Building Cyber Defenders of the Future: Curriculum Design for Emerging Roles

Toby Meyer, Austin Vershave and Jael Rivera
Carnegie Mellon University, Software Engineering Institute, Pittsburgh, USA

tmeyer@sei.cmu.edu
amvershave@sei.cmu.edu
jrivera@sei.cmu.edu

Abstract: Creating and maintaining curriculum for emerging cybersecurity work roles is a significant challenge for organizations. Training is expensive, and quality curriculum requires careful curation and sustained effort. Such curriculum typically combines cognitive learning with a considerable amount of applied, hands-on practice. Data is currency, both for emerging cybersecurity work roles and for instrumenting the curriculum itself. We are developing courses for emerging work roles on Cyber Protection Teams (CPTs), specifically for the positions of Analytic Support Officer (ASO) and Data Engineer (DE). Analytic Support Officers learn to ingest cyber threat intelligence, analyze cybersecurity datasets, map enemy courses of action, develop analytics, and provide expert assessments in support of operational decision-making. Data Engineers learn to explore cybersecurity datasets, implement effective data models, collect information from key data sources, transform data for usability, and store data for future analysis. We take a learning engineering approach that incorporates instrumentation, data collection, and behavioral analysis to support curriculum development while maximizing the use of open-source tools and open standards. The effort also includes integrating hands-on virtual environments, competency frameworks, and open standards such as Experience API (xAPI) and Computer Managed Instruction (cmi5) to track training effectiveness and ensure alignment with training goals. This paper discusses the technical and organizational challenges of developing cognitive and hands-on content, aligning instruction with learner motivations and competency frameworks, and applying learning engineering methods and open standards to support modern cyber workforce development.

Keywords: Cybersecurity curriculum development, Cyber threat intelligence, Emerging work roles, Learning engineering, Data-driven warfighting

1. Introduction: The Cyber Workforce Readiness Gap

Cyber Protection Teams operate in high-tempo, evolving threat environments where adversary tactics shift rapidly and unpredictably. Their Mission Essential Task Lists (METLs) for cyber hunts, incident response, and reinforcement to Defensive Cyberspace Operations (DCO) define core functions required for mission success. Executing these tasks demands more than familiarity with tools and platforms; it requires personnel who can apply technical expertise in realistic operational conditions.

Despite clear mission requirements, the Cyber Mission Force (CMF) continues to face personnel shortfalls and uneven capability development across the Joint Force. Many training approaches remain course-centric and event-based, emphasizing completion and certification rather than validated mission performance. These training models provide limited fidelity in measuring readiness because completing instruction does not demonstrate the ability to perform METL-driven tasks in applied environments. Reliance on Temporary Duty (TDY) training also introduces cost and operational inefficiencies without consistently improving capability.

These challenges are becoming more important as data-centric roles grow within CPTs. Analytic Support Officers and Data Engineers work with threat intelligence, data flows, analytics, and decision support aligned with the Joint Cyber Warfighting Architecture (JCWA). Preparing personnel for these responsibilities calls for more than small updates to legacy curriculum. It benefits from an approach that builds strong cognitive foundations, includes sustained hands-on practice, aligns outcomes with Knowledge, Skills, and Abilities (KSAs), Measurable Samples of Behavior (MSBs), and Joint Qualification Requirements (JQRs), and captures learner performance over time.

This paper presents that approach: a learning-engineered curriculum supported by a content-as-code architecture and instrumented, standards-based training environments built on open frameworks like xAPI and cmi5. By embedding measurement into applied learning, this strengthens the link between education, analytics, and warfighting capability in modern Defensive Cyber Operations.

2. Emerging Work Roles in Defensive Cyberspace Operations

Within CPTs, the Analytic Support Officer and Data Engineer ensure data is available, structured, and turned into actionable insight. Together, they enable effective decision-making and mission execution in complex environments.

2.1 Analytic Support Officer

ASOs are force multipliers. They contribute to the Commander's decision-making process by collecting, analyzing, and responding to network data using mathematics, programming, and domain knowledge to enable the unit to efficiently gain and exploit situational awareness. They are subject matter experts for the analytic function at each echelon. The ASO ensures analytic readiness, conducts analytic planning, executes analysis, and grows analytic capabilities. The ASO creates the Analytical Scheme of Maneuver (ASOM), refined by threat intelligence and available data sources. In practice, this means providing valuable insight into the Tactics, Techniques, and Procedures (TTPs) used by threat actors and the vulnerabilities they may target, ensuring analytic readiness, conducting analytic planning, executing analysis, and growing analytic capabilities in support of defensive cyber operations.

