Owin Ifill

Professor Diwakar Yalpi

Cybersecurity Social Science

24, November 2024

Social Science in Cybersecurity Careers for FBI and Military

Introduction

For my career paper I decided to pick two career paths. The FBI and the Military are very similar because they deal with safeguarding national security and public safety. Working these roles require technical expertise in area such as threat analysis, network protection, and counterintelligence. But they also depend heavily on principles of social science to understand human behavior, culture dynamics, and societal impacts of their work. Social science research offers insight into marginalized groups, human decision-making, and societal vulnerabilities, which are essential for professionals tasked with protecting the digital assets and ensuring ethical practices as well.

Behavioral Insights for Cybersecurity Training

Understanding human behavior is a cornerstone of effective cybersecurity. Attackers frequently exploit cognitive biases and emotional vulnerabilities through techniques such as phishing and social engineering. FBI cybersecurity professionals, as Powers and Burns (2019) highlight, use social science research to anticipate how individuals may respond to threats and to design interventions that strengthen user awareness and resilience. Behavioral insights also

inform military training programs, equipping personnel to recognize and counter manipulation in operational environments.

Cyber Leadership and Cultural Sensitivity

In their examination of cybersecurity education at U.S. service academies, Spidalieri and McArdle (2016) emphasize the importance of cultural awareness and leadership skills for military cyber professionals. Social science principles help these leaders understand diverse cultural norms and communication styles, which are crucial when working with international partners or addressing global cyber threats. For instance, understanding the cultural context of an adversary's actions can improve decision-making and reduce the risk of misinterpretation during conflict or negotiation.

Societal Trends and Marginalized Groups

Cybersecurity professionals must address societal inequities that worsen vulnerabilities. Dawson and Thomson (2018) showcase the need for cybersecurity workers to move beyond technical expertise and embrace a holistic approach that considers the societal impacts of their actions. For example, marginalized groups often lack access to cybersecurity resources, making them prime targets for exploitation. FBI and military professionals informed by social science can identify and mitigate these disparities by tailoring outreach and education programs to at-risk populations.

Effective Communication and Collaboration

Cybersecurity roles in the FBI and military require extensive collaboration across agencies, industries, and international partners. Social science principles enhance communication by translating technical findings into actionable strategies. Powers and Burns (2019) argue that partnerships between academia, government, and industry benefit from professionals who can effectively bridge these sectors using clear and inclusive communication.

Fostering Ethical Practices

The integration of ethics, a key area of social science, ensures that cybersecurity operations respect privacy and human rights. Spidalieri and McArdle (2016) note that ethical considerations are central to military cyber leadership, particularly in balancing security objectives with legal constraints. For FBI professionals, ethical practices are equally vital when conducting surveillance or handling sensitive data, fostering public trust in their operations.

Preparing for the Future Workforce

As cyber threats evolve, so must the workforce. Dawson and Thomson (2018) highlight the need for cybersecurity professionals to develop critical thinking, emotional intelligence, and adaptability—skills rooted in social science research. These attributes not only enhance individual performance but also ensure that the field remains inclusive and representative of the broader population.

Conclusion

Social science principles are indispensable to cybersecurity careers in the FBI and military, providing the tools to understand human behavior, navigate cultural dynamics, and address ethical challenges. By integrating social science research, these professionals are better equipped to protect society while fostering equity and trust. From training the next generation of cyber leaders to addressing the vulnerabilities of marginalized groups, the intersection of social science and cybersecurity strengthens both national security and societal well-being. As threats grow more sophisticated, the role of social science in cybersecurity will only become more critical.

References

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology, 9*, 744.

Powers, K., & Burns, J. (2019). The FBI, cybersecurity, and American campuses: Academia, government, and industry as allies in cybersecurity effectiveness. In *The Routledge International Handbook of Universities, Security and Intelligence Studies* (pp. 94-107). Routledge.

Spidalieri, F., & McArdle, J. (2016). Transforming the next generation of military leaders into cyber-strategic leaders: The role of cybersecurity education in US service academies. *The Cyber Defense Review, 1*(1), 141-164.