Developing Cloud-Based Cyber Capacity Building Platforms

David Tileston, Adam Welle, Nuria Pacheco-Casanova, Matt Kaar, Toby Meyer and Rick Luz
Carnegie Mellon University, Software Engineering Institute, Pittsburgh, USA

dftileston@sei.cmu.edu
arwelle@sei.cmu.edu
npacheco@sei.cmu.edu
mkaar@sei.cmu.edu
tmeyer@sei.cmu.edu
eluz@sei.cmu.edu

Abstract: Creating and maintaining an effective cybersecurity workforce is a significant challenge for organizations due to the complexity of the cyberspace domain. Military organizations especially have problems due to the transitory nature of personnel and retention challenges. The Integrated Multinational Cyber Information Sharing and Training Environment (IMCITE) is a system that facilitates organizational development using a learning management system, organic and government-off-the-shelf training materials, hands-on cyber training labs, large-scale cyber exercises, and information sharing with other organizations. Additionally, IMCITE incorporates learning plans and competency frameworks to track training effectiveness and ensure alignment with training goals, enabling targeted and measurable training initiatives to help identify skill gaps, streamline career progression, and improve workforce readiness. In this paper, we will discuss the technical and other challenges involved with developing, deploying, maintaining, and training in the use of such a system.

Keywords: Cyber capacity building, Workforce development, Competency frameworks, Cyber exercises, Virtualization

1. Introduction

Cyber readiness is becoming an increasingly critical aspect of building cyber capacity. Nations are dependent on policies, cyber skills, and infrastructure to safeguard against an evolving threat landscape across the cyberspace domain. The Integrated Multinational Cyber Information Sharing and Training Environment (IMCITE) aims to provide a high-fidelity, realistic environment for training and rehearsing cyber operators. The goal is to support a force in readiness by exercising military functions and mission-essential tasks (METs) to enable operational resources and capabilities. Traditional military functions, including land, air, and sea, now depend on space and cyberspace operations to effectively conduct mission requirements. This necessitates training the cyber workforce in a contested environment to enhance cyber resiliency, manage risk, and bolster the protection of critical assets, including the defense of critical infrastructure that supports modern warfighting functions.

Cyber capacity building efforts require applications to host traditional learning content, deploy hands-on cyber training labs, host cyber exercises, and facilitate information sharing between allied nations. These features enable organizations to develop tailored training content in response to emerging regional cyber threats. By incorporating applications that enable team-oriented training, IMCITE fosters a more effective cybersecurity learning environment, emphasizing collaborative problem solving and operational readiness.

Cyber training labs and cyber exercises play a vital role in preparing teams for real-world scenarios. These events simulate unique scenarios that individuals or teams may encounter in their work, allowing participants to practice and refine learned cybersecurity skills in a controlled, repeatable environment. These events can range from small-scale labs focusing on individual skills to large-scale simulations that test the capabilities of multiple teams or organizations. By participating in these exercises, cybersecurity teams can refine their skills and identify areas for improvement (Kick, 2014).

This paper explores the purpose and components of the IMCITE program as an example for cyber capacity building. We begin by providing an overview of the workforce development challenges addressed by the program and its strategic objectives. We then explore the system's architecture and features, highlighting how each component addresses these challenges and objectives. We then elucidate the challenges encountered during the development and maintenance of the platform, offering insights into strategies for overcoming these hurdles. Finally, we discuss our roadmap for future development of the platform and its potential to serve as a blueprint for other organizations seeking to build cyber capacity.

2. Challenges in Creating and Maintaining a Cyber Workforce

Creating and maintaining an effective cybersecurity workforce is challenging for any organization, but it is even more challenging for governments and militaries due to the nature of their work and limitations in how they recruit and retain talent. The IMCITE program aims to address additional challenges faced by U.S. Government partners who may have fewer financial and personnel resources.