2.2 Data Engineer

Where the ASO focuses on the analysis of creating and weaponizing the ASOM, the DE is responsible for ensuring the data to support the ASOM in the hunt for Malicious Cyber Activity (MCA) is in the right format, structure, and location for analysis or ingestion. CPTs cannot find what they cannot see. Ensuring the requisite data is available to identify each TTP is the responsibility of the DE. When the storage environment is complex, the DE ensures optimal placement of data to provide parallel or stream processing capabilities, makes modifications to tune capabilities for different environments, and automates data collection and processing through extract, transform, and load (ETL) pipelines. Data Engineers provide scalable analytics across mission environments, assisting ASOs in exploratory data analysis and visualizations and making them an essential enabler of the analytic function.

2.3 Why These Roles Matter

Cyber operations are at the heart of modern military strategy. Together, these two roles reflect a shift in how defensive cyber operations are conducted, prioritizing data-driven warfighting. Advanced analytics are indispensable in maintaining information dominance, and data is operational currency. The ability to ingest, filter, analyze, and act on cyber terrain data at speed is central to mission success. The ASO and DE work roles formalize that capability within the Joint Force structure, establishing dedicated personnel whose primary function is to ensure that data flows are purpose built, and analytics are actionable to ensure commanders have the insights they need to make decisions in time-sensitive environments.

3. Curriculum Design Philosophy: Learning Engineering at Scale

Here we outline our instructional approach used to design and deliver the curriculum. We begin with learning engineering as the foundation, guiding how content is developed, evaluated, and refined. Then, we describe the content-as-code model used to build and deploy training at scale, followed by the balance of cognitive and applied instruction.

3.1 Learning Engineering as the Foundation

Developing curriculum for emerging cybersecurity work roles is not just a matter of content selection and course structure. It also means creating training in a way that can be refined over time based on learner needs and instructional results. Goodell and Kolodner (2022) describe learning engineering as a "process and practice that applies the learning sciences using human-centered design methodologies and data-informed decision-making to support learners and their development." Put simply, it helps bring research-informed practices into real-world training environments.

For the curriculum described in this paper, learning engineering serves not only as a guiding perspective but also as a practical framework for design. Decisions about content sequencing, assessment design, and instructional support are informed by learning science principles and revisited over time based on learner performance. The curriculum is therefore not treated as fixed or final. Instead, it is designed to be refined as evidence accumulates about where learners struggle, where instruction is effective, and where gaps remain between cognitive understanding and applied performance. (Goodell, Kessler, Kurzweil, Greenwald, & Craig, 2022)

3.2 Content-as-Code Model

To support curriculum development at scale, the program uses a content-as-code model. Lessons, labs, scenarios, and assessments are maintained as structured files in GitLab, where they can be versioned, reviewed, updated, and reused in a controlled way. This approach reduces dependence on static course files, makes changes easier to manage across modules, and supports consistent delivery over time. Each module includes

instructional content, hands-on activities, and assessments, and is built using open-source tools and open standards such as xAPI and cmi5 to improve portability and interoperability across training environments.

When a content-as-code release is tagged, it triggers a Continuous Integration and Continuous Delivery (CI/CD) workflow that builds the deployable course package automatically, running automated checks on structure, formatting, and configuration before the final artifact is produced. The resulting package is a cmi5-compliant artifact that bundles instructional content, applied hands-on practice, assessments, and the backend infrastructure needed to deliver them – essentially a self-contained learning environment. A human review step follows, where the package is uploaded to a Learning Management System (LMS) for post-validation and functional testing before distribution to learners. This step functions much like a production approval gate in a software release pipeline. illustrates how this pipeline operates across a single module, from content authoring through validation and deployment. How this architecture supports the measurement of learner performance and training effectiveness is discussed in detail in Measuring What Matters: Instrumentation and Validation.

