Daniel Monbrod

Dr. VanDerMoere

ENG-102-W06

28 February 2025

The Paradox of Protection: Unpacking Cybersecurity Expertise

In the continuously evolving world of cybersecurity, defining an "expert" requires more than just a surface-level assessment of technical skills. While technical expertise is undeniably vital, the complexity and interdisciplinarity of the field necessitate a more nuanced understanding of what it means to be an expert. This essay argues that a true expert in cybersecurity is a composite figure: technically proficient, ethically grounded, philosophically aware, and existentially courageous. The discourse that defines and validates expertise in this domain is explained in academic journals such as "*Information and Computer Security*," "*Frontiers in Psychology*," "*Journal of Cybersecurity*," and "*Computers & Society*."

The first crucial characteristic that separates an expert from a mere practitioner in cybersecurity is an unwavering commitment to empirical research. Academic journals like "*Information and Computer Security*" have articles that apply rigorous scientific methodologies to tackle intricate cybersecurity challenges. For example, Haney and Lutters' paper discusses the evolving roles and required skill sets in cybersecurity, emphasizing the importance of diverse skills and evidence-based approaches. Such methodological rigor is also resonant with Karl Popper's philosophical principle of falsifiability, which emphasizes the importance of empirical validation. In Popper's view, a hypothesis gains validity not only by withstanding tests that seek to falsify it but also by providing actionable insights that can be universally applied. Hence, experts in the cybersecurity field are those who can develop, evaluate, and validate theories about information security, adding to the collective knowledge of the community and effectively enhancing the security of digital landscapes.

Ethical consideration serves as a crucial element in defining expertise within cybersecurity. A paper by Dawson and Thomas in the journal "*Frontiers in Psychology*" suggests that a comprehensive understanding of cybersecurity transcends mere technical knowledge, requiring a solid ethical foundation. The stance that ethical responsibility is integral to being a cybersecurity expert aligns seamlessly with longstanding societal and ethical principles. One notable example is Immanuel Kant's Categorical Imperative, a widely accepted ethical guideline that posits an action is morally acceptable only if it can be universally applied. This universal ethical principle reinforces the argument that ethical considerations are not merely an add-on in cybersecurity; they are foundational. Therefore, a cybersecurity expert is more than someone proficient in technical skills. They can also make ethically sound decisions that stand up to scrutiny from both a technical and moral standpoint. An expert protects digital assets and upholds broader social values such as human rights and privacy.

Another layer of expertise is the expert's interdisciplinary approach to problem-solving. Journals like "*Computers & Society*" often publish articles that explore the interconnections between technology, ethics, and society. Hermeneutics, or the theory of interpretation, is an asset for cybersecurity advocates. It equips them with the tools to understand the differences between block ciphers and cryptographic algorithms and the social, cultural, and psychological factors influencing human interaction with technology – information philosophy. For example, an article in "*Computers & Society*" might explore how cultural attitudes towards privacy impact cybersecurity practices.

Interdisciplinary knowledge is essential for cybersecurity experts because their challenges are technical, ethical, and societal. An expert knowledgeable in disciplines such as sociology, psychology, and even philosophy is merely a foundation to be set and ready to anticipate their actions' broader implications, adding depth to their expertise.

The notion of existential courage as an underpinning of expertise adds a more humane touch to our understanding of a cybersecurity savant. Articles in journals like "*Journal of Cybersecurity Education, Research, and Practice*" often emphasize the importance of mentorship, leadership, and cultivating a growth mindset. These traits resonate with existentialist principles like the existential courage concept, which emphasizes the importance of authentic action despite uncertainty and risk. A true expert not only masters the extant body of knowledge but is also courageous enough to venture into the unknown, willing to take risks for the greater good, and capable of mentoring the next generation of cybersecurity professionals.

Integrating these multi-layered criteria—academic rigor, ethical grounding, interdisciplinary awareness, and existential courage—provides a complete understanding of what it means to be a true expert in cybersecurity. Such experts are not just repositories of technical knowledge; they are leaders whose influence reverberates through various dimensions of cybersecurity, including its ethical and societal implications. A true expert appreciates that the domain is not static but ever evolving, demanding an agile mindset, open to learning, and committed to growth.

To validate this integrated notion of expertise, looking at the types of articles published in high-impact journals is essential. For instance, "*CyberGenomics: Application of Behavioral Genetics in Cybersecurity*," published in "*Behavioral Sciences*" demonstrates an innovative blend of genetics, behavior studies, and cybersecurity. This amalgamation of various disciplines into cybersecurity research epitomizes the expertise increasingly regarded in the field.

Likewise, those who publish their work in these journals also matter. Typically, those who contribute unique insights, challenge the status quo, and expand the field's intellectual boundaries get their work published. For example, articles like Seshadri's "W*hat Makes a Good Cybersecurity Professional*?” at ISACA are breaking new ground by discussing soft skills and psychological traits that are not often addressed but are highly valued in the field. These authors employ rhetorical, stylistic, and content choices to establish their expertise, often using a combination of case studies, empirical data, and theoretical frameworks to support their arguments.

In summary, a true expert in cybersecurity is a multi-faceted individual who transcends technical proficiency to encompass ethical fortitude, interdisciplinary understanding, and existential courage. The articles published in leading journals exemplify this integrated form of expertise, crucial for tackling the multi-dimensional challenges that define the modern digital landscape. As cybersecurity continues to evolve, the criteria for expertise will undoubtedly expand and diversify, requiring ongoing discourse and reevaluation. However, for now, these multi-layered criteria provide a robust framework for understanding and identifying true experts in cybersecurity. These individuals are well-equipped to navigate the technical and ethical aspects that define our digital world.

Works Cited

Dawson, Jessica, and Robert Thomas. "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance." Frontiers in Psychology, vol. 9, 2018, https://doi.org/10.3389/fpsyg.2018.00744.

Domarkienė, Ingrida, et al. “CyberGenomics: Application of Behavioral Genetics in Cybersecurity.” Behavioral Sciences, vol. 11, no. 11, Nov. 2021, p. 152, EBSCOhost, https://doi.org/10.3390/bs11110152.

Haney, Julie M., and Wayne G. Lutters. “Cybersecurity Advocates: Discovering the Characteristics and Skills of an Emergent Role.” Information and Computer Security, vol. 29, no. 3, 2021, doi:10.1108/ics-08-2020-0131.

Payne, Brian K., et al. “Journal of Cybersecurity Education, Research and Practice.” Journal of Cybersecurity Education Research and Practice, vol. 2021, no. 2, 2021, digitalcommons.kennesaw.edu/jcerp/vol2021/iss2/.

Seshadri, Deepa. "What Makes a Good Cybersecurity Professional?" ISACA, 15 Nov. 2022, www.isaca.org/resources/news-and-trends/industry-news/2022/what-makes-a-good-cybersecurity-professional. Accessed 15 Sept. 2023.