2.1 Military Assignments

Workforce development challenges are intensified in military contexts. The rotational and temporary nature of military personnel assignments, with frequent transfers and limited enlistment periods creates gaps in workforce continuity. Additionally, retaining skilled personnel is an increasing challenge, given the competitive nature of the private sector (Bates & Rose, 2022). This dynamic necessitates continuous training of new individuals with consistent access to training materials and qualified instructors. To optimize the training's effectiveness, it is essential to assess incoming personnel's existing knowledge and skills to ensure that the provided training is targeted toward areas of deficiency but is not redundant.

2.2 Technological Advances and Evolving Threat Actors

Cybersecurity is a rapidly evolving field that requires specialized skills that can be difficult to cultivate and maintain. Cybersecurity professionals must be knowledgeable about current trends in cyber threats, understand threat actors and their tactics, tools, and techniques (TTPs), and keep up to date on new technologies in the field of cyber operations. New networking protocols and the advent of generative AI are just two examples of these advances. To mitigate this challenge and build an effective cybersecurity workforce, continuous training and education are required, especially as new technologies and threats emerge (Orye & Faith-Ell, 2020).

2.3 Cyber Threat Intelligence Sharing

Success in the field of cybersecurity requires collaboration and information sharing. Most organizations are reluctant to share threat information due to trust and data privacy concerns. Military and government organizations may also have restrictions related to sensitive information and system classification. Interoperability issues may also even hinder information sharing attempts (Brilingaite et al., 2022).

While threat intelligence platforms can provide threat information, many governments lack the financial resources to purchase these tools and must rely on publicly released vulnerability notifications and industry reports to understand new threats. These organizations must analyze threat data to derive updated training requirements and then either develop their own updated training or acquire this training from a vendor.

Training content is even less commonly shared than cyber threat intelligence. Training platforms are generally not designed to provide content-sharing capabilities across organizations. Additionally, many organizations use proprietary learning management systems that do not use common standards, limiting the transfer of content between organizations. Without an easy process to share training content, each organization must duplicate effort in generating their own training for new threats.

2.4 Resource Constraints

While necessary, it takes significant financial resources to develop and maintain cyber workforce and cyber training systems, cyber threat intelligence platforms, learning management systems, and cyber ranges. Most of these expenses will be incurred through the procurement of hardware and licensing for hypervisors and virtual machine operation systems but there are additional expenses related to staffing and support.

3. IMCITE Program Overview

3.1 Objectives

Due to the global nature of cyber threats, the U.S. Government recognizes that ensuring its partners have robust defensive cyber capabilities is critical to ensuring its own defense. One of the Five Pillars of the National Cybersecurity Strategy of the United States is to Forge International Partnerships. The 2018 National Cyber Strategy outlined the objective of maintaining "an active international leadership posture to advance American influence and to address an expanding array of threats and challenges to its interests in cyberspace." (U.S. Government Accountability Office, 2024). Within each of the five pillars there are strategic objectives. Relevant to the IMCITE program is Strategic Objective 5.1: Build coalitions to counter threats to our digital ecosystem. To build such a coalition, the Department of Defense (DOD) will often leverage a Significant Security Cooperation

Initiative (SSCI) to engage with international partners. Security cooperation agreements for capacity building are authorized by United States Code Title 10. Specific authorization for cyberspace security and defensive cyber operations is authorized under section 333(a)(9) (U.S. Government Publishing Office, 2022).

DOD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation, identifies combatant commands and their campaign plans as the conduit for security cooperation activities (U.S. Army, 2024). There are 11 combatant commands at present and each one has a specific mission that is based either on function or geographic region. One of these geographic commands, Indo-Pacific command (INDOPACOM), is collaborating with the Carnegie Mellon University (CMU) Software Engineering institute (SEI) and other organizations to build cyber capacity in their region. The SEI is a Federally Funded Research and Development Center (FFRDC) that partners with U.S. Government agencies and the DOD to improve national defense.

