

CYSE 368 / Internship — Final Paper

Troy Bannister

SA Tech — Subcontractor to Huntington Ingalls Industries (HII)
Navy Integrated Training Environment (NITE) Contract

Professor Teresa Duvall
CYSE 368 — Internships in Cybersecurity
Spring 2026

Date: April 19, 2026

Table of Contents

1. Introduction.....	3
2. Management Environment.....	4
3. Major Work Duties, Assignments, and Projects.....	5
4. Cybersecurity Skills and Knowledge.....	7
5. ODU Curriculum and Internship Connection.....	8
6. Learning Objectives: Fulfillment Assessment.....	9
7. Most Motivating Aspects.....	10
8. Most Discouraging Aspects.....	10
9. Most Challenging Aspects.....	11
10. Recommendations for Future Interns.....	11
11. Conclusion	12

1. Introduction

My path into this internship is not a traditional one. I have been working in my current position as an LVC Engineering Technician V for the past seven years — long before I enrolled at Old Dominion University to formalize the cybersecurity knowledge I had been applying in practice. When the opportunity came to fulfill my internship requirement through CYSE 368, the decision was straightforward. My workplace sits at the intersection of network engineering, systems administration, and cybersecurity in a high-stakes, operationally real environment. There was no better laboratory for this course than the one I was already working in every day.

The organization I work within is built around the Navy Integrated Training Environment, or NITE — a U.S. Navy contract that supports how Strike Groups and Air Wings prepare for deployment. NITE provides a Live, Virtual, and Constructive (LVC) training framework that simulates escalating geopolitical conflict scenarios against a fictional adversary nation. These exercises are not simple drills; they require the precise coordination of dozens of networked systems across multiple geographic ranges to present realistic, real-time scenarios to training audiences that include carrier strike groups and their command staff. The contract is administered through Huntington Ingalls Industries (HII), and my direct employer, SA Tech, assumed the subcontractor position on the NITE contract in November of 2025. Over my seven years in this role, I have technically been employed by four different companies as the subcontractor position has changed hands — a reality that speaks to the nature of government contracting more than it does to any instability in the work itself. The role of LVC Engineering Technician V has remained constant throughout.

My specific assignment within NITE falls under the Large Area Tracking Range, or LATR, Operations department. LATR is the system responsible for tracking, displaying, and recording all assets operating within the exercise environment — aircraft, surface vessels, and their associated electronic signatures. My role within LATR Maintenance places me at the operational core of keeping those systems running. I manage hardware, apply patches, maintain inventory, troubleshoot peripherals, and serve as the coordination layer between departments and ranges when data integrity across the system is at stake.

When I formally enrolled in CYSE 368 and completed my Memorandum of Agreement with my supervisor, we established four primary learning objectives for this internship period:

1. Further develop system and operational competency.
2. Apply system knowledge to troubleshooting evaluation skills in real-time.
3. Increase administrative knowledge that impacts inter-departmental workflows.
4. Integrate cybersecurity academics with real-world engineering practices.

What made these objectives meaningful rather than formulaic was the timing of the semester. The Spring 2026 period aligned nearly exactly with a major exercise evolution, meaning that from the first week of the course, I was operating in a live environment where these goals were immediately relevant. The reflective nature of CYSE 368 also shifted something in my daily approach. Rather than simply executing tasks, I began evaluating them through a more formal cybersecurity lens — asking not just whether something worked, but whether it aligned

with security principles, documentation standards, and the kind of professional discipline that academic coursework had been building toward.

2. Management Environment

The management structure within LATR Operations is layered in a way that reflects both the union environment and the government contracting context that surrounds it. All LATR Operations personnel, including myself, are unionized employees under SA Tech. Our immediate supervisors are LATR Operations and Maintenance Supervisors who are employed directly by HII, the prime contractor. They serve as the onsite management layer and translate requirements that flow down from the government customer and HII leadership into actionable direction for the technical staff.

Within the LATR Ops workforce itself, technicians are tiered at either Level IV or Level V. Level V technicians, which is my classification, are considered shift leads and subject matter experts. A Level V can run a mission independently, delegate tasks to Level IV personnel, and communicate directly with our government liaison, the government customer, or visiting VIPs and exercise guests without needing to escalate to the Operations managers. That autonomy is earned and carries real responsibility. When something goes wrong during an exercise, the Level V on shift is the first point of accountability.

