

# Grey Areas and Egress

## Artifact-Based Collaborative Learning in Cybersecurity Ethics

Ryan M. Straight<sup>1</sup>

<sup>1</sup>University of Arizona (ryanstraight@arizona.edu), ORCID: 0000-0002-6251-5662

---

### Abstract

This reflective essay examines my implementation of artifact-based collaborative learning in cybersecurity ethics education through the analysis of authentic but fictional case studies. Rather than analyzing pre-digested narratives, such as the case of Edward Snowden, students engage with hypothetical primary source materials (internal memos, encrypted communications, investigative reports, and exit interviews) that mirror reality and professional investigative practice. The assignment requires collaborative groups to produce a written analysis addressing six analytical tasks that integrate ethical frameworks, legal analysis, and stakeholder perspectives. Students learn to craft arguments that synthesize documentary evidence, construct legal analyses using appropriate discourse, and develop policy recommendations in professional genres. Students navigate the grey areas of cybersecurity ethics, law, and policy, wrestling with competing approaches where reasonable people disagree. The artifact-based collaborative writing approach demonstrates how technical students can develop integrated writing and reasoning capabilities essential for cybersecurity governance roles when these skills are embedded in meaningful professional contexts.

---

Teaching cybersecurity ethics has taught me that students arrive expecting algorithms for moral decision-making and leave, if we succeed, comfortable with uncertainty. The EXODUS case study described here presents undergraduate cybersecurity ethics students with a scenario involving corporate data theft, potential whistleblowing, and conflicting professional loyalties. Students often expect clear-cut moral positions and straightforward policy recommendations from such materials. Instead, they encounter ethical, legal, and policy grey areas—complex ethical ambiguity surrounding characters whose decisions potentially affected millions of people. This pattern of student responses revealed a critical gap in cybersecurity education (Frusci, 2024): while technical students often excel at identifying security vulnerabilities and implementing protective measures, they sometimes struggle to analyze ethically ambiguous circumstances, precisely the kind of analysis essential for leadership roles in this field.

The challenge extends beyond individual analytical capabilities. Cybersecurity is inherently interdisciplinary, involving aspects of law, policy, human factors, ethics, and risk management (Blair et al., 2020). Professionals increasingly work within interdisciplinary teams, negotiating between corporate executives prioritizing cost-effectiveness, legal counsel managing liability concerns, and technical staff advocating for robust security measures. These professionals need collaborative approaches for navigating competing professional values, yet traditional case study approaches typically emphasize individual analysis rather than the consensus-building processes that characterize real-world policy development (Christensen et al., 1991; Herreid, 2007).

This reflective essay examines my implementation of an artifact-based learning approach that addresses both the challenge of individual ethical reasoning under ambiguity and the need for collaborative, interdisciplinary synthesis. In artifact-based learning, students engage with hypothetical primary source materials similar to those that professionals would encounter in actual cybersecurity incidents: emails, reports, transcripts, technical logs, and other content.

**prompt**  
a journal of academic  
writing assignments

Volume 10, Issue 2 (2026),  
pages 94–104.

DOI: 10.31719/pjaw.v10i2.280  
Submitted August 31, 2025; accepted  
May 22, 2026; published August 17,  
2026.

© 2026 The Author(s). This work is  
licensed under a Creative Commons  
Attribution- NonCommercial 4.0  
International License.

This approach differs from traditional case narratives where authors summarize information and guide interpretation. Instead, students examine primary source materials in professional genres—internal memos, investigative reports, legal correspondence—that cybersecurity practitioners encounter in actual incidents, drawing conclusions through careful document analysis rather than authoritative accounts.

Building on document-based historical inquiry methods (Bean, 2011), I designed a collaborative assignment, the EXODUS Collaborative Writing Assignment, requiring students to synthesize evidence across multiple artifacts while applying ethical frameworks, legal analysis, and stakeholder perspectives. The assignment uses cross-disciplinary writing as the vehicle through which students demonstrate their analytical synthesis, preparing them for professional contexts where cybersecurity practitioners must communicate complex findings to diverse stakeholders (Herreid & Schiller, 2013). The genre they encounter—investigative analysis, legal argumentation, policy recommendation—mirror how practitioners communicate findings, acculturating students to disciplinary conventions through practice.

