A Journey Through College

Jessiah Davis

IDS 493

Dr. Phan

May 1, 2026

Abstract

This reflection goes through three fundamental abilities I developed while attending Old Dominion University—leadership, teamwork, and the capacity to collaborate with AI and data-driven cybersecurity systems—this reflection examines my academic and personal growth. I have developed a deeper comprehension of the intersections between technical systems, human behavior, and ethical decision-making through education in philosophy, cybersecurity labs, and multidisciplinary research. My artifacts, which include studies on attention span and system vulnerabilities, philosophical case analyses, and cyber defense labs, show how I have progressed from merely doing assignments to actively studying issues and coming to well-organized, fact-based conclusions. This essay considers those encounters and how they influenced my preparedness for future graduate work and a career in cybersecurity.

Introduction: I have gained a deeper grasp of cybersecurity throughout my time at Old Dominion University, not only as a technical field but also as an interdisciplinary area influenced by human behavior, ethics, and quickly developing technology. As a senior who will graduate in the fall of 2026, I've seen that success in my area demands more than simply technical proficiency—it also calls for the capacity for critical thought, cross-disciplinary collaboration, and adaptation to cutting-edge technology like artificial intelligence. The three abilities that most accurately reflect my development are teamwork, leadership, and my capacity to collaborate with AI and data-driven systems in cybersecurity settings. A combination of practical labs, philosophical case studies, and research-based writing tasks helped to improve these abilities. All of these experiences show how I've evolved from a student who was only concerned with finishing assignments to someone who can evaluate challenging challenges, make connections

between concepts from other fields, and apply structured reasoning to cybersecurity-related real-world problems.

Leadership Development Through Ethical and Technical Decision-Making. My cybersecurity coursework and philosophical case analyses best demonstrate my growth as a leader. I was constantly pushed in my PHIL 355E class to develop systematic arguments based on opposing ethical frameworks rather than relying solely on my own ideas. This necessitated writing and thought discipline, particularly when examining intricate subjects like information warfare, technological deceit, and military whistleblowing. I looked at how digital platforms are used to affect political processes and public opinion in my case study on information warfare. I learned to assess these behaviors using ethical frameworks that prioritized community, accountability, and moral consequence rather than responding to them emotionally. This made it easier for me to see leadership as the capacity to make logical decisions in circumstances where there are no simple answers. Another case study examined professional accountability and misleading software design. I discovered in that assignment how simple it is to employ technology to sway user behavior in an opaque manner. I learned how to assess responsibility at both the individual and organizational levels while writing that report. In this way, leadership became about spotting moral weaknesses and figuring out who is accountable when mechanisms are abused. My cybersecurity curriculum reinforced these experiences, particularly in lab-based settings where making decisions under duress was necessary. I discovered that cybersecurity leadership frequently entails making prompt, well-informed judgments while being aware of the possible repercussions of those decisions, whether analyzing network traffic or spotting vulnerabilities.

My growth through Multiple Facets. My integrative academic work and cybersecurity labs both demonstrate my improvement in teamwork. I worked through virtual machine laboratories that replicated real-world network environments over long nights in CYSE 301. In order to fix systems that did not always respond as expected, these labs required perseverance, problem-solving skills, and a methodical approach. Working with tools like Wireshark and pfSense in network protection scenarios was one of the most influential experiences. These exercises taught me how to keep an eye on traffic, spot suspicious activity, and set up firewall rules to prevent unwanted access to computers. I finished these labs alone, but because they involved collaboration across several systems, tools, and conceptual frameworks, the approach was similar to real-world cybersecurity teamwork. It taught me how collaboration in cybersecurity is not always about people working together directly, but also about systems working together effectively. My IDS 300W research report on diminishing attention spans also reaffirmed the value of interdisciplinary cooperation. In order to comprehend how short-form digital information impacts cognitive focus, that assignment needed me to mix psychology, neuroscience, media studies, and education. It took a lot of effort and was frequently difficult to find reliable sources for that paper, but it forced me to go beyond cursory research. I had to learn how to combine concepts from several domains into a single, cohesive argument rather than depending just on brief citations to satisfy criteria. As a result of this approach, I started to see cooperation as more than just teamwork; it now involves integrating expertise from several fields to address challenging issues.