The LATR department is also divided into two functional groups: Analysts and Maintenance. Analysts are the system operators — they run the display products, generate and distribute debriefing materials, file required reports, and serve as direct on-site representatives during underway periods aboard training vessels. They interact directly with the Carrier Strike Group Four Admiral and the exercise director, who holds a GS-15 government civilian designation. Maintenance, which is my group, handles the infrastructure that makes all of that possible. We manage hardware, apply patches, maintain inventory, troubleshoot peripherals, and serve as the inter-departmental and inter-range communication layer to ensure data integrity across all systems during an exercise.

As a Level V on the Maintenance side, my day-to-day supervision is relatively hands-off in terms of technical direction — my supervisors trust my judgment on system matters and I am expected to operate with a high degree of independence. Where supervision is more active is in coordination with government requirements, scheduling, and compliance documentation. That balance between technical autonomy and administrative accountability has been one of the defining features of my work environment throughout this internship period.

3. Major Work Duties, Assignments, and Projects

The 150 hours covered by this internship course spanned three distinct operational phases, each of which brought a different mix of responsibilities.

Pre-Exercise Preparation and Laptop Deployment Validation: The first 50 hours were centered on pre-embarkment preparation of the deployable laptop systems used to support training commands aboard vessels. Each laptop required connection testing, application

validation, and firewall coordination before being certified as operationally ready. During this phase, I identified and corrected configuration file issues written in C++ and Python that stemmed from an incomplete version update rollout across the fleet. I also discovered that a security patch had broken Microsoft Suite authentication on one system, which pointed to a gap in our standard pre-deployment validation process. In response, I developed and submitted a Pre-Embarkment Operational Testing Checklist, which was formally approved and added as an addendum to our Work Instructions. This contribution directly addresses a recurring documentation gap and reduces the likelihood of small validation failures compounding into larger operational problems.

A significant connectivity issue also emerged during this phase when deployed laptops experienced failures on port 22, disrupting SFTP file transfer operations through WinSCP — a critical tool for field operations. I used netstat with the target IP address and port 22 to monitor connection attempts in real time and supported coordination between our Navy Operational Support Center and the shipboard IT team. The issue was resolved without escalation.

Live Exercise Operations and System Administration: The second 50 hours shifted into active exercise support under shift work conditions. The nature of the work changed significantly — troubleshooting became reactive and time-sensitive, and the stakes of any delay were directly tied to the integrity of an ongoing training evolution. During this period, my day-to-day tasks included restarting unresponsive applications, resolving KVM and keyboard peripheral issues, and remotely accessing closed-out VM sessions to restore operator access. I also submitted and received approval for master virtual image recompose requests, which demonstrated that my technical assessments were being acted on at the systems level.

The most technically substantive challenge of this period involved a cross-range display forwarding issue between our Virginia Beach range and the North Carolina range. A mission being run in North Carolina needed to be displayed on our Linux-based TSPI display system. All multicast configurations and port settings were verified correct, and network operations confirmed no firewall restrictions were in place, yet incoming data was arriving fragmented. We reversed the data direction as a diagnostic step — sending our data to North Carolina — and they received a clean picture, isolating the problem to our ingress side. Tcpdump captures and Wireshark analysis confirmed packet fragmentation. MTU adjustments at the application and server level did not resolve it, and the issue was escalated to our DevOps and software engineering teams, who investigated UDP message format and network-level MTU configurations. This issue remained under investigation through the end of the semester.

Building Migration, Service Disruptions, and Diagnostic Work: The third 50 hours were defined by the operational impact of a neighboring building's temporary relocation into our facility during their refurbishment. This building operates one of our primary source input systems on a separate server and has historically functioned in a largely isolated network environment. Their move into our space required them to share our Linux-based display server — the same systems already involved in the North Carolina forwarding issue — which meant reconfiguring those systems to support two separate operational configurations simultaneously. The challenge was not at the GUI level but in the underlying configuration files and in the inter-departmental coordination required to register new ports and establish digital communications configurations for the relocated team, whose debriefing workflow within the Linux system differed entirely from ours.

