Teaching Cyber Professionals to Think: Reframing Graduate Cyber Education via Mission Engineering

Timothy Shives
Naval Postgraduate School, Monterey, California, USA

timothy.shives@nps.edu

Abstract: Graduate cyber education has become increasingly effective at developing technical expertise, but the environments in which cyber professionals work often demand more than technical proficiency. Practitioners may be required to understand mission objectives, identify dependencies, reason about adversary behavior, advise nontechnical decision-makers, execute selected courses of action, and assess whether those actions produced the intended effect. This creates a curriculum-design challenge: technical competence remains essential, yet it must increasingly be applied within organizational and mission contexts. This paper proposes the Mission-Driven Cyber Education (MDCE) Framework, a conceptual curriculum architecture that adapts Mission Engineering principles to graduate cyber education. MDCE begins with the mission rather than the technology. Its five interconnected layers move through mission understanding; systems thinking and mission dependency analysis; adversary reasoning and decision-making under uncertainty; operational course-of-action development and execution; and mission assessment and organizational learning. The layers are iterative rather than sequential. Execution generates new information, assessment may change the understanding of the mission, and learners revisit earlier assumptions as conditions change. The framework was developed through a design science approach drawing on cyber education and workforce guidance, adult and experiential learning, professional military education, Mission Engineering, and reflective observations from graduate cyber mission-planning instruction. Those observations helped identify an instructional problem that motivated the framework: technically proficient students may move quickly toward feasible technical solutions before fully defining the mission or organizational problem they are trying to solve. MDCE is presented as a conceptual design artifact, not as an empirically validated instructional intervention. Its contribution lies in using Mission Engineering as the organizing logic for connecting established educational approaches to the demands of graduate cyber practice. The paper illustrates how the framework may be applied in mission-planning instruction and identifies opportunities for comparative, mixed-method, and longitudinal research to test whether this approach improves systems thinking, operational reasoning, interdisciplinary communication, and transfer of learning.

Keywords*:* Cyber Education, Mission Engineering, Curriculum Design, Systems Thinking, Experiential Learning, Design Science Research.

1. Introduction

Over the past two decades, cyberspace has moved from a specialized technical domain to a central element of national security, economic resilience, and organizational performance. Universities have responded with increasingly sophisticated graduate programs in software engineering, network defense, malware analysis, digital forensics, cloud security, vulnerability research, and cyber operations. Workforce initiatives such as the Workforce Framework for Cybersecurity (NICE Framework) and *Cybersecurity Curricula 2017* have also helped define common expectations for cyber work roles and academic preparation (National Institute of Standards and Technology, 2020; Joint Task Force on Cybersecurity Education, 2017).

This investment has been successful. Graduate cyber education produces technically capable professionals. The challenge is that the profession has continued to evolve. Cyber professionals are often expected to contribute to mission planning, organizational resilience, interdisciplinary collaboration, and senior decision-making rather than operate solely as technical specialists. In military organizations, they must understand mission objectives, dependencies, authorities, adversary behavior, timing, and operational risk. Comparable demands exist in civilian sectors, where technical decisions may have to be balanced against business continuity, patient care, public safety, financial risk, or other mission-critical outcomes. Technical expertise remains essential, but professional effectiveness increasingly depends on the ability to apply that expertise within a larger organizational context.

This raises a basic educational question: Are graduate cyber programs preparing students primarily to master cyber technologies, or are they also preparing them to employ those technologies effectively within the organizations and missions they support?

Many graduate cyber programs retain an instructional architecture inherited from computer science, information technology, and engineering. Courses are commonly organized around technical domains, with integration expected to occur later through capstones or professional experience. That model has produced highly capable engineers and cybersecurity practitioners. It may be less deliberate, however, in developing the

systems thinking and operational judgment required when cyber professionals must solve problems that extend beyond the network itself.

