My Self-Assessment

Joshua Morton

Old Dominion University

IDS 493 - Electronic Portfolio Project

Dr. LaFever

December 3, 2025

Introduction:

For as long as I can remember I have always been fascinated by computers and technology. Growing up I was always known as the “computer guy” fixing PC desktops and setting up the internet every time we moved. When starting my time at Old Dominion University I naturally gravitated to the cybersecurity program, and eventually minored in political science. Participating in coursework and building my portfolio as a cybersecurity major with a minor in Political Science has given me the opportunity to reflect on how my academic path has shaped my identity as an interdisciplinary learner and emerging professional. Cybersecurity is a field defined by technical complexity and understanding human behavior. Political Science, which is far from being separate in my opinion, helped to deepen my understanding of how governments create laws around cyber crime and technology. To help characterize the relationship of the two disciplines I have worked on academically I included works that ranged from hands-on technical labs, programming assignments, and ethical hacking projects to research based writing and moral and political reflections. This reflection and portfolio does more than show what I know technically; it also reveals how I think and integrate knowledge from multiple fields. Interdisciplinary experts argue that such integration builds “epistemic agility,” an ability that allows individuals to address complex problems that don’t fit into one discipline. (Repko & Szostak, 2021) Moving through college I have truly understood the natural progression and importance of having such “epistemic agility” especially as a student pursuing a major and minor of separate disciplines. I believe that this essay reflects my journey through college, analyzing what each artifact represents in my personal skillset growth and how my academic experiences have prepared me for an interdisciplinary cybersecurity career.

Skill 1: Technical Experience Through Hands on Learning

One of the clearest examples of my growth throughout my time at Old Dominion University is that of the progress of my technical abilities. I believe that my time working through my cybersecurity classes have shaped my confidence in certain fields, such as the python programming language, the many computer operating systems, and cybersecurity tools, to the point at which I am confident I could hold my own in a cybersecurity work environment. Much of my time working through my more technical cybersecurity courses was spent experimenting, breaking down, and fixing technical devices. At times I felt it was frustrating but looking back I believe that these struggles were where I grew the most.

Skill 1: Ethical Hacking and Network Security Lab

My first artifact is of my process of ethically hacking into Windows 7 and XP through MetaSploit. This assignment required me to understand the intricacies of Windows and how to exploit them. I also learned and understood the ethical ramifications of hacking offensively and exploiting vulnerabilities. I found this assignment to be one of the most challenging, and rewarding, parts of my coursework. I remember when running the labs for the first time I had expected perfect outcomes but got errors a majority of the time. At first many of the labs left me feeling overwhelmed, but gradually through peer help and studying I learned how to diagnose problems by slowing down, really intricately checking the process, and putting myself in the mind of both an analyst and attacker. These labs definitely taught me the importance of persistence and patience especially when tools didn't work the way I wanted them to. As Dr. Erdal Ozkaya describes in *Cybersecurity: The Beginner's Guide,* hands-on practice is the bridge between simple understanding and real capability and as such running through real hacking scenarios bolstered my understanding to a level that dwarfs what I had known previously.

(Ozkaya, 2019) Those moments of confusion turned into confidence and they helped me appreciate how cybersecurity requires not just technical skill but an interpersonal understanding of attackers and defenders to solve attack problems.

Skill 1: Python Programming Project

Another technical project I completed in my coursework was for CYSE 250 - Basic Cybersecurity Programming and Networking and was a project putting together a basic program that highlights the concept of socket programming. For this project I had decided to create a choose your own adventure game in which a client connects to a server and sends their choices to walk through a written adventure created by me. I still believe that this programming project has been the most fun I've had doing an assignment as it helped move me towards combining my love of narrative writing and programming. Much of the project involved hours of trial and error involving setting up a network connection and server. These pushed me to understand how data moves across systems and what happens beneath the digital surface. The project also required me to combine my love of programming with my passion for writing in that I had to create an actual narrative for the project. As stated in chapter 6 of *Hack the Cybersecurity Interview* programming, math, and analytical thinking, all characteristics I had to exemplify in the project, creates the foundation for more specialized cybersecurity paths, particularly in cybersecurity engineering. (Foulon et al., 2024)

Skill 2: Writing and Communicating

Communication is not something I expected to be so central to cybersecurity, but as I moved through coursework, I learned how important communication is to a cybersecurity professional. Being able to explain how and why complex threats happen or speaking on the ethics of cybersecurity is a core part of a professional's job. Much of my coursework that wasn't practical required writing, and these assignments helped me discover my voice as someone who can translate technical concepts into understandable terms.

Skill 2: Navigating the Dangerous Waters of Phishing Attacks within Microsoft Programs

In my paper "Navigating the Dangerous Waters of Phishing Attacks within Microsoft Programs" I researched and described the still relevant efficiency of social engineering as a concept to exploitation, and how it persists despite technological advancement. Writing this paper required me to dig not only into technical elements of phishing emails but also the psychological ones, why people fall for scams and how attackers manipulate emotions to make users vulnerable. Admittedly I struggled with balancing technical terminology with language that was accessible but eventually I pulled through. There was a feeling I had in which I wanted to be accurate but not overwhelming, and I believe through my coursework I learned to balance writing with technical knowledge into something that was easy to understand. The FBI's report on Cybersecurity and American campuses emphasized the phenomenon I discussed within the essay, the human side of technical risk.(Powers & Burns, 2017) Writing the paper helped me understand how cybersecurity professionals can serve as communicative educators, not just technicians.