## Course Context

CYBR 329: Cyber Ethics is an upper-division, writing-intensive course in the College of Information Science at the University of Arizona. The course enrolls approximately 36 students per section, primarily juniors and seniors pursuing degrees in cybersecurity operations, intelligence operations, information science, and related technical fields. Most students enter with strong technical backgrounds but limited experience with legal reasoning or formal ethical analysis.

The course meets in person twice weekly over a 15-week semester. The EXODUS Collaborative Writing Assignment occurs approximately halfway through the semester, after students have developed foundational knowledge in ethical frameworks, including consequentialism (evaluating actions by their outcomes), deontology (evaluating actions by their adherence to duties or rules), and virtue ethics (evaluating actions by the character they reflect), as well as relevant legal concepts. By this point, students have already completed several case analyses, building toward ever more complex collaborative challenges. The in-person format enables the real-time collaborative synthesis that defines this assignment.<sup>1</sup>

## The Assignment

The artifact-based approach emerged from my observation that cybersecurity students often struggle when ethical scenarios lack clear technical solutions. Traditional case presentations give students summarized scenarios with predetermined discussion questions (e.g., Manjikian 2022). Even compelling real-world cases like Edward Snowden’s disclosures arrive pre-digested, with the ethical positions already mapped and the key facts selected by textbook authors. This format fails to replicate the investigative complexity of professional cybersecurity work, which requires piecing together incomplete information, interpreting conflicting accounts, and developing policy recommendations amid uncertainty.

### The EXODUS Case

The EXODUS case, one of seven immersive case studies in the *Cyber Dimensions* textbook (Straight, 2025a), unfolds through a collection of hyper-realistic but ultimately fictional primary source documents that students must piece together to understand the complete narrative. This 25-page case contains over a dozen distinct artifacts that students navigate independently. It centers on Alex Chen, a quantum computing engineer who allegedly transferred proprietary code to a competitor, and the case takes its name from Chen’s departure: an act of egress whose

ethical and legal dimensions prove far from straightforward. Rather than reading a linear story, students examine:

- internal cybersecurity memos alerting executives to suspicious data access patterns,
- encrypted chat logs between Chen and unknown parties,
- FBI investigation reports detailing forensic evidence,
- exit interview transcripts revealing Chen’s ethical concerns about military applications of artificial intelligence,
- legal strategy documents from competing firms, and
- news coverage with conflicting perspectives.

Interpretive ambiguity emerges from the artifacts themselves. An internal security memo reports that Chen accessed “design files for three separate AI model architectures” (Straight, 2025a) during off-hours and transferred data to personal cloud storage, facts that could indicate corporate espionage. Yet the exit interview transcript reveals Chen expressing that “the applications being developed didn’t align with my personal ethics” and describing a desire to work on “open and collaborative projects” (Straight, 2025a). Students must reconcile these documents: Does the security memo describe theft or an ethical actor protecting work they believe serves broader humanity? Does the exit interview reveal genuine moral conviction or calculated justification? The artifacts provide evidence without interpretation, requiring students to construct meaning across contradictory possibilities.

The legal analysis compounds rather than clarifies. Two federal laws prove particularly relevant: the Computer Fraud and Abuse Act (CFAA) (1986) criminalizes unauthorized access to computer systems, though what constitutes “authorization” remains contested, especially when employees access systems they are permitted to use but for purposes their employers did not sanction; the Economic Espionage Act (EEA) (1996) criminalizes theft of trade secrets, requiring prosecutors to prove both that information qualifies as a trade secret and that the defendant knew or intended to cause harm; the International Traffic in Arms Regulations (2023) and Export Administration Regulations (2023) describe specific actions that could be considered illegal depending on Chen’s behavior. Students must apply both statutes to Chen’s actions while grappling with factual ambiguity about what Chen actually did and why. The legal uncertainty runs parallel to the ethical: the same artifacts that leave Chen’s motivations open to interpretation also leave questions of liability contested.