Educational theory suggests that context matters. Adult learners benefit when instruction is relevant to problems they recognize from professional practice (Knowles, 1984). Experiential learning emphasizes the interaction among experience, reflection, conceptual understanding, and application (Kolb, 1984), while situated learning argues that expertise develops through participation in authentic professional contexts (Lave and Wenger, 1991). Recent cybersecurity education research similarly points to experiential approaches as a way to narrow the gap between classroom preparation and professional practice (Bertone, Wagner and Pauli, 2025).

Graduate cyber mission-planning instruction provides a practical illustration of the problem. Technically proficient students may move quickly toward feasible solutions before fully defining the mission problem those solutions are intended to address. Their recommendations can be technically sound while remaining incompletely aligned with mission priorities, operational constraints, or the decisions leaders actually have to make. The issue is not a lack of technical competence. It is how that competence is framed, organized, and applied.

Mission Engineering offers a useful way to rethink this curriculum architecture. It begins with the mission problem and examines how systems, people, processes, dependencies, and capabilities contribute to mission outcomes (Office of the Under Secretary of Defense for Research and Engineering, 2023). Applied to education, the same logic suggests that students should first understand the mission and then develop and apply technical expertise within that context.

This paper develops that idea through the Mission-Driven Cyber Education (MDCE) Framework. MDCE does not claim experiential learning, systems thinking, or scenario-based instruction as new ideas. Its contribution is in how those ideas are organized. Mission Engineering supplies the organizing logic: students begin with the mission, examine dependencies and adversary behavior, develop and execute courses of action, and assess whether those actions produced the intended effect.

The paper makes three contributions. First, it identifies a curriculum-design gap between technically organized graduate cyber education and professional environments where cyber expertise must be integrated with mission objectives, organizational dependencies, adversary behavior, and decision-making. Second, it introduces MDCE as a mission-centered curriculum architecture that connects established educational approaches to the demands of graduate cyber practice. Third, it establishes a research agenda for examining whether this architecture improves systems thinking, operational reasoning, interdisciplinary communication, and transfer of learning.

2. Literature Review and Theoretical Foundations

2.1 Graduate Cyber Education

Graduate cyber programs developed largely from computer science, information technology, software engineering, and information assurance. As the field matured, curricula expanded from programming, networking, operating systems, and cryptography to malware analysis, cloud security, digital forensics, vulnerability research, cyber threat intelligence, and offensive and defensive cyber operations. The NICE Framework and *Cybersecurity Curricula 2017* helped formalize this development by defining work roles, knowledge, skills, and curriculum expectations across the field (National Institute of Standards and Technology, 2020; Joint Task Force on Cybersecurity Education, 2017).

These developments strengthened cyber education, particularly in technical depth and professional standardization. The problem examined here is different. Many cyber practitioners now work alongside organizational leaders, intelligence analysts, mission planners, engineers, legal advisors, and risk managers. In those settings, technical competence is necessary but not sufficient. Practitioners must also be able to explain why a technical issue matters, what mission functions depend on a system, and how a technical decision may affect broader organizational outcomes.

2.2 Adult Learning and Authentic Professional Practice

Adult learning theory helps explain why context matters. Knowles (1984) argues that adult learners bring prior experience into the classroom and are motivated by learning that has immediate professional relevance. Kolb (1984) describes learning as an iterative process linking experience, reflection, conceptual understanding, and active experimentation. Situated learning makes a related point: expertise develops through participation in authentic communities of practice rather than through decontextualized knowledge alone (Lave and Wenger, 1991).

Recent cybersecurity education research makes a similar argument. Experiential approaches can bring students closer to the uncertainty and complexity of professional practice, particularly when learners are required to make decisions rather than merely demonstrate technical procedures (Bertone, Wagner and Pauli, 2025).

The educational implication is straightforward. A technically correct answer may still be a poor professional answer if it ignores context, timing, risk, or the larger objective. Graduate cyber education therefore has to develop judgment alongside technical skill.

2.3 Professional Military Education and Operational Thinking

Professional military education provides a useful comparison because it deliberately connects functional expertise to broader operational reasoning. Current officer professional military education policy emphasizes outcomes-based education, critical and strategic thinking, integrated operations, and performance in changing operational environments (Chairman of the Joint Chiefs of Staff, 2024).

