warfare. It delves into how technology empowers state and non-state actors to manipulate information and sway societies, yielding significant strategic implications. The term "social cybersecurity" is defined within the article as a discipline focused on grasping and predicting cyber-mediated shifts in human behavior, social outcomes, and political landscapes, with a specific aim of safeguarding society in a cyber-mediated information environment.

Key takeaways from the article include:

1. Information Warfare's Strategic Importance: Information warfare is increasingly recognized as a primary strategy to shape beliefs, ideologies, and societal values. It involves reinforcing one's narratives while undermining opposing viewpoints and eroding trust in institutions and national values.

2. Information as a Key Element of National Power: Information has become a pivotal aspect of national power, akin to diplomatic, military, and economic elements. Advancements in technology enable actors to extend their influence in the information domain, with strategic implications comparable to physical warfare.

3. Distinguishing Social Cybersecurity from Traditional Cybersecurity: Social cybersecurity focuses on using technology to influence human behavior and societal structures, contrasting with traditional cybersecurity's focus on protecting information systems. This includes tactics such as cognitive hacking, targeted marketing, and leveraging insights from psychology and social sciences for coordinated information operations.

4. Russian Influence Operations: The article highlights Russia's historical and ongoing utilization of information warfare, showcasing tactics like active measures and strategies aimed at sowing discord within societies for strategic advantage.

5. Forms of Maneuver in Social-Cyber Domain: Various forms of maneuver are discussed, including manipulating information flow (information maneuver) and social networks (network maneuver) to achieve desired outcomes.

6. Role of Bots in Information Operations: Bots, particularly in social media, serve as force multipliers by leveraging machine learning and automation to conduct large-scale information transactions. They often operate in tandem with human operators, amplifying the impact of information operations.

7. Addressing Challenges and Solutions: The article acknowledges challenges such as decentralized information flow and the vulnerability of open societies to manipulation. It emphasizes the necessity for agile policies and educational initiatives to tackle social cybersecurity threats effectively.

Overall, the article underscores the criticality of comprehending and mitigating social cybersecurity threats within modern warfare and national security, highlighting the evolving landscape where information plays a pivotal role in shaping geopolitical dynamics.

Beskow, D. M., & Carley, K. M. (2019, March). Social Cybersecurity an emerging national security requirement. Army University Press. <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/>