INDOPACOM has a strategic objective to improve cybersecurity in the region, including the ability of partners to protect against, recover from, respond to cybersecurity incidents (National Security Council, 2022). To achieve this strategic objective, INDOPACOM planners envisioned a platform where international cyber capacity could be built through the integration of multiple technologies into a cloud-based environment. The IMCITE program combines learning management, cyber threat information, and cyber range environments to create a novel approach to solving cyber workforce development challenges that inhibit cyber capacity building.

3.2 Design Overview

At a high level, the IMCITE platform consists of a learning management system, an information sharing platform, and applications to design and deploy virtual training environments. These components interact with each other to further enhance learning capabilities.

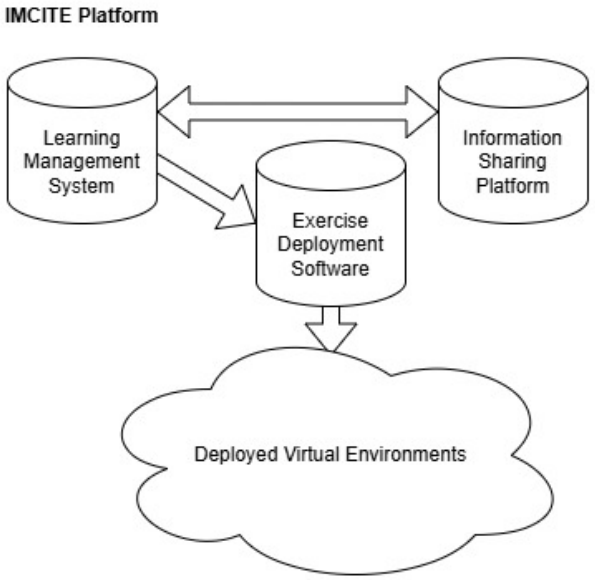

Figure 1: Components of the IMCITE platform

The learning management system (LMS) is where users will primarily interact with the IMCITE platform. From the LMS they can access traditional training content and can also deploy hands-on cyber training labs. The LMS will also provide the user with links to other relevant IMCITE platform applications, based on the user's roles and permissions across the various applications.

The IMCITE platform's cyber threat intelligence integration enables an atypical approach to training by aligning training content to the related cyber threat actors and the TTPs relevant to their region. Integrating the use of both cyber workforce frameworks and cyber threat intelligence frameworks enables organizations to train their personnel based on both work roles and the latest threats. The specific tools integrated into the IMCITE platform will be explained in more detail in the following sections.

To generate further inter-organization collaboration, each IMCITE platform will have tools that enable organizations to share threat intelligence information and training content with each other. As part of the program, organizations may have IMCITE platforms deployed both to the cloud and to on-premises hardware,

enabling sharing between different IMCITE deployment schemes while allowing organizations to retain sensitive data on servers they control.

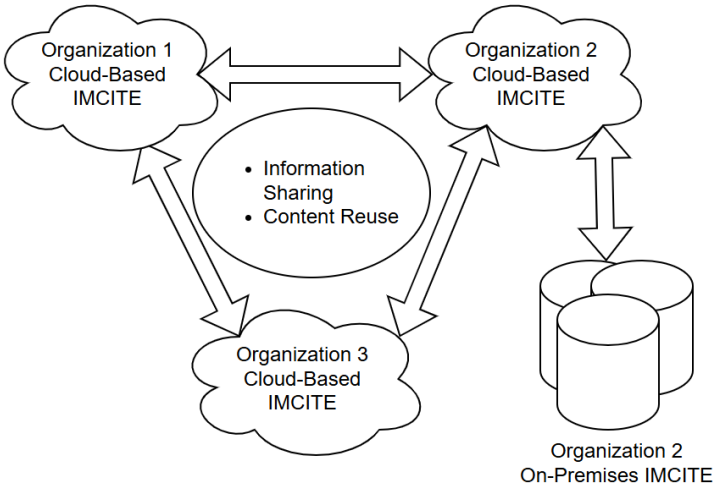

Figure 2: Information and content sharing examples between organizations and deployment types