That comparison is especially relevant in graduate military cyber education. Cyber professionals may have to understand commander intent, mission dependencies, authorities, adversary adaptation, timing, and organizational risk while communicating with leaders whose expertise lies outside the cyber domain. In that environment, technical skill cannot be separated from planning and decision-making.

The broader lesson is that operational judgment does not have to be deferred until after graduation. It can be developed while students are still building technical competence, provided the curriculum consistently places that competence inside realistic decision contexts.

2.4 Mission Engineering as an Educational Paradigm

Mission Engineering provides the organizing concept that connects these ideas. The Department of Defense *Mission Engineering Guide* describes an interdisciplinary process that begins with a mission problem or opportunity, characterizes the mission and its measures, examines mission architectures and dependencies, and evaluates alternative approaches to improve mission outcomes (Office of the Under Secretary of Defense for Research and Engineering, 2023). Its focus is not on optimizing individual systems in isolation, but on understanding how multiple capabilities contribute to the mission as a whole.

Applied to graduate cyber education, this changes the sequence of the learning problem. Instead of beginning with technology and asking students to integrate it later, instruction can begin with the mission and then ask what technical capabilities, dependencies, and decisions matter within that context.

Mission Engineering therefore serves here as more than another topic to be taught. It provides a way to organize the curriculum itself.

2.5 Critical Synthesis and Gap

The literature offers several useful pieces of the problem, but they do not yet form a complete curriculum architecture for graduate cyber education. Cyber workforce and curriculum frameworks provide a useful account of competencies and professional roles, but they say much less about how those competencies should be organized around a mission problem (Joint Task Force on Cybersecurity Education, 2017; National Institute of Standards and Technology, 2020).

Adult, experiential, and situated learning address a different part of the problem. They explain why context, reflection, and professional relevance matter, but they do not by themselves provide a structure for connecting cyber decisions to mission outcomes (Knowles, 1984; Kolb, 1984; Lave and Wenger, 1991). Professional military education contributes an emphasis on judgment and integrated decision-making, while Mission Engineering offers a way to examine how systems and capabilities contribute to mission performance.

The gap, then, is less about the absence of useful educational concepts than about how those concepts are organized for graduate cyber practice. Existing approaches support technical competence, authentic learning, systems thinking, and professional judgment, but they do not explicitly structure learning from mission understanding through dependency analysis, adversary reasoning, course-of-action development and execution, and mission assessment.

MDCE addresses that gap by using Mission Engineering as the curriculum architecture rather than simply as another instructional topic. Its contribution is not that any one of these educational ideas is new. The contribution is the way they are connected around a mission-centered cycle in which students interpret technical choices through organizational context, carry selected courses of action into execution, and assess whether those actions produced the intended effect.

3. Research Approach and Framework Development

This study uses a design science approach to address a curriculum-design problem in graduate cyber education. The aim is not to test a completed instructional intervention, but to develop and theoretically ground a conceptual framework that better aligns technical cyber education with mission-oriented professional practice. The guiding question is how graduate cyber education might be reorganized to prepare students for environments where technical expertise must be integrated with organizational decision-making.

Design science is appropriate when the intended contribution is an artifact such as a framework, model, method, or process designed to improve practice (Hevner et al., 2004). In this study, that artifact is the Mission-Driven Cyber Education Framework. MDCE is intended as an organizing architecture rather than a prescribed course design. The framework was developed through five related stages. First, the educational problem was defined as a mismatch between technically organized cyber curricula and professional environments that demand systems thinking, interdisciplinary collaboration, and mission-oriented decision-making. Second, four bodies of knowledge were examined for what they contributed to that problem: cyber education and workforce guidance, adult and experiential learning, professional military education, and Mission Engineering. Third, those sources were used to derive a set of design requirements for the framework.