### Assignment Structure and Timing

The assignment unfolds across two in-class phases designed to scaffold collaborative analysis, preceded by individual preparation. In this pre-work, students review the entire EXODUS case independently, reading all artifacts and composing low-stakes written notes identifying key evidence and initial analytical observations. Through this preparatory writing, students process documentary information before discussion, sketch interpretations they will later defend or revise, and produce reference materials for collaborative work. Before the collaborative session, I provide explicit guidance about productive group practices, emphasizing that research demonstrates group case study discussions are more effective than individual analysis for developing critical thinking skills (Mahdi et al., 2020).

In the first phase, a collaborative synthesis during a 75-minute class session, self-selected groups of three to four students work through six analytical tasks characteristic of cybersecurity governance and policy work:

1. applying consequentialist, deontological, and virtue ethics frameworks to evaluate Chen's actions;
2. conducting comprehensive stakeholder analysis (identifying all affected parties, from Chen's former colleagues and the companies involved to the broader public who might benefit from or be harmed by AI applications);
3. determining potential legal violations;
4. analyzing the ethics of military artificial intelligence development;
5. evaluating corporate response through deontological and social contract theory (examining whether institutional actions reflect agreements that rational individuals would accept as fair) lenses; and
6. developing three organizational policy recommendations (addressing institutional practices rather than regulatory proposals) with implementation analysis.

During this session, I circulate among groups, listening to their discussions, fielding questions about case details or assignment requirements, and occasionally redirecting conversations that become mired in single frameworks. Groups become mired when they reach consensus too quickly through a single lens. For instance, some groups conclude that Chen clearly violated the law without examining whether the law itself reflects sound ethical principles. Others determine that Chen acted ethically without considering the legitimate interests of former colleagues who relied on proprietary code.

When I observe such narrowing, I pose questions that complicate their emerging consensus: "What would a virtue ethicist say about Chen's choice to act secretly rather than openly?" or "How might this same evidence look from the perspective of employees who stayed?" These prompts do not provide answers but rather model the kind of multi-perspective interrogation the assignment requires. The session concludes with brief oral presentations of one to two minutes each, where groups share their findings, exposing students to alternative interpretations and analytical approaches. The oral presentations receive formative feedback rather than formal grades, encouraging students to take intellectual risks during the synthesis phase.

In the second phase, groups produce a 900- to 1200-word collaborative written analysis, due at the module's conclusion, demonstrating mastery of multiple disciplinary writing conventions: legal analysis citing specific statutory provisions, ethical argumentation using philosophical frameworks, and policy writing with implementation considerations. The assignment requires students to work exclusively with the provided artifacts, developing analytical skills through careful documentary interpretation rather than from external research.

Groups organize their collaborative writing process autonomously. I have experimented with assigning individuals specific analytical roles, but found that students produce stronger work when they sort responsibilities organically, leveraging their own interests and strengths. Some groups divide the analysis by framework, others by section, and still others draft collectively. To ensure accountability and guard against uneven contribution, each group submits a brief reflection alongside their analysis describing their collaborative process, identifying who contributed what, and reflecting on how the collaboration shaped their thinking. This reflection makes visible whether one member carried the analytical weight or whether the group genuinely synthesized perspectives. When I observe contributions beginning to shift unevenly, I remind groups that the workload should be distributed equitably, though not necessarily discretely.

### Assessment Approach

Evaluating this assignment required developing rubrics capturing both process and product outcomes. The multi-dimensional requirements challenged traditional grading approaches, so I assess the written deliverable across six weighted dimensions: multi-stakeholder analysis

(25%), synthesis and integration of perspectives (20%), policy development with implementation pathways (20%), evidence of genuine collaborative process (15%), understanding of technology transfer and strategic protection concepts (15%), and writing quality including proper citation practices (5%). What distinguishes excellent from adequate work is not merely accuracy but sophistication: excellent submissions demonstrate nuanced understanding of how the same ethical framework can support competing conclusions, while adequate submissions apply frameworks mechanically without recognizing their interpretive flexibility. This distinction reflects how expertise functions in cybersecurity governance: professionals navigate contested interpretations rather than apply predetermined formulas. Policy development requires maintaining multiple analytical frames, recognizing that stakeholders with legitimate interests may reach different conclusions from identical evidence.