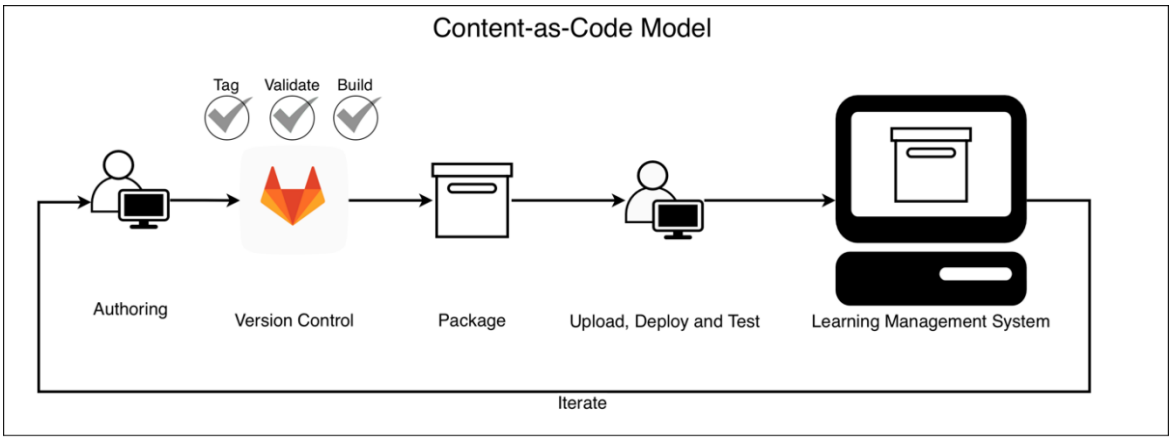

Figure 1: Content-as-Code Model

3.3 Cognitive and Applied Balance

The curriculum uses two complementary layers of instruction: cognitive content and applied practice. Cognitive content establishes the conceptual and theoretical foundations for each work role. Applied, hands-on practice then gives learners the opportunity to apply those foundations under realistic conditions, reinforcing and deepening understanding through execution. Each layer includes its own assessment. Quizzes, knowledge checks, and exams evaluate cognitive mastery, while performance-based assessments and labs measure applied proficiency by requiring learners to execute tasks rather than describe them. All modules map to competency frameworks, KSAs, MSBs, and JQRs, ensuring each unit of instruction aligns with operational standards.

The curriculum intentionally weights the majority of instructional time toward applied instruction, where learners work through hands-on practice mirroring real mission conditions, requiring them to make decisions, execute technical tasks, and adapt to unexpected outcomes. These scenarios are deployed within a persistent cyber range infrastructure that provides sufficient fidelity for meaningful applied learning. Specifics are addressed in Technical Architecture and Standards Integration.

Notably, the curriculum culminates in a capstone experience. In the capstone, learners complete advanced scenarios that draw on competencies from all modules and apply their full range of knowledge and skills in an integrated mission context. The course structure, module organization, and capstone design for both ASO and DE curriculum are examined in greater detail in Course Structure and Modular Design.

4. Technical Architecture and Standards Integration

This section describes the technical and standards-based foundation that supports training and performance measurement. It covers how open standards and environments enable tracking of learner activity, how training systems integrate within the Joint Cyber Warfighting Architecture (JCWA), and how learner behavior is captured. It also presents the competency frameworks used to map, measure, and validate performance against operational requirements.

4.1 Open Standards and Tooling

This section describes how xAPI enables consistent tracking of learning experiences, how an LRS stores and retrieves that data, and how cmi5 defines how content launches, tracks, and reports within the LMS. When used together, these components create an interoperable architecture that supports performance measurement, analytics, and consistent data exchange across systems.

4.1.1 xAPI

Tracking activity across learners and environments provides insight into evaluating assumptions, learning pipelines, and outcomes. IEEE Learning Technology Standards Committee (LTSC) defines standards to support this capability, called xAPI. xAPI serves as an interoperability standard (language) for capturing and sharing data about learning experiences across platforms.

xAPI records learner actions in a consistent *actor-verb-object* format, enabling detailed tracking of activity such as opening modules, viewing content, and completing labs or assessments. This data supports both performance measurement and analytics, allowing instructors to identify learner progress, detect struggles, and adjust instruction. It also allows verified skills to transfer across xAPI-enabled environments.