Those requirements were practical as well as theoretical. MDCE needed to preserve technical rigor while beginning with mission context rather than technology alone. It also needed to expose learners to interdependencies, uncertainty, adversary adaptation, comparison among alternative courses of action, execution, and assessment tied to mission outcomes. These requirements were then organized into five interconnected layers: mission understanding; systems thinking and dependency analysis; adversary reasoning; operational course-of-action development and execution; and mission assessment and organizational learning. The intent was not to create a five-step checklist, but to establish a structure that could be revisited as new information changes the problem.

Reflective observations from graduate cyber mission-planning instruction provided a practical check on that structure. One recurring instructional problem was that technically proficient students could move quickly toward feasible solutions before fully defining the mission or organizational problem. Those observations helped reinforce the decision to place mission understanding at the beginning of the framework and to make reassessment part of the cycle.

The observations are not treated as empirical findings or as evidence that MDCE is effective. They were not collected through a formal research protocol, and they do not establish causal relationships. Their role in this study is narrower: they helped identify and refine the design problem the framework is intended to address.

MDCE should therefore be understood as a conceptual design artifact rather than a validated instructional model. Its current value lies in its theoretical coherence, practical relevance, and ability to support future empirical investigation.

4. Mission-Driven Cyber Education (MDCE) Framework

The MDCE Framework adapts Mission Engineering principles to graduate cyber curriculum design. Applied to education, the central shift is from asking *What technology should students learn?* to asking *What mission must students understand, and what technical capabilities are required to support it?*

MDCE does not replace traditional technical education. Programming, networking, software engineering, cryptography, cloud computing, malware analysis, digital forensics, secure systems design, and cyber operations

remain foundational. The difference is the context in which students organize and apply that knowledge. Technical competence remains essential, but learners repeatedly connect technical decisions to mission objectives, constraints, and consequences.

The framework consists of five interconnected layers: mission understanding; systems thinking and mission dependency analysis; adversary reasoning and decision-making under uncertainty; operational course-of-action development and execution; and mission assessment and organizational learning. Although the layers are presented in sequence for explanation, they are not intended to operate as a linear checklist. Each can reshape the others as new information becomes available.

Mission dependencies may change the way the original problem is understood. Adversary analysis may reveal a dependency or vulnerability that was not apparent at the outset. Execution may expose constraints that require an earlier course of action to be reconsidered. Assessment, in turn, feeds new information back into mission understanding. Figure 1 represents this iterative architecture.