The relocation also severed a tertiary multicast source input that several of our subsystems relied on. The backup system providing the equivalent input does not support multicast, resulting in a loss of redundancy for those subsystems. At the government level, this triggered a formal service disruption documentation process — initialization logs, follow-up reports, and fielded inquiries — all managed in parallel with active exercise operations. The administrative overhead of that process was instructive in its own right, reinforcing that in government-supported environments, accountability does not end when a problem is identified.

Two additional diagnostic efforts stood out during this period. The first involved monitoring parent and child process logs in a Linux-based error logging system to investigate why a tertiary source input was being consistently dismissed. The log analysis revealed a tangent plane configuration incompatibility — the receiving system was rejecting the input because the geometric reference frame being provided did not match its expected format. The fix required a configuration correction rather than a network or hardware intervention, a good reminder that surface-level symptoms do not always point to surface-level causes.

The second was a live logging failure in our debriefing application. The application records files to a shared network drive in four-hour increments, and the team had been arriving to find that logging had stopped overnight and required a manual restart, causing data loss during off-hours. I was specifically assigned to investigate given my operational background with the application. Using Windows Event Viewer and Reliability Monitor, I pulled error timestamps for both the application and the mapped drive and cross-referenced them against network maintenance logs. The correlation was exact — approved maintenance windows were severing the shared drive mapping, causing the application's target directory to disappear and logging to halt without any alert. The interim resolution was a scheduling workaround to avoid those maintenance windows during active exercise periods, with an additional local save option added as a fallback. Identifying this through Windows-based tools was a personal note worth acknowledging — I consider myself primarily a Linux-oriented technician, and working through the Event Viewer environment was a deliberate step outside my usual diagnostic toolkit.

Hardware Declassification: This period also included participation in the declassification and disposition of approximately 20 older laptops being cycled out of service. The process involved physically removing RAM modules and hard drives from each machine, removing classified asset stickers, and inventorying every component — laptops and drives separately — on material transfer forms for proper chain-of-custody accounting. The inventoried assets were then packaged and transferred to logistics for either reutilization or disposal through appropriate government channels. While the physical work was straightforward, the process carried real procedural weight. Classified media handling and accurate material accounting are not optional formalities — they exist because the consequences of a documentation gap in classified asset disposition can be severe and legally significant.

4. Cybersecurity Skills and Knowledge

Going into this internship, my technical foundation was already well-developed from seven years in the role. My existing skill set included hands-on proficiency with Linux system administration, virtual machine management, network configuration and troubleshooting, application-level diagnostics, and the operational understanding of how multi-range networked

environments function under exercise conditions. I could work through a packet capture, interpret error logs, manage KVM hardware, and coordinate across departments with confidence.

What this internship period added, or more precisely what it made more conscious and deliberate, was the application of a formal cybersecurity framework to work I had previously executed more intuitively. The reflective structure of CYSE 368 pushed me to evaluate what I was doing through the lens of security principles rather than just operational effectiveness. When I coordinated a firewall exception during the port 22 connectivity issue, I was also thinking about least-privilege principles and the risk of creating unnecessary network exposure. When I developed the Pre-Embarkment Operational Testing Checklist, I was formalizing a process that had previously relied on individual memory and tribal knowledge — and recognizing that documentation is itself a security control.

On the job learning during this period came primarily through the diagnostic challenges. The MTU fragmentation investigation required me to go deeper into UDP transmission behavior and network-layer MTU settings than I had previously needed to in a practical context. The tangent plane configuration incompatibility introduced me to the specifics of how geometric reference frames are handled at the source input level in TSPI systems — something that is genuinely specialized knowledge not easily found in academic coursework. And the Windows Event Viewer correlation work expanded my diagnostic toolkit into a platform I had previously been less comfortable with.

Across all of these experiences, my understanding of cybersecurity has shifted in one meaningful way: I now see the administrative and procedural dimensions of the field as equal in importance to the technical ones. The service disruption documentation process, the material transfer forms, the checklist addendum — these are not paperwork for paperwork's sake. They are the mechanisms through which accountability is maintained, audits are survived, and institutional knowledge is preserved across contractor transitions.