4. IMCITE Pillars: Effective Cyber Capacity Building

To achieve the objectives of the SSCI, the IMCITE platform has been designed with core capabilities to resolve the challenges outlined in this paper. These core capabilities are referred to as the pillars of the IMCITE platform and are implemented by a set of integrated applications. The four pillars are learning management, hands-on cyber training labs, team-based cyber exercises, and cyber threat intelligence.

4.1 Learning Management

Moodle has been selected as the LMS due to its open-source codebase (Moodle, n.d.). Moodle can be easily customized and extended by developing custom plugins to provide additional capabilities and using plugins developed and maintained by a worldwide community. Moodle also contains two key capabilities that enable efficient and effective skills training: competency frameworks and learning plans.

Moodle's competency framework capability allows organizations to enter frameworks such as the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity (NICE Framework) (Petersen, 2020) and Cybersecurity Framework (Pascoe, 2024) into the LMS and assign specific competencies such as tasks, knowledge, and skills at both the course level and the activity level. These competencies can be automatically marked as complete or proficient upon receipt of a passing grade. Instructors can also manually record a learner's competency, taking into consideration learning and assessment outside of the LMS.

Moodle's learning plan capability allows the competencies to be mapped into the requirements for different work roles. The learning plans also track the learner across all activities on the LMS and are not limited to a single course or grouping of courses. This structured approach enables learners to identify necessary training content to achieve proficiency in their work roles. These learning plans can be directly aligned with established frameworks, such as the NICE framework, ensuring training outcomes abide to industry-recognized standards. To streamline the creation and configuration of these templates, the SEI has developed a Moodle plugin that facilitates the import, export, and automated generation of learning plan templates based on competency frameworks (Carnegie Mellon University, 2025a).

Content from the SEI, other FFRDCs, and government agencies can also be hosted inside the IMCITE platform. To facilitate controlled access to the content, Moodle course categories, roles and permissions can be effectively leveraged. Many of the partners that will receive the IMCITE platform have already been provided with training content from organizations hosting content, and the Moodle application will further streamline delivery and access to training.

4.2 Hands-on Cyber Training Labs

Another essential tool used in the IMCITE platform is TopoMojo, an open-source lab builder and player application developed by the SEI. TopoMojo enables the design and delivery of small-scale hands-on cybersecurity training labs within a secure and isolated virtual machine environment (Carnegie Mellon University, 2025c). TopoMojo provides a challenge capability that allows players to be assessed with a variant of short answer questions. It also includes a generation of "transforms" which are uniquely generated phrases that can be used to customize both content inside the virtual machines and the challenge questions. This ensures that players are not able to cheat because each player will have unique questions and answers. To enable maximum flexibility for differing organizations, TopoMojo can deploy virtual machines to VMware and Proxmox hypervisors.

To enhance accessibility and streamline the learning experience, a Moodle plugin was developed to integrate TopoMojo labs directly into Moodle courses (Carnegie Mellon University, 2025b). This integration ensures that students can access all necessary training resources from a single interface. The plugin allows for standard Moodle questions and TopoMojo-specific questions to be added to the Moodle activity, enabling robust assessment and tracking within Moodle.

4.3 Team-Based Cyber Exercises

Another key component of the IMCITE platform is its capability for large scale cyber exercises. This capability is Crucible, an open-source application framework for cyber training, experimentation, and exercise developed by the SEI (Software Engineering Institute, 2025). It is a modular framework that allows the integration of different components to meet the specific needs of each exercise. Using single-sign-on (SSO) and application programming interfaces (APIs), the applications integrate with each other to provide customization and unique capabilities. Popular open-source applications that support Open Authorization (OAuth) can be used to further extend the environment beyond the range and scenario-based applications that have been developed as part of the Crucible framework itself. This section will provide a brief overview of the Crucible applications used to enable cyber exercises.

