

IDS493 - Reflection Essay

India Henry

Old Dominion University

Dr. Sherron Gordon-Phan

May 5, 2026

Abstract

Over the duration of this course, I have learned to reflect on instances that have developed my educational and professional identity. Through various courses, I have knowingly developed hard skills while also developing soft skills that can be applied as I continue forward (Henry, n.d.). This project has helped me to develop my educational and professional identity by allowing me to reflect on the experiences I have had and how they have shaped me as a person overall (Nguyen, 2013, 135-148).

Introduction

During this class, I have learned a lot about the necessity of reflecting. For me, the reflection process goes back to elementary school, when I was first introduced to computer science; however, I have learned that there are people and projects that have shaped the way that I understand cybersecurity as a whole. Something that I find especially important in reflecting is understanding how certain experiences led to me learning soft skills, and growing to view soft skills as equally important as hard skills (Henry, n.d.).

Networking

My first introduction to networking was actually in a programming and networking course that I took freshman year. I thoroughly enjoyed that class, and at the time I thought it was because of the programming portion, but reflecting on that experience, I now know that I also enjoyed using the program Cisco Packet Tracer to design networks. Later on, I took an introductory networking and security course, which has shaped my outlook on the possibilities for careers I may have. The artifacts I chose to use are from my networking and security course; I chose to display them in a chronological order to show both the hard skills I learned from the course, being the progression of my understanding of networking, and the progression of my soft skills, being business communication through creation of presentations designed to explain technical concepts to non-technical audiences.

The first assignment I added is *Designing a Simple Network*; this was one of the first assignments that I completed in the class, and is reminiscent of the networks I created in my programming and networking class using Cisco Packet Tracer. Now knowing more about networking, this isn't the best assignment, but I decided to add it because it helps me to show the

progression of learning networking and the numerous soft skills that I was starting to develop by completing these projects. This project demonstrates my use of Microsoft Office, using visio and powerpoint, creating a budget so I am more conscious about the financial side of cybersecurity, while also being one of the first iterations of business communication.

The second assignment I decided to add is the first of a two-part assignment of *Wiring Constant Hall*. I decided to add the first version of this because I think it helps to show how I had built upon the hard skills from the first networking assignment, but there was still major need for improvement. This was also a larger assignment that I spent a lot of time on, and while I can recognize that I can create a better version of this assignment now, I am still proud of what I was able to accomplish with the knowledge that I had. This assignment also shows my further development of soft skills: Microsoft Office, business communication, and budgeting.

The final assignment that I added was the final project for my networking and security class, a *Case Study on Wiring Maury High School*. This assignment is a compilation of every topic that I learned during the course; it shows many hard skills like discussing different types of wiring, creating diagrams and justifications for the wiring, creating a more complex network configuration that includes redundant hardware, and firewall implementation and configurations. This assignment also shows the development of my soft skills: business communication, Microsoft Office, and budgeting. While I can admit that this assignment can still be improved, I think it helps to best show my development of various skills over the course of a semester.

Threat Knowledge

While researching cybersecurity jobs and internships, one skill that comes up frequently is threat knowledge. This skill is more detailed than simply knowing the name and description of

a cyber-threat, it is about understanding how known-threats work, knowing about threat detection, and having hands-on experience with exploitations. While my hands-on experience comes from course work, the examples that I use show a varying degree of difficulty of my threat knowledge as well as showing my ability to learn about cyber threats more thoroughly. Following the same strategy I used before, I placed my assignments in chronological order to show how my hard skills surrounding threat knowledge and analysis developed over time; instead of following one specific class, I decided to show how these skills developed across different classes.

The first example I added for threat knowledge is a *Password Cracking* assignment from a Linux Systems class. This assignment was my first exposure to threat knowledge in a hands-on, lab, environment. While the assignment is not the most sophisticated, it does show a variety of hard and soft skills. Some of the hard skills include navigating the Linux Operating System, navigating directories, creating user accounts and passwords of various difficulties for those users, then using a tool to show the password vulnerabilities. The main soft skill that I learned from this course was the importance of documentation; I had limited experience with technical documentation before this class, and it is something that I carried with me into my future classes and will eventually carry into the workforce.

The second assignment I used was a *Traffic Sniffing* assignment from my cybersecurity techniques and operations course. The reason I decided to include this assignment is because since this class, I have used Wireshark in various other classes and I learned a lot from this initial exposure. This assignment shows mostly hard skills, those being navigating linux, navigating wireshark, and analyzing the information found in the assignment. However, I think the most important thing I learned from this assignment, or the class overall, was the soft skill detailed and

thoughtful documentation. For this class, I learned to create easy to follow documentation and explain my strategy for completing assignments, which is an important skill to have and can be carried across different careers.