5. ODU Curriculum and Internship Connection

My ODU coursework has connected to my internship experience in ways that are both direct and indirect. On the direct side, coursework covering Linux systems, virtualization, networking fundamentals, and server administration has provided a formal vocabulary and conceptual structure for things I was already doing in practice. Understanding OSI layers academically, for example, gave me a more precise framework for approaching the MTU fragmentation issue — being able to articulate which layer the problem was likely occurring at helped structure both my own thinking and my communication with the DevOps team during escalation.

Networking concepts around multicast, UDP, and packet behavior were reinforced throughout the cross-range forwarding investigation. While the specifics of the TSPI display system are not something any academic course would cover directly, the underlying principles of how multicast group membership works, how fragmentation occurs at layer three, and how MTU mismatches propagate through a transmission chain were all grounded in material I had studied at ODU.

The curriculum has also provided context that extends beyond my direct work environment. My exposure to CISA frameworks and cybersecurity governance has informed how I communicate with people outside my immediate team. When coordinating with other departments or explaining a service disruption to stakeholders, having a formal understanding of risk management, service continuity, and security documentation gives me credibility and structure that pure operational experience does not always provide.

Where the curriculum has not yet fully connected is in the deeply specialized areas of my work — TSPI data formats, LVC architecture, tangent plane geometry, and the specific protocols used in military training range networks. These are areas where my seven years of on-the-job experience far outpaces what any academic program would reasonably cover. That is not a criticism of the curriculum; it is simply the nature of a field where real-world specialization runs deep. What ODU has provided is the foundational fluency that makes everything else learnable.

6. Learning Objectives: Fulfillment Assessment

Objective 1 — Further develop system and operational competency: This objective was fulfilled across all three phases of the internship. Pre-exercise preparation deepened my familiarity with the deployment validation process and led to a formal procedural contribution. Live exercise operations placed me in high-tempo troubleshooting scenarios that required both technical precision and real-time decision making. The third period introduced new operational complexity through the building migration and its cascading system effects. Competency in this environment is not static, and this semester confirmed that there is always a more complex version of a problem waiting.

Objective 2 — Apply system knowledge to troubleshooting evaluation skills in real-time: The MTU/fragmentation investigation, the tangent plane log analysis, the live logging failure diagnosis, and the port 22 connectivity resolution all represent direct fulfillment of this objective. Each required working through a problem methodically under operational time pressure, without the luxury of taking the system offline. The logging diagnosis in particular — using Event Viewer timestamp correlation to identify a non-obvious root cause — was the clearest example of applying structured analytical thinking to a real-time problem.

Objective 3 — Increase administrative knowledge that impacts inter-departmental workflows: The service disruption documentation process, the material transfer form inventory, the Pre-Embarkment Checklist approval, and the port coordination with the networks department all contributed to this objective. Of these, the service disruption documentation was the most instructive because it forced engagement with the government administrative process in a way that purely technical work does not. Understanding how formal service disruption records are initialized, followed up, and closed out is knowledge that will directly support future work in government or government-adjacent environments.

Objective 4 — Integrate cybersecurity academics with real-world engineering practices: This was perhaps the most personally meaningful objective because it speaks directly to why I enrolled in this program in the first place. The reflective structure of CYSE 368 created a habit of evaluating my work through a formal cybersecurity lens rather than purely an operational one. The connections I identified between least-privilege principles and firewall coordination,

between documentation as a security control and the checklist I created, and between network security frameworks and the way I communicate risk to non-technical stakeholders — all of these represent the integration this objective called for.

7. Most Motivating Aspects

The most consistently motivating aspect of this internship has been the experience of watching academic concepts land in practice in real time. There is a particular kind of satisfaction that comes from sitting in a networking course, building a mental model of how UDP multicast works, and then finding yourself six months later staring at a Wireshark capture during a live exercise trying to figure out why packets are fragmenting across a range boundary. The academic knowledge does not solve the problem on its own, but it gives the problem a shape — and that is genuinely motivating.

Beyond the technical dimension, the operational context of the work is intrinsically meaningful. The systems I maintain support how the Navy prepares for real-world deployments. That is not a metaphor. The training audiences on the other end of these exercises include actual strike group commanders and their staff. Knowing that the integrity of the data flowing through systems I am responsible for has a direct bearing on the quality of that preparation makes even the routine tasks feel purposeful. That sense of consequence is something I have come to recognize as a core part of what keeps me engaged in this field.