## Student Responses

Analysis of student submissions revealed consistent learning patterns. Students moved from ethical oversimplification toward sophisticated multi-framework analysis. They developed collaborative synthesis capabilities and transformed abstract framework knowledge into applied professional reasoning. Students immediately recognized the assignment's unprecedented complexity. Groups frequently observed that the EXODUS case felt far more ambiguous than previous case studies, marking a crucial shift from expecting clear answers to engaging with authentic professional ambiguity.

The collaborative process surfaced productive tensions. Groups commonly noted that the breadth of the CFAA, with its overlapping civil and federal prosecution pathways, posed distinctive challenges for collaborative analysis. Rather than viewing this complexity as a barrier, students came to see it as representative of professional practice. Writing instructors across disciplines may find this recognition familiar: students in many fields must learn to navigate ambiguity rather than expect tidy resolutions. These patterns emerged across four areas of student development: ethical framework application, legal-ethical integration, collaborative reasoning, and disciplinary writing.

### Ethical Framework Application

Students discovered that ethical theories could support different conclusions depending on application approach and interpretive emphasis. Groups frequently identified how a single framework could yield opposing conclusions. Several groups, for instance, observed that deontological reasoning about treating people as ends rather than means could support both Chen's open-source advocacy and the former employer's proprietary interests, depending on which stakeholders and duties the analysis foregrounded.

This recognition, that frameworks are analytical tools rather than answer keys, indicates professional sophistication. Other groups described arriving at a similar realization through close analysis: what initially appeared as a question with a definitive answer revealed itself as a set of competing interpretations, each defensible within different ethical traditions.

### Legal-Ethical Integration

Students developed nuanced understanding of how legal considerations apply to contemporary technology contexts. Groups commonly observed that Chen's actions might not violate the CFAA yet could constitute a clear EEA violation, a distinction that led many to question whether decades-old statutes adequately address modern technology practices. This observation reflects students recognizing that legal frameworks designed decades ago may not anticipate modern technological realities. This tension creates interpretive space requiring careful analytical

judgment. This integration of legal and ethical analysis mirrors professional practice, where cybersecurity work regularly requires considering multiple frameworks simultaneously.

### Collaborative Reasoning

Groups demonstrated sophisticated collaborative reasoning in their reflections. Several described extended deliberation over whether to defend Chen's position, ultimately distinguishing between the validity of Chen's ethical convictions and the problematic methods of secrecy and unauthorized access through which those convictions were enacted. Students also articulated metacognitive awareness of the assignment's structure, noting that nearly every aspect of the case could be argued persuasively from multiple sides and that the ethical frameworks themselves could be marshaled to support opposing conclusions. This recognition indicates readiness for professional contexts requiring both ethical judgment and legal analysis capabilities.

### Disciplinary Writing Development

Analysis of student written submissions revealed significant growth in disciplinary writing capabilities. In earlier assignments, groups often separated ethical, legal, and policy analyses into discrete sections with minimal integration. As the class progressed and collaborative negotiation within their groups emerged, students learned to weave these perspectives together. Groups also submitted a reflective summary describing their decision-making process, which revealed how productive disagreement led to more sophisticated analysis. One group's process exemplified this development: their initial draft presented each ethical framework in isolation, but their final submission wove utilitarian, deontological, and legal analyses together, arguing that potential societal benefits could not override the contractual and statutory obligations that the EEA was designed to protect.

Students also developed competency in citation practices specific to legal and policy writing, learning to reference specific sections of the relevant federal statutes, quote directly from case artifacts as evidence, and distinguish between descriptive summary and analytical argumentation.

## Reflection and Broader Applications

Reflecting on the EXODUS implementation, I found that artifact-based collaborative learning created investigative capabilities I had not achieved through previous case study implementations. Students moved from viewing legal analysis as an external constraint to embracing it as integral to ethical reasoning. Initial student frustration gave way to intellectual engagement I had rarely observed in traditional assignments.

Several challenges warrant consideration. The 75-minute in-class synthesis session creates productive urgency mirroring workplace decision-making, but some groups rushed through complex analytical tasks. Group dynamics also presented challenges as teams navigated competing viewpoints. Conflict generated productive discourse in most cases, but some groups struggled to synthesize divergent perspectives, suggesting the need for additional scaffolding or prerequisite collaborative learning experiences.