The last assignment I added was my *Digital Forensics Final*. I wanted to add this assignment because threat knowledge is equal parts technical and conceptual. While the course was lab-based, the final took the knowledge from the labs, put it into a realistic context, and required documentation according to the context. Digital forensics is a different type of threat knowledge than the previous examples, in that it is more about documenting failed defensive operations and investigating successful offensive operations. The hard skills this assignment demonstrated was mostly in the knowledge of digital forensics and navigating it in a realistic context. The soft skills were thorough, yet easy to understand documentation.

Cyber Policy

While the other two skills were important to my development, and ultimately skills that I will continue to grow, I would say that cyber policy is a skill that helped me develop my educational and professional identity. This skill is a convergence of my major, cybersecurity, and my minor, political science. To be able to accurately understand and analyze cybersecurity policy, it is imperative to know the technical side of cybersecurity to truly understand how cybersecurity policy is integrated into society.

The first assignment I decided to add was from cybersecurity, technology, and society, which was about the *CIA Triad* for cybersecurity. This was one of the first times I learned about the CIA Triad, and while this concept was developed far more in future classes, I think this example shows how cybersecurity is integrated into society from a more technical perspective.

Later on it was discussed how the CIA Triad impacts people outside of the technological perspective, and how cybersecurity professionals have to adapt knowing the mentality of people outside of the cybersecurity field. I included this paper because while it focuses on the technical perspective, it is an example of how cybersecurity policy impacts non-cybersecurity professionals.

The second assignment I decided to add is an *Article Review* that focuses on criminology and cybersecurity. While I added this to cybersecurity policy, I did it to juxtapose two things: the consequences of the lack of AI policy on society and to show the growth in both global AI policy and my own responses to it. This assignment also helps to show how interdisciplinary cybersecurity is and the importance of addressing different disciplines while creating policy, or in this case choosing to leave AI unregulated.

The third assignment I added provides an *overview of the European Union's Artificial Intelligence Act (EU AI Act) (2024)* (Kusche, 2025, 1-14). from the course Cybersecurity Policy and Strategy. For this course, I wrote a series of papers that addressed the political, ethical, and social implications of the EU AI Act. These papers go in depth on the impact of cybersecurity policy in different areas of society, whether the policy addresses AI to prevent negative impacts or if the policy itself had a negative impact after integration.

Interdisciplinary Research Paper

My long-term goal with cybersecurity is to focus on cybersecurity policy. One controversial topic is the prolific creation of AI data Centers (Kirpes & Klingert, 2016, 1-6). I decided to focus my research on *the consequences of the xAI, or Colossus, Data Center in Memphis, Tennessee* to provide an overview of the nuance of the creation of data centers. When

this paper was written, there were a few cities domestically that were facing a data center boom; however, now this is a more viral controversy as more data centers are being built in cities across America. This research was an attempt to bridge the disciplinary gap between the computer, environmental, and political sciences and directly relates to my policy work (Garrett-Peltier, 2017, 439-477).

Conclusion

During the duration of this course, I have learned to view my coursework as assignments that have built my academic and professional identity by helping me to grow my hard and soft skills. Admittedly, I focused a lot on developing my hard skills, and while those are skills that I will continue to work on, the soft skills that I developed along the way are equally important to my development, ultimately contributing to my educational and professional identity (Nguyen, 2013, 135-148).

References

- Garrett-Peltier, H. (2017). Green versus brown: Comparing the employment impacts of energy efficiency, renewable energy, and fossil fuels using an input-output model. *Economic Modelling*, 61(1), 439-477. <https://doi.org/10.1016/j.econmod.2016.11.012>
- Henry, H. (n.d.). *Top Soft Skills in the 21st Century Workplace*. Junior Achievement of South Florida. <https://jasouthflorida.org/top-soft-skills-in-the-21st-century-workplace/>
- Kirpes, B., & Klingert, S. (2016). Evaluation process of demand response compensation models for data centers. *E2DC '16: Proceedings of the 5th International Workshop on Energy Efficient Data Centres*, 1(4), 1-6. <https://doi.org/10.1145/2940679.2940683>
- Kusche, I. (2024). Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk. *Journal of Risk Research*, 1-14. <https://doi.org/10.1080/13669877.2024.2350720>
- Nguyen, C. F. (2013). The ePortfolio as a Living Portal: A Medium for Student Learning, Identity, and Assessment. *International Journal of ePortfolio*, 3(2), 135-148. <https://files.eric.ed.gov/fulltext/EJ1107805.pdf>