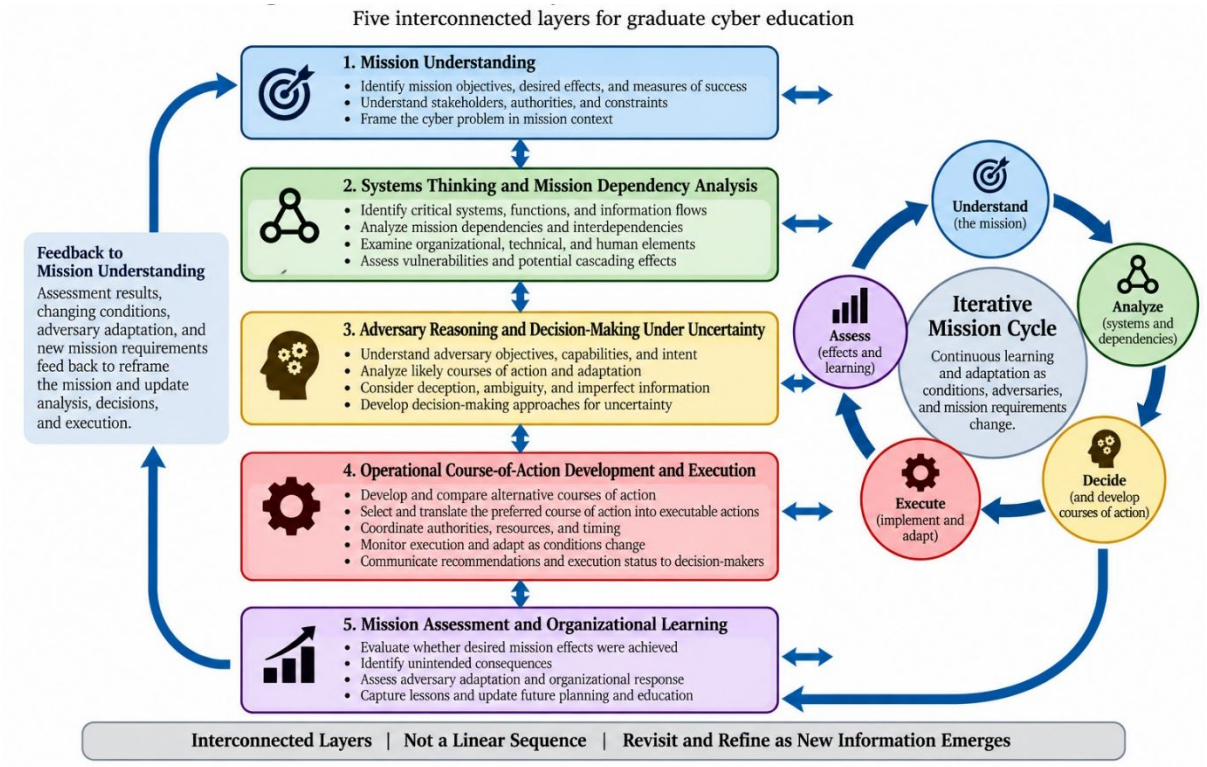

Figure 1: Mission-Driven Cyber Education (MDCE) Framework

Figure 1 illustrates the recursive relationship among the five layers. Mission understanding frames the problem. Systems thinking identifies the dependencies through which the mission is enabled. Adversary reasoning introduces competition, adaptation, and uncertainty. Course-of-action development translates that understanding into choices for decision and execution, while mission assessment evaluates the effects that follow.

Within MDCE, execution remains part of Layer 4, marking the transition from selecting a course of action to implementing, monitoring, and adapting it as conditions change. Assessment feeds what was learned back into the next cycle of mission understanding. The result is a pattern of understanding, analysis, decision, execution, assessment, and adaptation rather than a fixed five-step process.

4.1 Mission Understanding

The framework begins with a question that is often postponed in technically organized education: *What mission is the organization attempting to accomplish?* Before considering technologies, vulnerabilities, or architectures, students identify the supported mission, organizational objectives, relevant stakeholders, constraints, desired effects, and measures of success. Technical systems are then examined according to how they enable or constrain those outcomes.

Beginning with the mission changes how students frame the problem. Rather than asking which capability is most technically sophisticated, learners must determine which option best contributes to the desired outcome. This more closely reflects professional environments in which cyber practitioners are expected to explain not only what can be done technically, but why an action matters.

4.2 Systems Thinking and Mission Dependency Analysis

Once the mission is understood, students examine the systems and dependencies that enable it. Organizations depend on relationships among people, information, communications, software, infrastructure, logistics, governance, and external partners. Mission success therefore rarely depends on a single technical system.

Students move beyond cataloging assets and identify mission dependencies. They examine which systems and functions are critical to execution, where vulnerabilities create disproportionate risk, and how disruption in one component may produce cascading effects elsewhere. Systems thinking is useful here because it encourages attention to relationships and feedback rather than only linear cause-and-effect reasoning (Senge, 1990). A network, application, or infrastructure node matters, then, not simply because it is vulnerable, but because of the mission function it supports.

4.3 Adversary Reasoning and Decision-Making Under Uncertainty

Cyber professionals operate against intelligent adversaries who observe, learn, deceive, and adapt. The third layer therefore asks students to move beyond static technical analysis and consider the problem from an adversary perspective.

Students examine adversary objectives, likely courses of action, incentives, decision processes, deception, and possible responses to friendly action without assuming perfect information. Research on naturalistic decision-making emphasizes the importance of pattern recognition, context, experience, and adaptive judgment when professionals make decisions under uncertainty (Klein, 1998). This changes the educational problem. Cybersecurity is no longer treated simply as a contest between technologies. It becomes a competitive decision environment in which both sides can adapt.