The structured collaborative approach offers potential for transfer across disciplines requiring complex professional reasoning. Importantly, collaborative learning environments function as social learning systems (Wenger, 2000) that can provide more equitable access to professional reasoning skills. Students from diverse backgrounds contribute unique perspectives while developing shared analytical competencies through participation. Technical programs in engineering, computer science, and health sciences face similar challenges preparing students for interdisciplinary professional contexts.

Writing Across the Curriculum programs (Kiefer et al., 2000–2021) can leverage this approach because it explicitly develops disciplinary writing capabilities through authentic genres: investigative reports synthesizing documentary evidence, legal memoranda analyzing statutory requirements, ethical analyses using philosophical frameworks, and policy recommendations with implementation strategies. The methodology creates a replicable framework for courses requiring investigative reasoning and evidence-based synthesis. Instructors interested in developing their own immersive case study materials can find detailed guidance and resources in an [open educational resource](#) I have developed for this purpose (Straight, 2025b).

A public health course, for instance, might present students with epidemiological data, interview transcripts from affected community members, internal communications from health officials, and media coverage of a disease outbreak. Groups could determine whether institutional responses reflected appropriate precaution or excessive intervention while developing policy recommendations for future incidents. The approach transfers readily to scenarios involving privacy regulations, artificial intelligence governance, digital rights, or any domain where professionals must interpret documentary evidence, apply contested frameworks, and develop defensible recommendations amid uncertainty.

This artifact-based collaborative approach demonstrates that technical students can develop sophisticated ethical and legal analysis skills when provided with primary source materials requiring investigative reasoning across multiple analytical frameworks. Students develop disciplinary writing skills when those skills are embedded in meaningful professional contexts rather than taught as isolated competencies. As cybersecurity education evolves to meet emerging challenges in artificial intelligence governance and global technology policy, artifact-based collaborative learning provides a foundation for developing the investigative reasoning and collaborative synthesis capabilities essential for effective professional practice.

---

## ASSIGNMENT

### EXODUS Collaborative Writing Assignment

#### The Case

Alex Chen is a quantum computing engineer at Quantum Frontier, a leading AI company with government contracts in defense and intelligence. After five years of high-impact work on Project Daedalus, the company's flagship quantum machine-learning initiative, Chen accepts a position at NexGen Cybernetics, a competitor known for an open-source, collaborative approach to AI development.

Before departing, Chen copies portions of the quantum AI algorithms she worked on at Quantum Frontier to personal cloud storage. Her stated intent, later recorded in her exit interview, centers on two threads: using some material as a portfolio piece, and continuing to develop algorithms she feels personally invested in. Quantum Frontier detects the exfiltration. The FBI investigation that follows produces charges under the Computer Fraud and Abuse Act (CFAA) and the Economic Espionage Act (EEA).

The case itself consists of primary source artifacts rather than a summarized narrative: internal memos, encrypted chat logs, FBI investigation reports, exit interview transcripts, legal strategy documents, and news coverage. Your task is to reconstruct meaning across these artifacts and arrive at a defensible position on the ethical, legal, and policy dimensions of what happened.

### Before the Collaborative Session

Read the entire EXODUS case independently, including all artifacts. As you read, compose brief notes identifying key evidence and your initial analytical observations. These notes are low-stakes and ungraded, but your group will rely on them during the collaborative session. Students who arrive having only skimmed tend to become passengers in their groups rather than contributors.

### Phase 1: In-Class Collaborative Synthesis (75 minutes)

Form self-selected groups of three to four students. Over the course of a single 75-minute in-class session, work through the six analytical tasks below. You do not need to tackle them in order, but do not tackle Task 6 (policy development) until at least three of the prior tasks are substantially engaged. Policy recommendations produced without grounding in ethical and legal analysis tend to be superficial.