An xAPI profile defines how activities are tracked. It is a constrained set of rules for implementing xAPI within a specific domain. It describes vocabulary, statement templates, and data patterns to ensure consistent use. Profiles standardize how organizations structure and share data, allowing systems to use a common language. They also organize xAPI statements within a Learning Record Store (LRS) for consistent tracking and analysis.

4.1.2 Learning Record Store

An LRS is a database that stores and retrieves xAPI statements. It receives statements from Learning Record Providers (like a quiz, module, or lab) which send data using standard, RESTful HTTP web requests (PUT, POST, GET, DELETE). Learning Record Consumers (dashboards or analytical tools) use GET requests to retrieve the data. The LRS also strictly checks the structure of the data to ensure it does not receive malformed JSON. The LRS, though, is not instructed to understand the semantics of an xAPI statement according to the IEEE LRS standards. The statement could contain a verb like “sing” to be accompanied by “math equation” to create “the student sang to complete the math equation.” The LRS would accept this statement if the correct syntax was followed. To counter this, tooling can be placed before the LRS to adhere to IEEE standards by allowing the LRS just to store statements.

4.1.3 Computer managed instruction

These standards capture behavioral data within a module or course by combining xAPI with cmi5. While xAPI provides the flexibility to track activity anywhere, cmi5 defines how that data communicates with the LMS. As an xAPI profile, cmi5 uses xAPI to store behavioral data in an LRS and establishes rules for content launching, tracking, and reporting.

Developers package content as courses composed of Assignable Units (AUs), which contain the learning content and generate xAPI data. cmi5 defines a strict set of required verbs for session management between the AU and the LMS, including Launched, Initialized, Completed, Passed, Failed, Terminated, and Abandoned. These “cmi5 defined” statements standardize core interactions, while “cmi5 allowed” statements support additional custom tracking. Once enrolled, learners launch AUs through the LMS and generate data as they interact with the content.

4.2 Persistent Cyber Training Environment

4.2.1 Integration with joint cyber warfighting architecture

The Joint Cyber Warfighting Architecture established a shared platform for training with cyber systems, tools, and sensors. Within that environment, cmi5 supports data exchange between the learning management system (LMS) and the learning record store (LRS), while a common xAPI profile captures more detailed learner performance data. This creates a more consistent structure for sharing learner data across services while still allowing each service to tailor implementation to its needs.

4.2.2 Range-based applied learning

Classroom-based learning from presentations and textbooks is a sound foundation for cyber security capacity. Applying the lessons, however, is best in a high-fidelity simulated environment such as a cyber range. These

cyber ranges allow participants to perform live exercises launched through an LMS in PCTE and tracked by xAPI statements. The xAPI statements help instructors understand a participant's thought process within the nonlinear learning path of a cyber range. The cmi5 standard records when the range is launched within the LMS and if it is completed.

4.2.3 Instrumented learner behaviors

Capturing participant interactions in the LMS and cyber range provides evidence of learning outcomes. Measuring how a learner navigates the range helps determine whether they are guessing or acting with precision. Observing tool usage shows whether they rely on established tools or create their own. It also confirms that they follow the rules of engagement and avoid disrupting (accidentally or otherwise) systems marked as production in the simulated environment. With xAPI, these actions can be tracked in real time, enabling adaptive learning and assessment based on performance rather than knowledge alone.

4.3 Competency Mapping Framework

4.3.1 Knowledge, skills and abilities

KSAs are specific attributes, qualifications and traits required to perform a job effectively. They can be measured in course work and captured using xAPI statements. By storing the statements into an LRS, KSAs can be mapped, identified, and attributed to a learner and aggregated in a learner profile throughout a career.

4.3.2 Measurable samples of behavior

MSBs are specific, observable actions quantified to track progress. Representative samples are identified, reflecting the desired learning objectives connected to the instructional goals. It is important that there are sufficient samples to assert consistent learned behaviors. MSBs are categorized as: outcomes, processing, and errors. Outcomes show whether the participant learned the objective. Processing shows whether the participant followed the correct methodology. Errors identify what mistakes the learner made and whether they are critical or non-critical.