4.4 Operational Course-of-Action Development

Mission understanding, dependency analysis, and adversary reasoning provide the basis for developing and executing operational courses of action. Students first compare alternatives according to mission effect, technical feasibility, organizational risk, authorities, available resources, timing, and anticipated adversary responses. The objective is not merely to identify what can be done technically, but to determine which course of action best supports the mission under the conditions presented.

Once a course of action is selected, the problem changes. Learners must determine how the selected option will be translated into executable tasks, coordinated across relevant organizations and capabilities, sequenced in time, and monitored as conditions change. Execution becomes a source of information rather than the endpoint of planning. Unexpected technical conditions, adversary responses, resource constraints, or changes in the supported mission may require the selected course of action to be modified or earlier assumptions to be revisited.

Communication remains central throughout this process. Cyber professionals routinely advise commanders, executives, planners, and other leaders who may not share their technical expertise. Students must translate technical analysis into language that supports decisions, communicate the selected course of action to those responsible for execution, and explain when changing conditions require adaptation. Reflective practice reinforces this process by requiring learners to revisit assumptions and modify recommendations as new information becomes available (Schön, 1983).

4.5 Mission Assessment and Organizational Learning

Execution does not complete the learning cycle. The fifth layer asks whether the selected and executed course of action produced the intended mission outcome. Students assess whether desired effects occurred, identify unintended consequences, consider adversary adaptation, and determine how results should influence subsequent decisions. Measures of technical performance remain relevant, but they are interpreted alongside measures of mission effectiveness.

This creates a feedback loop rather than a terminal assessment event. Students return to mission understanding, revise dependency analysis, reconsider adversary behavior, and develop or adapt courses of action as conditions change. The process parallels experiential learning by connecting action with reflection, conceptual understanding, and subsequent application (Kolb, 1984).

4.6 Curriculum Integration

The MDCE Framework represents an evolution of graduate cyber education rather than a replacement for its technical foundations. Its contribution is architectural: technical competence and operational reasoning develop together instead of being treated as separate stages of professional development. Mission understanding provides the organizing principle. Systems thinking connects technical components to organizational dependencies. Adversary reasoning introduces competition and uncertainty. Course-of-action development and execution connect technical feasibility to mission requirements, decision-making, coordination, and adaptation. Assessment closes the cycle by linking technical performance and operational execution to organizational effects and future learning.

The relationships among these layers are recursive. A change identified during mission assessment may require the original problem to be reframed. Adversary adaptation may force a new dependency analysis. Conditions encountered during execution may expose assumptions that require earlier stages to be revisited. The point is to develop a habit of continuous reassessment, not to teach students a fixed five-step procedure. The recurring question throughout the curriculum becomes simple: *How does this technical decision contribute to the mission?*

5. Illustrative Application in Graduate Cyber Mission Planning

The following example shows how the MDCE Framework can be applied in graduate cyber mission-planning instruction serving experienced military and government professionals. These observations serve a narrow purpose: to illustrate the instructional problem that helped motivate the framework and to show what the five layers can look like in practice. These observations emerged through reflective teaching practice rather than a formal research protocol. They were not systematically collected, coded, or analyzed as human-subject data, and they are not presented as evidence of instructional effectiveness.

Students in these courses often arrive with substantial technical and operational experience. When they are presented with realistic planning problems, one recurring instructional observation is that some move quickly toward technically feasible solutions before fully defining the mission problem. Given a compromised network, for example, students may initially focus on defensive countermeasures, remediation, or recovery. In offensive scenarios, attention may shift rapidly toward access, exploitation, and technical execution.

Those responses are technically reasonable. The instructional challenge is to move the first question from *What can cyber do?* to *What does the mission require?* Mission-driven instruction changes the sequence of the problem. Students first identify the supported mission, organizational objectives, constraints, stakeholder requirements, and measures of effectiveness. They then conduct mission dependency analysis to examine relationships among organizational functions, information flows, technologies, infrastructure, and human decision-makers. The discussion shifts from whether a vulnerability can be exploited to why a system matters, what mission functions depend on it, and what second-order effects may follow from disruption.