Skill 2: Securing Tomorrow: Navigating the Security Challenges of Emerging and Future Technologies

The other paper I included in the portfolio, "Securing Tomorrow: Navigating the Security Challenges of Emerging and Future Technologies," was an assignment that required me to analyze the cyber war climate as emerging technologies like AI and cryptocurrency. With this project I started down the path of really appreciating the study of political science as it relates to cybersecurity. Writing on cyber war was extremely interesting as it forced me to look at multiple factors and explore more than two disciplines to answer the question. It required me to draw not just cybersecurity knowledge but also political science concepts about governance, societal risk, and institutional responsibility to threats. The integration of political science and cybersecurity to answer my questions pertaining to my research aligns with the principles outlined in the *Routledge Handbook of Interdisciplinary Research Methods:* real world problems often require blending technical and social science analysis. (Fensham et. al, 2018) I recall this essay having a learning effect in my ability to synthesize research and communicate complex ideas in a persuasive way.

Skill 3: Leadership

Beyond technical, writing, and ethical skills, I believe it important to highlight my personal experience with leadership and self-assessment and how that has contributed to my growth as a student and a cybersecurity professional. In my portfolio I include two reflection essays I was told to write for CPD 494 - Entrepreneurship Studies and IDS 493 - E-portfolio project. In these essays I highlighted my continued knowledge of leadership and gave examples of my time in AFJROTC and leading by example throughout my life. To supplement the experiences explained in these essays I also added photos of my time leading cadets in the program as evidence of my leadership. In real cybersecurity work interpersonal and leadership skills are just as important as technical ability. I intend to move into the cryptography field of cybersecurity and as evidenced in chapter 6 of *Hack the Cybersecurity Interview* cryptography jobs usually require teamwork, communication, and time management among key soft skills and I believe my experience with leadership bolsters my ability to be successful in cryptography.

Why Consider Ethics in Cybersecurity?

One of the distinct pieces of experience I found outside of cybersecurity and primarily in my minor of political science was the importance of ethics and philosophy. I've come to realize that these two concepts are supremely important to understand on their own but also in the context of political science **and** cybersecurity. I chose to highlight a research paper I wrote for my World Religions class earlier in my time at ODU as an example. In this paper I presented multiple perspectives regarding the use of violence in Buddhist societies and attempted to explain the philosophical reasons for each.

In cybersecurity, decisions often involve tradeoffs: privacy vs. security, surveillance vs autonomy, convenience vs. protection. I credit my political science knowledge in teaching me to question power structures and the social impact of technological decisions. Writing on morality helped sharpen my ethical reasoning skills when contextualizing harm and intention within cybersecurity defensive measures. Whether deciding on monitoring policies or designing encryption protocols, I believe cybersecurity professionals must weigh technical effectiveness against ethical responsibility and respect for user rights. I have found that the intersection of technology, people, and governance is where cybersecurity truly lives. My inclusion of my research paper demonstrates my ideals of not just being someone who can code or hack but someone who can think deeply about what security means for individuals and society at large.

Interdisciplinary Thinking and I?

One of the most important lessons I realized my time at ODU gave me was that of how impactful interdisciplinary thinking is when approaching problems. Over time, I discovered that my thinking shifted: I stopped viewing technical problems as purely technical, or political problems as purely theoretical. Instead, I began to see them as interwoven challenges requiring multiple perspectives. That shift is at the core of interdisciplinary learning in my opinion.

According to Repko and Szostak, interdisciplinary research involves stepping through stages of problem definition, disciplinary framing, integration, and reflecting. I believe that through my artifacts this phenomenon is clear. (Repko & Szostak, 2021) Professionals must adapt, weigh trade offs and anticipate both technical and human factors. The interdisciplinary approach I created makes me more adaptable, thoughtful, and capable of contributing meaningfully in a professional context.

Conclusion

Writing and reflecting on my e-portfolio has shown me how much I've grown professionally, not just in knowledge, but also in perspective. This journey hasn't always been comfortable as I've struggled previously with technical confusion and stress but I believed that these moments taught me the most. Academic hardships have shaped me into a student capable of persistence and adaptation: qualities I expect to carry into my professional life. As I move toward graduation and begin seeking professional opportunities, I feel confident in my ability to tackle complex challenges. I'm not just prepared to code but also communicate and act responsibly. This portfolio is more than a record of my past, it's more like a map of who I have become and who I aim to become: a cybersecurity professional.

References:

Foulon, C., Underhill, K., & Hopkins, T. (2024). *Hack the Cybersecurity Interview: Navigate Cybersecurity Interviews with Confidence, from Entry-Level to Expert Roles* (2nd ed.). Packt Publishing, Limited.

Lury, C., Fensham, R., Heller-Nicholas, A., Lammes, S., Last, A., Michael, M., & Uprichard, E. (2018). *Routledge Handbook of Interdisciplinary Research Methods* (C. Lury, S. Lammes, E. Uprichard, R. Fensham, A. Heller-Nicholas, A. Last, & M. Michael, Eds.; 1st ed.). Routledge. https://doi.org/10.4324/9781315714523

Ozkaya, E. (2019). *Cybersecurity : the beginner's guide : a comprehensive guide to getting started in cybersecurity*. Packt.

Repko, A. F., & Szostak, R. (2021). *Interdisciplinary research: Process and theory* (3rd ed.). SAGE Publications.

Powers, K., & Burns, J. (2020). The FBI, cybersecurity, and American campuses: Academia, government, and industry as allies in cybersecurity effectiveness. In L. F. Gearon (Ed.), The Routledge International Handbook of Universities, Security and Intelligence Studies (1st ed., pp. 94–107). Routledge. https://doi.org/10.4324/9780203702086-4