4.3.3 Joint cyberspace training and certification standards

Joint Cyberspace Training and Certification Standards (JCT&CS) are specific tasks mapped to work roles in the Department of War Cyber Workforce Framework (DCWF). The tasks are closely aligned with KSAs but are distinct. A task is an activity an employee regularly performs to fulfill job responsibilities. The JCT&CS identifies certain tasks and KSAs as Core, highlighting them as critical for successful performance within a given work role. Others are considered additional and are not required for success in the work role.

4.3.4 Joint qualification requirements

Joint Qualification Requirements (JQRs) define the skills required for a learner to obtain a specific job. They are the checklists of tasks and competencies a learner must master to qualify for an operational work role. To complete a JQR, the learner demonstrates each task with proficiency to a qualified evaluator. JQRs set the course standard and determine what participants must do to meet professional requirements.

5. Course Structure and Modular Design

The design philosophy and technical architecture established in Learning Engineering at Scale and Technical Architecture and Standards Integration are integrated in the two courses built for the ASO and DE work roles. The modular architecture introduced in Learning Engineering at Scale organizes content at the lesson level. Modules build sequentially from introductory concepts and tools to the operational competencies each work role requires. This hierarchy makes the curriculum maintainable through the content-as-code pipeline. It also enables granular instrumentation with the xAPI and cmi5 architecture described in Technical Architecture and Standards Integration.

5.1 ASO Curriculum

The ASO curriculum offers a fast-track bootcamp comprised of fourteen modules and forty-eight lessons. The curriculum is a mix of approximately 70% applied and 30% cognitive instruction. The delivery is scaffolded: modules progress from foundational domains like cyber terrain, programming, development and data operations, mathematics, and statistics to applied data skills like data processing and visualization. Finally, it moves into operational training, covering Joint Cyber Hunt Kit (JCHK) familiarization and Joint Cyber Warfighting Architecture Common Runtime Stack for Data (JCRS-D) architecture and operations. Later modules focus on

critical thinking, analytic planning, SIEM and BDP operations, and machine learning, building end-to-end analytic workflow expected in a mission environment.

5.2 DE Curriculum

The DE curriculum follows the same delivery and applied-to-cognitive ratio, fourteen-module structure across forty-three lessons. Where the ASO curriculum is oriented toward analytic development and execution, the DE curriculum is built around the data engineering fundamentals and infrastructure that makes network hunt cyber data analysis possible. Modules progress from the cyber terrain and programming foundations through machine learning, data management, data storage architectures, data ingestion through batch and stream processing, data staging, and ETL pipeline development. Later modules address data visualization, JCHK familiarization, SIEM operations including log managements, content development and alerting, and JCRS-D architecture, operations, and data capture, preparing the DE to integrate data sources, manage pipelines, and support analytic development across mission environments.

5.3 Capstone as Readiness Validation

Both courses culminate in a capstone, presenting learners with a comprehensive set of mission-representative scenarios requiring them to apply the full range of competencies developed across the preceding modules. All objectives map directly to MSBs established throughout the course, making the capstone the primary point at which demonstrated readiness is formally assessed and where the instrumentation layer, described in Section 4, produces its most fulsome learner behavior assertion, which is examined in the next section.

6. Measuring What Matters: Instrumentation and Validation

This section focuses on measuring readiness using performance data instead of completion metrics. It outlines how learner behavior supports readiness modeling and highlights key organizational challenges.

6.1 From Completion to Capability

A persistent problem in cybersecurity training is that traditional LMS metrics do not result in mission readiness. Knowing a learner opened a module, spent 40 minutes on it, and passed a multiple-choice quiz at the end says very little about whether that learner can execute the associated tasks when it counts. Completion is not capability. Unvalidated readiness has real operational consequences. Commanders need to know: “Can this operator perform this mission task?”

The instrumented curriculum described in this paper takes a different approach. Rather than relying on whether a learner answered correctly or completed a task, the curriculum captures behavioral evidence across cognitive and hands-on instruction. Cognitive assessments contribute structured data about conceptual understanding, while applied hands-on practice generates a richer and more operationally meaningful record of how learners perform under realistic conditions. As described in Persistent Cyber Training Environment, a central xAPI profile defines which actions and tasks are captured throughout the hands-on environment, producing evidence that reflects demonstrated performance rather than recalled knowledge.