Scenario-based exercises provide the primary vehicle for applying this reasoning. The problems are deliberately constructed so that there is no single technically correct answer. Students must integrate intelligence, authorities, operational objectives, technical capabilities, and organizational constraints; compare possible courses of action; and justify a recommendation in terms of mission effect.

Where appropriate, the scenario then moves into execution. Students translate the selected course of action into coordinated actions, consider sequencing and resource requirements, respond to changing conditions, and revisit earlier assumptions as new information becomes available. Adversary reasoning adds another layer of complexity by forcing them to consider how an intelligent competitor may adapt, exploit dependencies, or respond to friendly action.

Communication and reflection are equally important. Students must translate technical analysis into language useful to commanders, executives, planners, legal advisors, and other decision-makers. Following planning and execution activities, they reconsider assumptions, unintended consequences, alternatives, and whether their recommendations actually supported the mission. This process connects action, reflection, and adaptation

(Kolb, 1984; Schön, 1983). These observations are best understood as practitioner reflections, not findings. They do not establish causal relationships or demonstrate that MDCE produces superior educational outcomes. They do, however, provide a practical illustration of how a mission-centered curriculum architecture can shape problem framing, decision-making, execution, communication, and reflection. Whether those changes produce measurable educational benefits remains a question for future empirical research.

6. Discussion and Limitations

The MDCE Framework addresses a curriculum-design problem, not a deficiency in technical cyber education. The question is how graduate programs can help students connect technical depth to the environments in which that knowledge will be used. MDCE therefore proposes a change in organization rather than a reduction in technical content. Mission context is introduced early and revisited as students move through analysis, decision-making, execution, and assessment.

Although the framework was developed primarily from graduate military cyber education, the underlying logic may have broader relevance in other mission-critical settings. Healthcare organizations must connect cybersecurity decisions to patient safety and clinical operations. Financial institutions balance cyber resilience with continuous business operations. Energy, transportation, manufacturing, and emergency-management organizations similarly depend on cyber professionals who understand both technical systems and the missions those systems support.

Those examples suggest possible transfer beyond defense, but they should not be treated as evidence that the framework will work equally well in every setting. That question remains empirical. MDCE is also not intended as a universal model for all cyber programs. Programs preparing cybersecurity researchers, software engineers, or highly specialized technical practitioners may reasonably prioritize disciplinary depth over broader mission-oriented integration. The framework is most relevant to programs preparing professionals for leadership, mission assurance, operational planning, organizational decision-making, and interdisciplinary roles in which cyber capabilities must be integrated with wider institutional objectives.

The study has several limitations. The framework was developed through conceptual analysis informed by educational theory, professional military education, Mission Engineering, cyber workforce guidance, and reflective practitioner observations. It was not developed or tested through a controlled empirical study. As a result, this paper cannot establish that MDCE produces better educational outcomes than other curriculum models.

Future research should test those claims directly. Comparative studies could examine whether mission-centered sequencing improves systems thinking, operational reasoning, interdisciplinary communication, and transfer of learning. Longitudinal research could follow graduates into professional assignments to determine whether the habits developed in the classroom persist in practice. Mixed-method studies could combine classroom observation, reflective writing, performance assessments, interviews, and employer feedback to examine both measurable outcomes and how students experience the curriculum.

MDCE is not intended as a new learning theory, nor does this paper argue that Mission Engineering is the only useful way to organize cyber education. The narrower claim is that Mission Engineering offers a useful architecture for connecting established educational approaches to the mission-oriented demands of graduate cyber practice. That is the contribution this paper is making: not replacing technical education, but providing a structure for helping students carry technical expertise into mission analysis, decision-making, execution, and assessment.

7. Conclusion

Graduate cyber education has successfully answered an important first-generation challenge: how to prepare technically competent professionals for an increasingly digital world. The emerging challenge is different. Cyber professionals are now expected not only to secure, exploit, and understand technical systems, but also to determine how those systems and capabilities contribute to organizational missions.