8. Most Discouraging Aspects

The most consistently discouraging aspect of this internship has been the experience of imposter syndrome in a technically dense environment. I have seven years in this role and a deep familiarity with these systems, and there are still moments — usually when working alongside engineers who hold decades of specialized domain expertise — where I feel acutely aware of the gap between what I know and what I do not. That feeling does not always correlate with actual competence. I have diagnosed problems that more senior personnel did not catch, and I have contributed solutions that were formally adopted. But the internal experience of uncertainty in those moments is real, and I do not think it fully goes away.

What I have come to understand, through both the work itself and the reflective process this course required, is that imposter syndrome in technical environments is often a signal of self-awareness rather than inadequacy. Recognizing the limits of your knowledge is part of what makes you a careful, honest technician. The goal is not to eliminate that uncertainty but to not let it become paralysis. That is an ongoing project.

9. Most Challenging Aspects

The most challenging aspect of this internship has been resisting the pull toward a narrow technical identity — what I would call the trap of being just the tech guy. In cybersecurity and IT roles, especially in operational environments, there is a comfortable lane where you fix what is

broken, hand it back, and move on. That lane is real and valuable. But the cybersecurity field increasingly demands that technical professionals be able to bridge the gap between the system and the stakeholder — to translate what is happening in a server log into language that an operations manager or a government customer can act on.

Throughout this semester, the moments that required me to step out of the purely technical role and into that liaison function were consistently the most demanding. Coordinating the port registration and digital communications configuration for the relocated building required me to manage expectations across multiple departments while also executing the technical work. Managing the service disruption documentation required me to be the technical expert and the administrative point of contact simultaneously. These are not skills that come naturally from technical experience alone — they require a kind of professional range that I have been actively building, and that this course has helped me name and articulate.

10. Recommendations for Future Interns

For anyone considering an internship in this role or one like it, the first thing I would say is that this is one of the best-kept low-profile opportunities in the Hampton Roads area. It is low-key enough that you can realistically pursue a full-time degree program while working forty hours a week and earning a competitive wage. That combination is rare, and it is worth taking seriously.

The second thing I would say is that the ease of the environment is also its biggest risk. It is genuinely possible to spend years in a role like this performing well below your potential because the baseline expectations are not always high. The work is real and the stakes are real, but there is enough ambient stability that a person can coast if they are not intentional about growth. Do not do that. The access this environment provides to real-world cybersecurity problems — network administration, system hardening, classified asset handling, inter-agency coordination, live operational troubleshooting — is extraordinary. There is no reason a motivated person working in this space should not be well-prepared for any cybersecurity role they want to move into.

Practically speaking, come in with a working knowledge of Linux and be comfortable in a command line environment. Understand basic networking — IP addressing, port configuration, and how protocols like UDP and TCP behave differently. Be comfortable reading logs. And perhaps most importantly, be willing to communicate. The technical work is only part of the job. The ability to explain what is happening to someone who does not share your technical vocabulary is what separates technicians who grow from those who plateau.

11. Conclusion

The central takeaway from this internship is not a single technical lesson but a shift in professional identity. I came into CYSE 368 as someone who had been doing this work for seven years without a formal academic framework to hang it on. I am finishing it as someone who can

articulate why the work matters, what principles it reflects, and how it connects to a broader cybersecurity discipline. That is not a small thing.

The reflective structure of this course changed how I operate day to day in a way that I expect to be durable. Before this semester, I executed tasks. Now I evaluate them — asking whether they are consistent with security principles, whether they are documented properly, whether they could be done better or more systematically. That habit of mind is something I intend to carry forward.

For the remainder of my time at ODU, this internship has given me a clearer picture of where my academic gaps are and where I am stronger than I sometimes give myself credit for. I want to lean into the governance and framework side of cybersecurity — CISA, NIST, and the policy and documentation dimensions of the field — because I have seen firsthand how much those areas matter in a government-adjacent environment and how often purely technical professionals undervalue them.

For my professional path, the internship has reinforced that I want to remain in operationally consequential environments. I am not drawn to cybersecurity as an abstract discipline — I am drawn to it because of what it protects and what breaks when it fails. The systems I have spent seven years maintaining support real naval readiness. That context is what makes the work worth doing, and it is the standard I will hold future roles to.