Player is the Crucible front end users interact with during a cyber exercise. It allows the participant to access all the integrated components necessary for the exercise. This includes links to other applications and console access to virtual machines. Access to the applications and the virtual machine consoles is restricted by team. This allows for teams of defenders and attackers, as well as exercise controllers, to have different accesses and permissions within the exercise.

Caster is an infrastructure-as-code (IaC) tool for building network topologies. It uses the popular Terraform tool to define the topologies, allowing for complex large-scale scenarios to be built with ease. Caster can interface with multiple hypervisors, including VMware, Azure, Amazon Web Services, and Proxmox, allowing for flexibility and cost-savings, depending on the needs of the organization.

Steamfitter is an inject delivery system. It allows for injects on Master Scenario Event List (MSEL) to be executed manually or on schedule via the implementation of a scenario. Steamfitter can interact with other Crucible applications, web APIs, and virtual machines through its integration with Stackstorm, another open source tool that provides automation across a variety of technologies. Steamfitter tasks can be used to update other applications, execute cyber-attack simulations inside the virtual machines, and assess participant performance by checking configurations made inside the virtual machines.

The Collaborative Incident Threat Evaluator (CITE) tool provides an exercise dashboard and a risk assessment capability to the platform. The dashboard allows participants to view information about the exercise scenario and to assign roles and tasks to each other. The risk assessment capability was based on the National Cyber Incident Scoring System (NCISS) developed by the Cybersecurity and Infrastructure Security Agency (CISA) but can be customized as needed by an organization to align with their requirements.

Gallery is an application that allows participants to receive non-technical injects, allowing for more inclusive gameplay by allowing analysts, commanders, and observers to receive relevant information. Gallery can display injects for source types such as intelligence reports, orders, news articles, social media posts, and telephone and email summaries. Gallery also contains a "wall" that visualizes the severity of the cyber incidents occurring in various categories, such as critical infrastructure sectors.

Blueprint is a tool that enables the exercise planning process to be conducted collaboratively within the platform. Exercise planners can create the MSEL directly inside of the platform. Blueprint can customize the

format of the MSEL, adding columns as needed to provide the required details for each event or inject. Additional columns can be used to provide assessment results and track the learning objectives and competencies related to each event or inject in the scenario. Blueprint can also push the inject details directly to the other Crucible applications, reducing the time and effort taken to configure and build an exercise.

In addition to the applications explored above, Crucible exercises also can be configured to run simulations inside of the virtual environment that create a more realistic experience. These include internet and user simulation capabilities such as GreyBox (Bumanglag, 2019) and GHOSTS (Updyke, et al., 2018). Assessment tools like SEER (System for Event Evaluation Research) can also be integrated to gather assessment data (Updyke, et al., 2024). The range of technologies used within Crucible allow for robust competency-based assessment of participant performance in a variety of work roles.

4.4 Cyber Threat Intelligence

The IMCITE platform integrates the open-source cyber threat intelligence platform MISP, the Malware Information Sharing Platform (MISP Project, 2025). MISP allows for indicators of compromise (IoCs) to be shared across organizations. MISP can subscribe to available public feeds as a baseline for integration into the IMCITE platform. Partners can then choose whether they want to publish and share their own threat information with each other. MISP uses common standards such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII) to store and transfer this data. By incorporating MISP into platform, the partner can choose learning content based on threats as they become aware of those threats via the MISP feeds. This integration also enables exercise planners to build new scenarios based on the most relevant and up to date threat information.