6.2 Behavioral Data and Readiness Modelling

Collecting behavioral data is only meaningful if it is realistic, mapped to learning objectives and outcomes, actionable, and actioned. As learners move through the curriculum, the xAPI statements generated across both cognitive and applied hands-on practice build a cumulative record of how individuals engage with the material, which tasks they complete successfully, where they struggle, and how their performance evolves over time. Mapping those actions to the operational tasks each work role demands is what transforms raw activity data into a meaningful picture of readiness, one that reflects demonstrated performance rather than assumed competency.

Over time and across participants, this accumulated evidence creates the conditions for a more predictive approach to readiness assessment. By understanding which learning behaviors and performance patterns are most strongly associated with successful outcomes, instructors and curriculum developers can begin to identify early indicators of readiness gaps and adjust their instruction, accordingly, getting ahead of capability shortfalls rather than reacting to them after the fact.

6.3 Overcoming Organizational Challenges

Realizing the full potential of an instrumented curriculum requires solving organizational and technical challenges. Cross-service interoperability demands not just technical compatibility but also wider adoption of

shared frameworks and a common data language across the Joint Force. The cross-service xAPI profile being developed within JCWA, referenced in Technical Architecture and Standards Integration, is an active effort toward addressing that gap.

Tempo is also a constraint. The distinction between "Ready Qualified" and "Ready Trained" is a real one, and the TDY model of pulling personnel away from primary responsibilities to achieve the latter is expensive and operationally inefficient. Finally, integration with existing platforms across joint environments remains an ongoing challenge, and the deliberate choice to build the curriculum around open-source tooling and established standards is a practical response to that reality, designed to work within those constraints rather than depend on resolving them first.

7. Organizational and Cultural Implications

This section presents the organizational impact of our approach. It identifies key stakeholders, outlines the shift from course completion/certification to capability-based training, and highlights how our model enables long-term relevance.

7.1 Stakeholders

The curriculum described in this paper serves a broad set of stakeholders, balancing requirements throughout development and delivery. Schoolhouses and training commands are responsible for course execution, while CPTs, National Mission Forces, and Joint Service personnel are the operational end users whose readiness ultimately determines whether training is successful. Leadership and decision-makers at the command level depend on the readiness insights the instrumented curriculum produces to make informed judgments about force capability.

7.2 Shifting from Course-Centric to Capability-Centric

Adopting this approach to training and mission readiness requires more than a technical change. It requires an organizational shift in how training success is defined, moving away from disparate training events measured by completion and certification toward continuous capability pipelines measured by demonstrated behavioral performance. Compliance metrics are a low bar for a high-stakes domain and sustaining this shift requires institutional commitment to treating curriculum as a living system rather than a product delivered and accomplished. From training completion checklist to behavioral validation of human and squadron performance capabilities.

7.3 Workforce Sustainability

Sustainability depends on building training infrastructure that does not require constant reinvestment to remain relevant. The open-source tooling, standards-based architecture, and content-as-code pipeline are designed with that goal in mind, reducing dependency on proprietary systems and enabling curriculum to evolve alongside the mission. Portable learner records further support sustainability by ensuring that the evidence of a learner's demonstrated proficiency travels with them across environments and assignments rather stored in siloed and proprietary systems.

8. Lessons Learned and Future Directions

This section evaluates the current state of the approach. It highlights what is working, identifies remaining gaps, and outlines areas for future research and development.

8.1 What's Working

The content-as-code pipeline, from authoring through automated validation and CI/CD packaging to LMS deployment, has been tested and functions as designed, demonstrating that a software-style release workflow is a viable and practical approach to curriculum development and delivery. The integration of cmi5 and xAPI ecosystem is operational, confirming that open-source tools and standards can serve as a reliable foundation for tracking and communicating learner activity across training environments. Together these foundational elements validate the core tenants of the approach. A learning-engineered, standards-based curriculum can be built, delivered, and instrumented at scale within the constraints of Joint Force training environments.

