Reflection Essay

Nathan Mack

Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Gordon-Phan

April 25, 2025

Abstract

This reflection essay examines my educational journey at Old Dominion University as a cybersecurity major, identifying how interdisciplinary learning contributed to my technical expertise, global perspective, and career preparedness. Through an analysis of artifacts from my portfolio, such as programming assignments, research reports, a business plan, and a public speaking video, I illustrate how my studies in law, philosophy, and communications complemented technical studies. Essential experiences, including the development of a machine learning framework for digit recognition and coursework on cyber law, compelled me to critically and ethically consider the implications of technology. While I have yet to attain a cybersecurity position, experience working as a pharmacy technician refined transferable abilities such as detail, communications, and stress management. This essay also considers how research and writing broadened knowledge regarding cybersecurity's social, legal, and philosophical implications. The outcome is a holistic education that equips me for future roles within cybersecurity, especially that of a security analyst or government position.

Introduction

When I first started out as a cybersecurity student at Old Dominion University, I knew only vaguely what the career entailed: safeguarding systems, blocking breaches, and perhaps one day working for the government. But what I did not expect was the breadth and interdisciplinary nature of the experience. From neural networks coded up in Python to public speaking arguments crafted to sway an audience, all of the classes and projects influenced not only technical skills but also critical thinking, communications, and ethics. This reflection examines the major artifacts from the academic portfolio, the skills they reflect, and how the experiences during and between classes prepared one for a future career in cybersecurity.

Programming and Problem-Solving

One of my most characteristic areas of learning was from technical classes such as "Problem Solving and Programming II." There, I perfected the skill of coding clean and effective code using challenging logic problems in C++. One product that demonstrates this is a console application made using C++ for a course assignment. Not only did it demonstrate that I can utilize data structures and control flow, but also that I can apply user-centered design, ensuring that the program was user-friendly.

Later, I would come to use these fundamental skills in more complex contexts, such as constructing a PyTorch digit recognition deep neural network for my CS467 class, “Intro to Reverse Engineering." The task pushed me outside of my comfort zone, requiring me to debug malfunctioning model weights, tweak activation functions, and rethink image data preprocessor design. My model's accuracy plummeted at one point following a layer switch, and I had to

backtrack every step. It wasn't coding alone; it was logic, patience, and pressure proof problem-solving, which are cybersecurity cornerstone skills, particularly when it came to threat analysis or system vulnerability.

Cyber Law and Ethics

My "Cyber Law" course ended up being one of the most significant classes, not only for its content, but for how it made me look at cybersecurity from a legal and ethical perspective. We didn't memorize laws and regulations; we studied real-world case studies of digital rights, intellectual property, and ethical hacking.

In one essay, I studied the legal implications of the Computer Fraud and Abuse Act (CFAA) and its impact on ethical hacking and bounty programs. This taught me the delicate line between safeguarding research and breaking the law. As a future government cybersecurity worker, learning these types of laws is not a choice but a necessity.

Philosophy surprised even me by influencing the way I approach cybersecurity. From dissecting moral frameworks to exploring ethical challenges, the philosophical ideas I studied equipped me to more critically evaluate the human consequences of technical choices. For example, while crafting policy recommendations for an imaginary data breach incident, I relied on Kantian ethics to make the case for transparency and responsibility.

Interdisciplinary Thinking in Action

Security is not done in isolation, and this is evident throughout my portfolio. A particular highlight is a Python application that I created to decrypt ciphertext using frequency analysis, a traditional demonstration of technical competence and historical insight. I did not create a simple brute-force application; I was researching encryption history, learning about language usage, and constructing an interface that users are going to use. This took not only programming skill but also a sense of language and an appreciation for user experience.

One of the larger interdisciplinary artifacts is my business plan for an imaginary cybersecurity training company. This involved tying together everything that I'd learned, from cybersecurity education to business communications. I researched target markets (healthcare, nonprofits, retail), created the services offered, and composed financial projections. This involved applying both technical and business strategy, and it taught me that cybersecurity professionals need to think both like entrepreneurs and teachers.

Communication and Public Speaking

Soft skills are given a bad rap in the tech world, but they are vital. My portfolio contains a video of a public speaking address, which was actually a class project on ADHD. I was freaking out to give that address, but it taught me how to explain difficult things so they make sense to people.