#### The Six Analytical Tasks

1. **Ethical Framework Application.** Apply consequentialist, deontological, and virtue ethics frameworks to evaluate Chen's actions. Explain how each framework might yield competing conclusions depending on interpretive emphasis. Resist the temptation to treat frameworks as answer keys.
2. **Stakeholder Analysis.** Conduct a comprehensive stakeholder analysis identifying all affected parties. Consider Chen's former colleagues at Quantum Frontier, the two companies, Chen herself, the broader public who might benefit from or be harmed by AI applications, and any relevant institutional actors (government agencies, the scientific community, investors).
3. **Legal Analysis.** Determine potential legal violations under CFAA, EEA, ITAR, and EAR. Evaluate whether Chen's actions meet the statutory elements of each, attending to ambiguities in "authorization," "trade secret," and intent. Note where the facts meet the statutory elements cleanly and where they do not.
4. **Ethics of Military AI.** Analyze the ethics of military artificial intelligence development, as raised in Chen's exit interview concerns. Consider benefits, risks, and the ethical responsibilities of AI researchers and the companies that employ them.
5. **Corporate Response Evaluation.** Evaluate the corporate response to the alleged data exfiltration through deontological and social contract theory lenses. Examine whether institutional actions reflect agreements that rational individuals would accept as fair.
6. **Policy Development.** Develop three organizational policy recommendations (addressing institutional practice, not regulatory or legislative proposals) with implementation analysis. Each recommendation should name the ethical framework grounding it, describe challenges in implementation, and address how it balances competing stakeholder interests.

The session ends with brief oral presentations of one to two minutes per group, sharing findings and exposing your group to alternative interpretations from others. These presentations are formative and ungraded.

### Phase 2: Collaborative Written Analysis

Your group produces a **collaborative written analysis of 900 to 1200 words, due at the end of**

**the module.** The written analysis must demonstrate integrated mastery of multiple disciplinary writing conventions:

- Legal analysis citing specific statutory provisions
- Ethical argumentation using philosophical frameworks
- Policy writing with implementation considerations

Work exclusively with the case artifacts. External research is neither required nor expected. The analytical challenge is documentary interpretation, not literature review.

Your group organizes the writing process autonomously. Some groups divide by framework, others by task, others draft collectively. There is no required approach, but there is a required outcome: the final document should read as an integrated argument rather than stitched-together individual sections.

### *Collaborative Process Reflection*

Alongside your analysis, each group submits a brief **250-word reflection** describing:

- Your collaborative process: how responsibilities were sorted, how disagreements were navigated
- What each member contributed
- How the collaboration shaped your group's thinking

This reflection is not counted toward the 900 to 1200 word limit of the analysis. Write it honestly. It helps the evaluator understand your process and serves as a check against uneven contribution.

### *Assessment Rubric*

The written analysis is assessed across six weighted dimensions (Table 1).

What distinguishes excellent work from adequate work is sophistication, not accuracy. Adequate submissions apply frameworks mechanically and treat the tasks as independent questions with independent answers. Excellent submissions demonstrate nuanced understanding of how a single framework can support competing conclusions depending on which stakeholders and duties the analysis foregrounds. Excellent submissions also show evidence of genuine deliberation: passages where the group visibly considered an alternative position and explained why they moved past it, rather than presenting the final position as the only defensible one.

### *A Note on the Work*

This assignment is demanding. It asks you to hold three frameworks, two statutes, six analytical tasks, and a full stakeholder landscape in productive tension at once. The case is designed to resist easy convergence. If your group reaches a unified position early, something has probably gone wrong: you have likely settled on a single framework and are deriving your other answers from its logic rather than treating the tasks as independent probes.

The gap between what is legal and what is ethically defensible is not a bug in the case but a feature. Professionals in cybersecurity governance navigate contested interpretations rather than apply predetermined formulas. This assignment asks you to practice that navigation.

## Notes

<sup>1</sup> An asynchronous online version of the course uses different pedagogical approaches for collaborative work.