Working Alongside AI and Cybersecurity Systems. Through both technical training and study into contemporary digital risks, I was able to work with AI and automated systems in cybersecurity. I examined assaults on Microsoft systems, such as malware campaigns, Windows

service vulnerabilities, and advanced persistent threats that target enterprise infrastructure, for my CYSE 280 research report. This task made it easier for me to see how automation, massive data analysis, and AI-powered protection systems are progressively influencing modern cybersecurity. The fact that both attackers and defenders depend on more sophisticated technologies was what most struck me. To find vulnerabilities, take advantage of them, and stay persistent in networks, attackers employ automated tools. In order to identify anomalous activity and take immediate action, defenders simultaneously rely on threat intelligence platforms and AI-driven monitoring systems. I came to the realization that working in cybersecurity nowadays requires knowing how to work in tandem with AI systems rather than apart from them as a result of this duality. This theme also relates to my examination of information warfare in PHIL 355E, where I looked at how algorithmic systems and digital platforms can affect public opinion. My understanding of how AI and algorithms actively affect behavior, attention, and decision-making on a broad scale has improved as a result of that assignment. By relating this to cybersecurity, it became evident that future professionals need to be able to critically analyze, assess, and react to AI-driven environments.

Interdisciplinary Growth and Personal Development. Learning to think across disciplines has been one of the most significant parts of my academic path. Early in my academic career, I frequently tackled assignments with the intention of finishing them quickly and receiving credit. As I came across increasingly complicated tasks that needed more in-depth analysis and drawn-out research procedures, my perspective gradually changed. One of the most difficult aspects of my academic growth was locating reliable sources for my research papers, particularly in IDS 300W. It took time, perseverance, and constant search strategy improvement. Over time, I discovered that comprehending and applying sources effectively is more important

for producing quality academic work than simply gathering them fast. This change made it easier for me to use research to develop my own understanding rather than depending on citations to fulfill criteria which I am ashamed to admit I used to do a lot of. In CYSE 301, the technical challenges of lab work pushed me in a different way. Working late nights to complete virtual machine exercises taught me persistence and problem-solving under pressure. There were moments of frustration when systems did not behave as expected, but those moments forced me to slow down, think critically, and try different approaches until I succeeded. Over time, I became more confident in my ability to troubleshoot and adapt. Together, these experiences helped me develop a more disciplined and intentional approach to learning. I began to see myself not just as a student completing assignments, but as someone actively building the skills needed for a professional career in cybersecurity.

To wrap it all up, When I reflect upon my academic career, I can clearly identify improvements in my capacity for collaboration, leadership, and interaction with AI-driven cybersecurity systems. Every item in my portfolio represents a distinct phase of my evolution, from research projects that enhanced my capacity to assimilate complicated material to technical labs that developed my cybersecurity abilities to philosophical case analyses that reinforced my ethical reasoning. Even while the journey hasn't always been simple, particularly when it comes to difficult lab work and demanding research assignments, those difficulties have been crucial in molding my growth. They helped me learn perseverance, flexibility, and the value of viewing issues from several angles. I feel more equipped to go deeper into the area as I work toward earning my degree and pursue doctoral studies in cybersecurity. In the long run, this portfolio is more than just academic work; it shows the process of developing into a more competent,

perceptive, and diverse thinker prepared to contribute to the rapidly changing field of cybersecurity.

References

arnett, jeffrey. (2019, January). *(PDF) Emerging Adulthood: The Winding Road from the Late Teens Through the Twenties (2nd edition)*. ResearchGate. https://www.researchgate.net/publication/330369978_Emerging_Adulthood_The_Winding_Road_from_the_Late_Teens_Through_the_Twenties_2nd_edition

Hongladarom, S. (2020). Shoshana zuboff, the age of surveillance capitalism: The fight for a human future at the new frontier of power. *AI & SOCIETY*, *38*(6). https://doi.org/10.1007/s00146-020-01100-0

Sorin Adam Matei. (2013, March). *The Shallows: What the Internet Is Doing to Our Brains, by Nicholas Carr. New York, NY: W. W. Norton,...* ResearchGate; Taylor & Francis. https://www.researchgate.net/publication/262245164_The_Shallows_What_the_Internet_Is_Doing_to_Our_Brains_by_Nicholas_Carr_New_York_NY_W_W_Norton_2010_276_pp_2695_ISBN_0393072223_hardcover

Wardle, C., & Derakhshan, H. (2017). *Information Disorder: toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Yeager, D. S., & Dweck, C. S. (2012). Mindsets that promote resilience: When students believe that personal characteristics can be developed. *Educational Psychologist*, *47*(4), 302–314. https://doi.org/10.1080/00461520.2012.722805