5. Development and Deployment of IMCITE

5.1 Infrastructure and Platform Challenges

As an enduring cyber capability development platform for U.S. Government partners, the IMCITE program integrates open-source software across cloud and on-premises datacenters. Deployed in cloud datacenters in close geographic proximity to training centers and personnel, the IMCITE platforms enable partners to “train as they fight” using low-latency network connections and modern software frameworks to ensure the environment will meet the cyber training needs of each partner for years to come. This section explores the infrastructure and backend challenges being address by the IMCITE program.

The IMCITE program serves many different partners, each with its own budget, legal constraints, and technical abilities. Given these natural disparities, open-source software serves as the foundation for the IMCITE program. Without open-source software, partners must license software across multiple layers of the deployment stack and become dependent on proprietary software for future upgrades and expansion. By prioritizing open-source operating systems, like Linux, as well as infrastructure automation tools, such as Kubernetes and Terraform, the IMCITE program leverages well-documented platforms with large communities to ensure that partners will be empowered to maintain and improve the platform as new requirements emerge.

This open-source focus extends to both cloud-based and on-premises IMCITE platforms. Where possible, the same software and deployment methodologies are used in both environments to maximize simplicity and minimize infrastructure training requirements across the platform. Container orchestration software, such as Kubernetes, allows applications to be deployed and maintained in different environments with less engineering effort than legacy deployments directly installed on a host operating system. Moving these workloads to Linux containers allows them to be portable across multiple cloud service providers (e.g., Amazon Web Services and Microsoft Azure) as well as on-premises Kubernetes clusters.

By automating the deployment and management tasks involved in a new cloud or on-premises environment, IMCITE engineers minimize human error and maximize scalability of the platform. While initial build steps are prototyped through manual actions in a graphical user interface (GUI) or command line interface (CLI), engineers translate these steps into infrastructure as code, enabling them to be recreated without manual intervention for subsequent environment builds. Tools like Terraform and Ansible enable both cloud and on-premises automation, shortening build steps that could take days or weeks down to hours. By focusing on automated deployments, engineers limit inconsistencies between peer IMCITE platforms to always deliver the same experience to all partners.

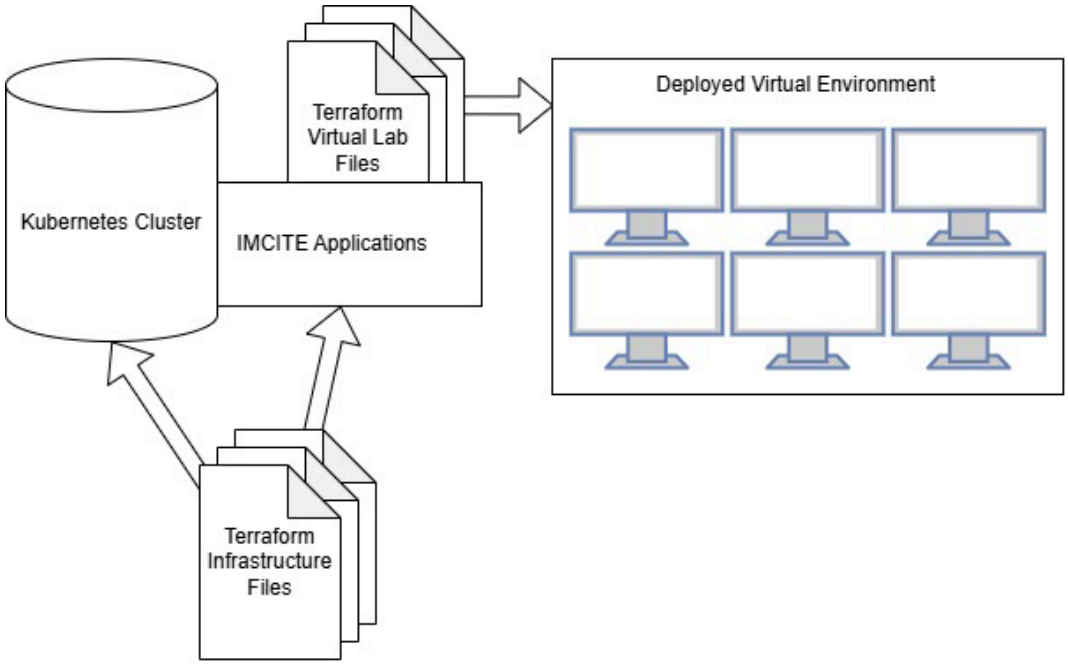

Figure 3: Utilizing infrastructure as code to deploy IMCITE environment and virtual lab environments