**Table 1.** Assessment rubric for written analysis

| Dimension                                                              | Weight | What the evaluator is looking for                                                                                                                                                                                                                            |
|------------------------------------------------------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multi-stakeholder analysis                                             | 25%    | <ul style="list-style-type: none"> <li>• Depth and breadth of stakeholder identification</li> <li>• Sophistication of handling competing legitimate interests.</li> </ul>                                                                                    |
| Synthesis and integration of perspectives                              | 20%    | <ul style="list-style-type: none"> <li>• Integration of ethical, legal, and policy analysis as woven argument rather than discrete sections</li> <li>• Recognition that frameworks yield competing conclusions depending on interpretive emphasis</li> </ul> |
| Policy development with implementation pathways                        | 20%    | <ul style="list-style-type: none"> <li>• Quality of organizational policy recommendations</li> <li>• Grounding in identified ethical frameworks</li> <li>• Implementation analysis including challenges and trade-offs</li> </ul>                            |
| Evidence of genuine collaborative process                              | 15%    | <ul style="list-style-type: none"> <li>• Reflection quality</li> <li>• Evidence of productive disagreement, shared intellectual engagement, and equitable contribution</li> </ul>                                                                            |
| Understanding of technology transfer and strategic protection concepts | 15%    | <ul style="list-style-type: none"> <li>• Accurate grasp of CFAA and EEA elements as applied to ambiguous facts</li> <li>• Recognition that decades-old statutes may not anticipate modern technology practices</li> </ul>                                    |
| Writing quality including proper citation practices                    | 5%     | <ul style="list-style-type: none"> <li>• Clarity, organization, mechanics</li> <li>• Correct citation of artifacts and statutes</li> <li>• Distinction between descriptive summary and analytical argumentation</li> </ul>                                   |

## Supplementary Material

For supplementary material accompanying this paper, including a PDF facsimile of the assignment description formatted as the author(s) presented it to students, please visit <https://doi.org/10.31719/pjaw.v10i2.280>.

## References

- Bean, J. C. (2011). *Engaging ideas: The professor's guide to integrating writing, critical thinking, and active learning in the classroom* (2nd ed.). Jossey-Bass.
- Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2020). Holistic cyber education. In G. Austin (Ed.), *Cyber security education: Principles and policies* (pp. 160–172). Routledge.
- Christensen, C. R., Garvin, D. A., & Sweet, A. (Eds.). (1991). *Education for judgment: The artistry of discussion leadership*. Harvard Business School Press.
- Computer Fraud and Abuse Act of 1986. 18 U.S.C. § 1030 (1986). <https://www.law.cornell.edu/uscode/text/18/1030>
- Economic Espionage Act of 1996. Pub. L. 104-294. (1996). <https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf>
- Export Administration Regulations. 15 C.F.R. § 734.8 (2023). <https://www.ecfr.gov/current/title-15/section-734.8>

- Frusci, J. (2024). Integrating humanities into cybersecurity education: Enhancing ethical, historical, and sociopolitical understanding in technical training. *Journal of Cybersecurity Education, Research and Practice*, 2024(1). <https://doi.org/10.62915/2472-2707.1209>
- Herreid, C. F. (2007). *Start with a story: The case study method of teaching college science*. NSTA Press.
- Herreid, C. F., & Schiller, N. A. (2013). Case studies and the flipped classroom. *Journal of College Science Teaching*, 42(5), 62–66.
- International Traffic in Arms Regulations. 22 C.F.R. § 120.34 (2023). <https://www.ecfr.gov/current/title-22/section-120.34>
- Kiefer, K., Palmquist, M., Carbone, M. C., & Melzer, D. (2000–2021). *An introduction to Writing Across the Curriculum*. <https://wacclearinghouse.org/repository/teaching/intro/>
- Mahdi, O. R., Nassar, I. A., & Almuslamani, H. A. (2020). The role of using case studies method in improving students' critical thinking skills in higher education. *International Journal of Higher Education*, 9(2), 297–308. <https://doi.org/10.5430/ijhe.v9n2p297>
- Manjikian, M. (2022). *Cybersecurity ethics: An introduction* (2nd ed.). Routledge. <https://doi.org/10.4324/9781003248828>
- Straight, R. (2025a). *Cyber dimensions: Immersive case studies across digital domains* (1st ed.). Kendall Hunt. <https://he.kendallhunt.com/product/cyber-dimensions-immersive-case-studies-across-digital-domains>
- Straight, R. (2025b). *Cyber dimensions: OER toolkit*. <https://ryanstraight.github.io/cyber-dimensions-oer/>
- Wenger, E. (2000). Communities of practice and social learning systems. *Organization*, 7(2), 225–246. <https://doi.org/10.1177/135050840072002>