

Reflection on Cybersecurity Skill Development and Professional Readiness

Sean M. Shreve

Old Dominion University

IDS-493: Reflection Paper

Professor Carin Andrews

May 05, 2026

Introduction

I am a Cybersecurity major, and while I am considered a senior at this point, I am also an unconventional student. I did not begin my college career eighteen years ago as a Cybersecurity major, rather a pre-med, pharmacy degree. After a couple of semesters, I joined the United States Navy and served a usual four-year contract. I resumed my studies afterwards and changed my major to a traditional pre-med for medical school. Some breaks had to be taken, and colleges changed to support my spouse and family as we moved due to the military family lifestyle. Now we come to late 2025, where I changed my major once more to cybersecurity to pursue reentering the Navy as an officer.

Suffice to say, I am still rather new to the discipline of cybersecurity even though I am a senior. I have developed some skills that directly support a transition into a role within the field, but I am more focused on my Navy return. I do plan on working in the field after my Navy career, I even hope to be in cyber while I am serving, but that is not a guarantee. With my current time in college and my prior service I have developed skills in threat analysis and security evaluation, systems maintenance and technical troubleshooting, and technical communication and systems documentation. These skills may be quite a mouthful, but I stand by their sincerity and their cultivation through coursework, interdisciplinary study, and hands on technical work. I look back on these experiences fondly and look forward to the remaining courses I have left for my degree.

Threat Analysis and Security Evaluation

Of the most impactful skills that I have developed in my experience is threat analysis and security evaluation. I have demonstrated this skill through several artifacts in my portfolio, including my research on cybersecurity risks in military medicine and my analysis of the Equifax

date breach in 2017. These assignments encouraged me to look beyond surface level risks and evaluate their deeper level consequences and impacts.

When I began my coursework in cybersecurity, I initially viewed the discipline as a technical process. Tools, configurations, defense systems, this was all that was needed besides an operator. How incorrect I came to be as I learned that exploitation of vulnerabilities are rarely isolated incidents. That these are often the result of technical gaps, human decision (or mistake) making, and organizational oversight all working together. The Equifax breach in particular made this clear. Something as routine and simple as a delay in patch scheduling and implementation had consequences on a national scale.

My telemedicine research was also part of a new area of study for myself, interdisciplinary. As I researched, I had to consider not just system security, but also patient privacy, operational requirements, and the realities of military combat zones. It became clear to be after that course (Interdisciplinary Theory & Concepts, IDW300) that cybersecurity decisions are rarely made in a vacuum. There is always a balance between effective measures, security, usability and mission effectiveness.

Systems Maintenance and Technical Troubleshooting

This section of my reflection comes primarily from my experiences in the Navy. I became familiar with preventative and corrective maintenance on cryptologic systems as that was my responsibility. I understood from a small slice of pie that systems can have clearance restrictions, vulnerabilities, and exploits. But my coursework so far has expanded and zoomed out my viewpoint, reaching enterprise level perspective.

I have worked through some system configurations, troubleshooting scenarios and maintenance practices through labs. A big takeaway that wasn't a surprise to me was having a

more specific process to security and management. Rather than guessing at solutions, I reviewed how to identify symptoms, test fixes, verify results, and more. Though not necessarily new information, it was a relief to know that the troubleshooting principles that I learned in the Navy were not specific to only the military branch.

The interdisciplinary aspect is not excluded here either. This reflection has shown me how systems maintenance connects to larger operational goals that exceed a classroom or a Navy ship for that matter. Reliability and continuity are mandatory for any semblance of cybersecurity strength, and the combination of information systems, military systems, and cyber intelligence depend on it. I was already applying this philosophy while I was maintaining systems, but these academic lessons are very relevant to my future goals. Whether I have the privilege to return to a cyber related role or not, the skill sets give me confidence that I can operate in new work settings where failure cannot be an option

Technical Communication and Systems Documentation

The final skill development I am reflecting on is technical communication and systems documentation. Perhaps a tad foolish, I did not expect the amount of writing and technical analysis, evaluating, and summarizing I have had to do in my small time in the major. Through various writing assignments, discussion posts, and research papers, communicating technical information in a clear and useful way is a skillset I never knew I needed.

I demonstrated this skillset in particular this semester with my research paper in my Windows System Management (CYSE 280) course. I focused on how federal Windows based enterprise systems and environments are configured, managed, and secured. I also delved into topics of Windows tools, such as Active Directory, Group Policy, and more. It was expected of me to explain how these systems work together to enforce security policies and mitigate threats

in a structured security environment. In that paper specifically I also developed simple policy diagrams to represent the processes of cybersecurity basics applied to federal systems.

My long-term goals especially aligned with this coursework and will be valuable in the future, especially if I am a part of policy development. I have a strong starting foundation to communicate technical processes, document systems, and explain security decisions.

Conclusion

I have done several reflection assignments over the course of my lengthy education journey, and I always find some great ways to improve. I still consider myself a novice to cybersecurity, but I have begun to really develop a strong foundation that allows me to approach problems with more confidence than I had before. It would be foolish to not give my military background the credit it deserves, because my transition to this major has been very successful overall. My academic and military experience have come together in a way that makes my artifacts and skills feel practical rather than just theoretical.

One of the strongest takeaways from the program would have to be the study of interdisciplinarity. It may be a tad embarrassing to say, but I have never heard of the subject or idea before this major. I have learned now that Cybersecurity is not limited to technical systems alone, and that it involves human behavior, decision making, and real world constraints.

Effective cybersecurity solutions require a balancing act with these factors.

My primary goal remains returning to the Navy as an officer, and while I do not know what role I will be assigned to, I am confident that this education will be instrumental to my success. I have a very strong starting point in regards to my major's subject, and I am sure I will be ready to apply these skills in a way that supports my professional growth moving forward.