[This file is supplemental material to Straight, *Grey Areas and Egress: Artifact-Based Collaborative Learning in Cybersecurity Ethics*, prompt 10.2 (2026), doi: 10.31719/pjaw.v10i2.280]

EXODUS Collaborative Writing Assignment

Project Overview: Full Assignment Description, Rubric, and Materials

Ryan M. Straight

Table of contents

Overview . . . 1
Course Context . . . 2
Learning Objectives . . . 2
Assignment Structure . . . 3
Assessment Rubric . . . 4
Materials . . . 5
Adaptation to Other Contexts . . . 5
Sources . . . 6

This supplemental file accompanies Ryan M. Straight, "Grey Areas and Egress: Artifact-Based Collaborative Learning in Cybersecurity Ethics," Prompt: A Journal of Academic Writing Assignments, Issue 10.2 (2026). It describes the EXODUS Collaborative Writing Assignment as delivered in CYBR 329: Cyber Ethics at the University of Arizona. The reflective essay presents an excerpted version of the assignment; this document provides the full project overview with rubric and instructional context for adoption or adaptation.

Overview

The EXODUS Collaborative Writing Assignment asks groups of undergraduate cybersecurity ethics students to synthesize evidence across artifact-based primary source materials, apply ethical and legal frameworks to an ambiguous professional dilemma, and produce a collaborative written analysis that integrates philosophical reasoning, statutory analysis, and policy development.

The case centers on Alex Chen, a quantum computing engineer who allegedly transferred proprietary code to a competitor. The case takes its name from Chen's departure: an act of egress whose ethical and legal dimensions prove far from straightforward. Students work exclusively from the case's primary source artifacts (internal memos, encrypted chat logs, FBI investigation reports, exit interview transcripts, legal strategy documents, and news coverage) rather than from pre-digested narrative, reconstructing meaning through careful documentary analysis.

The full EXODUS case, including every artifact referenced in the reflective essay, appears in *Cyber Dimensions: Immersive Case Studies Across Digital Domains* (Straight, 2025; Kendall Hunt).

Instructors who wish to run this assignment as described here will need the textbook. EXODUS is not open-access and is available only through Kendall Hunt.

Two companion open resources support related but distinct adopter paths. The Cyber Dimensions OER Toolkit provides the methodological foundations for authoring artifact-based cases in any domain. It is the resource for instructors who want to build their own cases rather than adopt EXODUS. The Cyber Dimensions Case Study Demo is a fully worked implementation (the CIRCUIT case, a cybersecurity incident affecting Ribera Municipal Utilities) that shows the complete behind-the-scenes setup in rendered form, with all Quarto source files, the YAML worldbuilding system, and the rendering pipeline available at the source repository. Adopters interested in replicating the production pipeline should start there.

Course Context

Element	Detail
Course	CYBR 329: Cyber Ethics
Institution	College of Information Science, University of Arizona
Level	Upper-division (juniors and seniors)
Enrollment	~36 students per section
Format	In-person, twice weekly, 15-week semester
Placement	Approximately midway through the semester, after foundational work in consequentialist, deontological, and virtue ethics frameworks and relevant cybersecurity law

Learning Objectives

On completion, students will be able to:

1. Apply consequentialist, deontological, and virtue ethics frameworks to an ethically ambiguous professional scenario, demonstrating that frameworks are analytical tools rather than answer keys.
2. Conduct multi-stakeholder analysis of a technology-transfer dilemma, integrating perspectives of individual actors, institutions, professional communities, and the public.
3. Apply relevant federal statutes (Computer Fraud and Abuse Act, Economic Espionage Act, ITAR, EAR) to ambiguous factual circumstances and evaluate where legal frameworks align with or diverge from ethical reasoning.
4. Develop organizational policy recommendations that address institutional practice, grounded in identified ethical tensions and accompanied by implementation analysis.
5. Produce integrated collaborative writing that synthesizes ethical, legal, and policy analysis across multiple disciplinary genres rather than presenting them as discrete sections.
6. Reflect metacognitively on the collaborative reasoning process, articulating how productive disagreement contributed to analytical sophistication.

Assignment Structure

The assignment unfolds across two phases, preceded by individual preparation.

Pre-Class Preparation (Individual)

Prior to the collaborative session, students independently:

- Read the entire EXODUS case, including all artifacts (internal memos, chat logs, investigation reports, interview transcripts, legal documents, and news coverage).
- Compose low-stakes written notes identifying key evidence and initial analytical observations.

This preparatory writing serves three purposes: students process documentary information before discussion, sketch interpretations they will later defend or revise, and produce reference materials for the collaborative session.