8.2 Remaining Gaps

Several meaningful challenges remain unresolved as this work continues to develop. Variance in cross-service weapons systems complicates joint practice as the tools, platforms, and data environments differ across

services. This makes a single standardized course difficult to execute uniformly. Training to capabilities and critical thinking rather than tool centric helps ameliorate to some extent. The TDY burden, while addressed in the curriculum's design philosophy, has not been fully eliminated, and the organizational and logistical structures that have historically supported TDY-based training do not change quickly. Integration with existing joint platforms also remains incomplete, and until the connections between the curriculum's instrumentation layer and broader joint infrastructure are fully established, the behavioral evidence the curriculum is designed to produce cannot yet flow to and be aggregated in the places where it would be most useful.

8.3 Research Agenda

This curriculum establishes a foundation for research that the field of cybersecurity training has not yet fully explored. The behavioral data generated as learners move through cognitive and applied hands-on practice represents a largely untapped resource for understanding how cyber operators develop proficiency over time, and future work will focus on developing the analytical methods needed to make that data actionable at scale. Predictive readiness modeling, using accumulated behavioral patterns to identify capability gaps before they become operational problems, is a particularly high-value direction that this learning architecture is designed to support as the data matures. More broadly, the application of learning engineering principles to cyber operations training remains a target rich environment, and the approach described here is intended both as an invitation for others to build on as it is a record of what has been built.

9. Conclusion

The challenge of building capable cyber defenders, let alone cyber defenders of the future, is not resolved simply by more training. It is solved by better training, training that is engineered, instrumented, and continuously refined in response to evidence of how learners in the cyber domain perform. The ASO and DE curricula described in this paper represent a deliberate effort to narrow the gap between a training approach of course completion and mission readiness by embedding learning engineering principles, open standards, and behavioral measurement into each component of the instructional design. This is not without its challenges, as the discussed organizational, infrastructure, and interoperability gaps make clear. But there is inertia, the foundation is in place, and the path forward toward predictive readiness modeling, scalable instrumentation, and a genuinely capability-centric training culture is one this work has begun to establish. There is also a network effect as increased adoption will provide additional impact and inertia. The use of learning engineering methodologies, instrumentation, and data collection in cybersecurity curriculum development is an area where much work is still to be done in support of advancing the practice. Hopefully, this will inspire other practitioners for the betterment of cybersecurity training, tooling and learners, data-driven mission ready warfighters. Advancing cybersecurity curriculum requires intentional integration of behavioral science, instrumentation, and open standards to support modern data-driven cyber workforce development.

10. Acknowledgements

Carnegie Mellon University 2026

This material is based upon work funded and supported by the Department of War under Air Force Contract Nos. FA8702-15-D-0002, and FA870225DB003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM26-0283

Ethics Declaration: Ethical clearance was not required for the research.

AI Declaration: AI tools are not used for the creation of paper.

References

Braitling, B., Allman, B.K., Allman, C., Haag, J., Rogers, J., Poltrack, J. et al. (2023) xAPI. [Online] Available at: https://opensource.ieee.org/xapi [Accessed August 2024].

Goodell, J., Kessler, A., Kurzweil, D., Greenwald, S.W. and Craig, S.D. (2022) *Learning Engineering is a Process*, in *Learning Engineering Toolkit*. New York: Routledge, pp. 29–45.

McDonald, B., Johnson, A., Miller, B., Werkenthin, A., Neumann, S., Koob, M. et al. (n.d.) *xapi-cmi5*. [Online] Available at: https://opensource.ieee.org/xapi-cmi5 [Accessed August 2024].

Advanced Distributed Learning Initiative (n.d.) *xAPI profiles*. [Online] Available at: https://github.com/adlnet/xapi-profiles [Accessed August 2024].

Advanced Distributed Learning Initiative (n.d.) *xAPI specification*. [Online] Available at: https://github.com/adlnet/xAPI-Spec [Accessed August 2024].

Challenge Server (n.d.) *Challenge Server*. [Online] Available at: https://github.com/cmu-sei/Challenge-Server [Accessed August 2024].

Department of Defense Chief Information Officer (n.d.) *DoD Cyber Workforce Framework (DCWF)*. [Online] Available at: https://dodcio.defense.gov/Cyber-Workforce/DCWF [Accessed August 2024].

IEEE Learning Technology Standards Committee (n.d.) *IEEE LTSC*. [Online] Available at: https://www.ieeeltsc.org [Accessed August 2024].

Yet Analytics (n.d.) *SQLLRS*. [Online] Available at: https://github.com/yetanalytics/lrsql [Accessed August 2024].