Whether it is describing threat vectors to a client or conducting a policy briefing, it is all about clear communications. This experience made me begin to feel confident about being an

ambassador for technical groups and communicating to non-technical stakeholders, which is an incredibly important thing to have as I enter the cyber landscape.

Writing has also been a big part of my experience. I have done dozens of essays on all topics from the ethics of surveillance to AI and its impact on society. These all made me slow down and think carefully, not only about what I think, but how to support it with evidence and reason. Writing clear, compelling reports is just as crucial to being a good cybersecurity specialist as conducting scans or coding.

Lessons from the Field: Pharmacy, Precision, and People Skills

While not cybersecurity-related, being a certified pharmacy technician for four years taught me discipline, precision, and the capacity to perform under stress. Preparing medications for hundreds of patients daily meant I just couldn't make mistakes. The same habits translate to cybersecurity, where one misconfiguration would result in a breach.

Working within a high-stress, high-responsibility environment also helped build people skills, resolving conflicts, working with sensitive information, and communicating effectively to a diverse array of people. These are transferable to a cybersecurity environment, particularly to incident response or security awareness training roles.

One of the unexpected areas where I improved was stress management. As a cybersecurity analyst, it is very easy to burn out. Being aware of how to remain composed if something goes wrong, how

to deal with conflicting deadlines, and how to function within a team amid stress are all things that I learned way in advance of producing code.

Broadening My Perspective

Something that did surprise me throughout this program was how crucial research and writing actually were. I used to believe that cybersecurity was largely composed of math, code, and firewalls. But the more I learned, the more I understood that knowing the larger picture means immersing oneself into what is going on right now, how policy impacts it, and what happened previously.

Several of my research assignments delved into issues such as the ethical use of surveillance technology, the privacy ramifications of social media, and the expanding application of artificial intelligence for defense and for cyber-crimes. These assignments got me to read widely and analytically, from government policy reports to academic journals. That research experience made me more aware of cybersecurity being so interrelated to law, politics, economics, and psychology.

It taught me how to synthesize information across disciplines, to make arguments, and to explain difficult ideas in simple language. These are definitely useful for the case of risk assessment or policy briefs that I'll be producing for the future. It also kept me aware that cybersecurity isn't technical only, but social, political, and personal.

Future Goals and Career Readiness

Currently, I am still determining my specific career direction, but I am aware that I wish to pursue a career in cybersecurity, perhaps as a security analyst and preferably within government-related affairs. My confidence lies in how comprehensive my education has been.

My technical background is solid. I've coded challenging software, combed through networks, and designed machine learning models. But I also learned about ethics, law, business, and communications. The interdisciplinary foundation provides the versatility to switch gears, be that from policy, pen-testing, or public engagement efforts. I've also come to discover that cybersecurity isn't only about protecting systems. On top of that, it's about people, behavior, motivation, and society. That's what I'm taking to the industry.

In the future, I hope to continue learning. That may mean pursuing certifications such as Security+ or continuing towards a master's degree. I understand that cybersecurity is a field that continues to evolve. I also hope to explore opportunities within the federal government, especially within DHS or the CISA. Working within those types of roles would enable me to make a valuable contribution to national security while continuing to advance within my career.

Conclusion

Looking back, what impresses me isn't what I learned from each course so much as how those lessons linked together. Cybersecurity at ODU wasn't code alone or policy alone or theory alone. It was putting all those together to develop a mindset. A mindset that is curious, flexible, and ethical.

Each and every item in my portfolio represents a chapter of that story, from deciphering cipher text to arguing about digital ethics, from constructing neural nets to selling a business concept. I'm more than graduating with a cybersecurity major, I'm graduating with an arsenal of techniques, insights, and hands-on experiences that prepare me for a career, regardless of where I end up within the industry.

Works Cited

Denning, D. E. (1999). *Information Warfare and Security*. Addison-Wesley.

Florêncio, D., Herley, C., & Van Oorschot, P. C. (2014). *An Administrator's Guide to Internet Password Research*. USENIX.

Nissenbaum, H. (2004). *Hackers and the Contested Ontology of Cyberspace*. New Media & Society, 6(2), 195-217.

Spinello, R. A. (2011). *Cyberethics: Morality and Law in Cyberspace*. Jones & Bartlett Learning.

Sussman, J. M., & Sussman, J. M. (2017). *Building a Career in Cybersecurity: The Ultimate Guide to Getting Hired*. Syngress.