This paper proposed the Mission-Driven Cyber Education Framework as one way to address that problem. Drawing on Mission Engineering, adult and experiential learning, professional military education, and graduate cyber practice, MDCE organizes learning around five interconnected elements: mission understanding; systems

thinking and mission dependency analysis; adversary reasoning and decision-making under uncertainty; operational course-of-action development and execution; and mission assessment and organizational learning.

The framework is intentionally mission-centered. Students begin by defining the mission problem, examine the systems and dependencies that enable it, account for adversary behavior and uncertainty, develop and execute a course of action, and then assess whether the action produced the intended effect. Because new information can emerge at any point, the process is recursive rather than linear.

MDCE remains a conceptual framework and requires empirical evaluation. Its contribution is not a claim of demonstrated instructional superiority. It is a theoretically grounded curriculum architecture that can be tested against questions that matter in graduate cyber education: whether students become better at connecting technical decisions to mission outcomes, reasoning across dependencies, communicating with nontechnical decision-makers, adapting during execution, and transferring classroom learning into professional practice.

Graduate cyber education should continue advancing technical excellence. It should also prepare students to understand why a technical capability matters, when it should be employed, how it should be translated into executable action, how it interacts with other organizational systems, and whether it ultimately contributes to the desired mission outcome. The goal is not simply to teach more technology. It is to prepare cyber professionals to use technical expertise in service of the mission.

Ethics Declaration

Ethical clearance was not required for this study. The paper develops a conceptual curriculum framework informed by existing scholarship, professional guidance, Mission Engineering, and reflective practitioner observations from graduate cyber instruction. No human-subject data were systematically collected, analyzed, or reported, and no personally identifiable student information is included.

AI Declaration

Open-source artificial intelligence (AI) tools were used for proofreading, citation formatting, and to illustrate initial drafts of the MDCE Framework into a cleaner depiction in Figure 1. All analysis, arguments, and conclusions presented in this paper are the original work of the author or are derived from appropriately cited sources.

References

Bertone, B., Wagner, P. and Pauli, J. (2025) “Experiential Learning: Innovative Approaches to Post-Secondary Cybersecurity Education”, *Journal of Cybersecurity Education, Research and Practice*, Vol. 2025, No. 1, Article 15.

Chairman of the Joint Chiefs of Staff (2024) *Officer Professional Military Education Policy*, CJCSI 1800.01G, Joint Staff, Washington, DC.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004) “DXXesign Science in Information Systems Research”, *MIS Quarterly*, Vol. 28, No. 1, pp. 75–105. doi:10.2307/25148625.

Joint Task Force on Cybersecurity Education (2017) *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*, Association for Computing Machinery, IEEE Computer Society, Association for Information Systems Special Interest Group on Information Security and Privacy, and International Federation for Information Processing Working Group 11.8.

Klein, G. (1998) *Sources of Power: How People Make Decisions*, MIT Press, Cambridge, MA.

Knowles, M.S. (1984) *Andragogy in Action: Applying Modern Principles of Adult Learning*, Jossey-Bass, San Francisco.

Kolb, D.A. (1984) *Experiential Learning: Experience as the Source of Learning and Development*, Prentice Hall, Englewood Cliffs, NJ.

Lave, J. and Wenger, E. (1991) *Situated Learning: Legitimate Peripheral Participation*, Cambridge University Press, Cambridge.

National Institute of Standards and Technology (2020) *Workforce Framework for Cybersecurity (NICE Framework)*, NIST Special Publication 800-181 Revision 1, National Institute of Standards and Technology, Gaithersburg, MD. doi:10.6028/NIST.SP.800-181r1.

Office of the Under Secretary of Defense for Research and Engineering (2023) *Mission Engineering Guide*, Version 2.0, Department of Defense, Washington, DC.

Schön, D.A. (1983) *The Reflective Practitioner: How Professionals Think in Action*, Basic Books, New York.

Senge, P.M. (1990) *The Fifth Discipline: The Art and Practice of the Learning Organization*, Doubleday, New York.