5.2 Platform Deployment and Maintenance

The IMCITE program enables cyber capacity building through systems designed and deployed by U.S. DOD FFRDC organizations. These systems are operated for five years as an SSCI partnership between the United States and each partner entity. At the end of the five-year period, all infrastructure, both cloud and on-premises, transitions to be owned and maintained by the IMCITE partner. Many elements of the system contribute to ensuring a smooth transition at the end of the SSCI. From independent domain name system (DNS) registrations to separation of cloud accounts to technical training on maintaining on-premises servers and networking equipment, each component of the IMCITE platform builds towards a successful handoff to the partner to enable capacity building well beyond the five-year initial engagement period.

As the IMCITE program footprint grows to include more partners and more technical capabilities, the core mission of increasing partners' capacity to train, equip, and fight across the cyber domain will not change. This common focus for the program enables unity of effort and sharing of best practices towards the success of that shared mission. To this end, comprehensive training on the use and maintenance of the platform is required to be given to each IMCITE partner. This training spans multiple weeks and is focused on how to utilize each component of the IMCITE platform.

6. Future Work

Initial work has been performed to map a portion of the existing learning content to NICE work roles and tasks. Using a large language model (LLM), it may be possible to identify additional competency mappings for the learning content. There is an opportunity to leverage Moodle's new artificial intelligence (AI) subsystem to integrate with an LLM to analyze the content of learning activities and perform competency mapping. This development would make it easier for training mangers to identify how content fits into their workforce development needs.

Further integration of cyber threat intelligence into the platform would also enable mission readiness by allowing learners to identity and conduct training related to current threats. Mapping training content to standards such as the MITRE ATT&CK framework could also improve the ability of a learner to identify relevant training content. Developing an integration between MISP and Moodle would enable learners more easily identify related content.

To address the financial restraints related to hypervisor licensing, the program aims to integrate with the open-source hypervisor Proxmox. The TopoMojo and Caster applications have already been prototyped to deploy virtual environments on Proxmox servers; further refinement of this work will leverage the scalability of cloud

infrastructure to allocate necessary resources, as needed. This will result in a significant cost savings on both licensing and infrastructure.

Learning engineering standards are also being integrated into the platform to further support the objectives of the IMCITE program. Full implementation of the Total Learning Architecture (TLA) standards (Johnson & Miller, 2022) will be considered as the program progresses. The TLA contains a standard for enterprise learner records which can be used to facilitate the transfer of training records between organizations. This will reduce redundant efforts and improve training efficiency when a learner moves between organizations.

The Experience API (xAPI) standard (ADL Initiative, 2025), developed by the ADL Initiative and now maintained by IEEE, is already implemented in Moodle and it is partially implemented inside of the Crucible applications. Further integration of xAPI inside of the Crucible applications will assist in more granular tracking of learner experiences and will enable additional opportunities for competency assessment across the IMCITE platform. The SEI has done previous work in logging student performance inside of virtual machines using the xAPI standard (Welle & Bumanglag, 2019) and intends to leverage that experience to infer competencies during cyber exercises.

7. Conclusion

To defend against global cyber threats, it is necessary to have a well-trained coalition of cybersecurity workforces. This is particularly important for U.S. Government organizations and partners defending critical assets and infrastructure that supports modern warfighting functions. Training must go beyond rote instruction and let students participate in hands-on training scenarios that develop and validate the skills necessary for their work roles. This training must also continuously incorporate new tools, tactics, and techniques used in the field of cybersecurity.