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

Self-selected groups of three to four students convene for a single 75-minute in-class session to work through six analytical tasks. The instructor circulates among groups, fielding questions, redirecting conversations that narrow prematurely on a single framework, and posing complicating questions when consensus forms too quickly.

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.
2. **Stakeholder Analysis.** Conduct a 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. **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.
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 companies.
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 rather than regulatory 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 concludes with brief oral presentations of one to two minutes per group, sharing findings

and exposing students to alternative interpretations. These presentations receive formative feedback rather than formal grades, encouraging intellectual risk-taking during synthesis.

Phase 2: Collaborative Written Analysis (Take-home)

Following the in-class session, groups produce a **collaborative written analysis of 900 to 1200 words, due the following Sunday.** 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

Groups work exclusively with the provided case artifacts. External research is neither required nor expected; the analytical challenge is documentary interpretation, not literature review.

Groups organize the collaborative writing process autonomously. Some groups divide by framework, others by analytical task, others draft collectively. To ensure accountability, each group submits a brief collaborative process reflection alongside the analysis.

Collaborative Process Reflection

A **250-word reflection** accompanies the written analysis, describing:

- The group's collaborative process (how responsibilities were sorted, how disagreements were navigated)
- What contributions each member made
- How the collaboration shaped the group's thinking

This reflection is not counted toward the 900 to 1200 word limit of the analysis. It serves as a check against uneven contribution and makes the group's metacognitive awareness visible to the evaluator.

Assessment Rubric

The written analysis is assessed across six weighted dimensions:

Dimension	Weight	Description
Multi-stakeholder analysis	25%	Depth and breadth of stakeholder identification and analysis. Sophistication of handling competing legitimate interests.
Synthesis and integration of perspectives	20%	Integration of ethical, legal, and policy analysis as woven argument rather than discrete sections. Recognition that frameworks yield competing conclusions depending on interpretive emphasis.

Dimension	Weight	Description
Policy development with implementation pathways	20%	Quality of organizational policy recommendations. Grounding in identified ethical frameworks. Implementation analysis including challenges and trade-offs.
Evidence of genuine collaborative process	15%	Reflection quality. Evidence of productive disagreement, shared intellectual engagement, and equitable contribution.
Understanding of technology transfer and strategic protection concepts	15%	Accurate grasp of CFAA and EEA elements as applied to ambiguous facts. Recognition that decades-old statutes may not anticipate modern technology practices.
Writing quality including proper citation practices	5%	Clarity, organization, mechanics. Correct citation of artifacts and statutes. Distinction between descriptive summary and analytical argumentation.

What distinguishes excellent from adequate work is sophistication, not accuracy. Excellent submissions demonstrate nuanced understanding of how the same ethical framework can support competing conclusions. Adequate submissions apply frameworks mechanically, without recognizing their interpretive flexibility. The distinction reflects how expertise actually functions in cybersecurity governance. Professionals navigate contested interpretations rather than apply predetermined formulas.

Materials

Required

- EXODUS case from *Cyber Dimensions: Immersive Case Studies Across Digital Domains* (Straight, 2025; Kendall Hunt). Not open-access. Available only through the textbook.
- The relevant federal statutes (CFAA, EEA, ITAR, EAR) or faithful teaching summaries

Instructor-provided

- Case artifacts in hard copy or digital packet for in-class annotation
- Brief guidance on productive collaborative practices (approximately ten minutes at the start of Phase 1, emphasizing research findings that group case-study discussions outperform individual analysis for developing critical thinking)

Adaptation to Other Contexts

The structural template (primary source artifacts, six-task analytical synthesis, collaborative writing, and process reflection) transfers readily to any domain where professionals must interpret documentary evidence, apply contested frameworks, and develop defensible recommendations amid

uncertainty. Examples include public health outbreak scenarios, privacy regulation disputes, artificial intelligence governance cases, and digital rights conflicts. The reflective essay accompanying this project discusses transfer pathways in more detail.

For instructors seeking to develop their own artifact-based cases, the Cyber Dimensions OER Toolkit provides authoring guidance, pedagogical foundations, and templates. The Cyber Dimensions Case Study Demo is a complete worked example showing the CIRCUIT case in rendered form, with its full Quarto and YAML source available for inspection or forking.

Sources

Straight, R. (2025). *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. (2025). *Cyber Dimensions OER Toolkit* (methodology and authoring guidance for artifact-based case design). https://ryanstraight.github.io/cyber-dimensions-oer/

Straight, R. (2025). *Cyber Dimensions Case Study Demo* (complete worked implementation of the CIRCUIT case). Rendered site: https://ryanstraight.github.io/cyber-dimensions-demo/. Source repository: https://github.com/ryanstraight/cyber-dimensions-demo