This paper introduced the IMCITE platform, a high-fidelity, realistic environment for training and rehearsing cyber operators for real-world scenarios. IMCITE addresses the cybersecurity workforce development challenges that U.S. Government partners face and serves as a comprehensive solution for cyber capacity building by integrating learning management, hands-on cyber training labs, team-based cyber exercises, and cyber threat intelligence. We have also reviewed the philosophy behind the design of IMCITE as well as the challenges that went into developing and maintaining the system.

Acknowledgements

Carnegie Mellon University 2025

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM25-0273

AI declaration: AI tools were not used in the development of this paper.

Ethics declaration: No ethical clearance was required for the research presented in this paper.

References

ADL Initiative. (2025). *Experience API (xAPI) Standard*. Available at: https://adlnet.gov/projects/xapi/ (Accessed: 6 February 2025).

Bates, C., & Rose, C. (2022). "Understanding and Fixing the Army's Challenge in Keeping Cyber Talent". Available at: https://mwi.westpoint.edu/understanding-and-fixing-the-armys-challenge-in-keeping-cyber-talent/ (Accessed: 6 February 2025).

Brilingaite, A., Bukauskas, L., Juozapavicius, A., & Kutka, E. (2022). "Overcoming information-sharing challenges in cyber defense exercises". *Journal of Cybersecurity*, 9. Available at:https://academic.oup.com/cybersecurity/article/8/1/tyac001/6516499 (Accessed: 6 February 2025).

Bumanglag, K. L. (2019). "Constructing Large Scale Cyber Wargames." *International Conference on Cyber Warfare and Security*, pp. 653-X. Academic Conferences International Limited.

Carnegie Mellon University. (2025a). "Learning Plan Template Manager for Moodle". *GitHub*. Available at: https://github.com/cmu-sei/moodle-tool_lptmanager (Accessed: 6 February 2025).

Carnegie Mellon University. (2025b). "mod_topomojo". *GitHub*. Available at: https://github.com/cmu-sei/moodle-mod_topomojo (Accessed: 6 February 2025).

Carnegie Mellon University. (2025c). "TopoMojo". *GitHub*. Available at: https://github.com/cmu-sei/TopoMojo (Accessed: 6 February 2025).

Johnson, A., & Miller, S. (2022). *TLA Standards Digital Learning Acquisition Guidance.* Advanced Distributed Learning.

Kick, J. (2014). *Cyber Exercise Playbook.* Wiesbaden, Germany: The MITRE Corporation.

MISP Project. (2025). "MISP Threat Sharing". Available at: https://www.misp-project.org/ (Accessed: 6 February 2025).

Moodle. (n.d.). *Moodle*. Available at: https://moodle.org (Accessed: 6 February 2025).

National Security Council. (2022). *The White House*. Available at: https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf (Accessed: 6 February 2025).

Orye, E., & Faith-Ell, G. (2020). "Cyber Workforce Recruitment and Retention: An Awareness Assessment". Available at: https://ccdcoe.org/uploads/2021/01/Workforce-Sep_20_final.pdf (Accessed: 6 February 2025).

Pascoe, C. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.CSWP.29 (Accessed: 6 February 2025).

Petersen, R. S. (2020). *Workforce Framework for Cybersecurity (NICE Framework).* Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-181r1 (Accessed: 6 February 2025).

Software Engineering Institute. (2025). "Crucible: A Cyber Experimentation and Exercise Framework". Available at: https://insights.sei.cmu.edu/library/crucible-a-cyber-experimentation-and-exercise-framework/ (Accessed: 6 February 2025).

U.S. Army. (2024). *Understanding Security Cooperation.* Available at: https://api.army.mil/e2/c/downloads/2024/10/17/faf2497c/no-25-01-768-understanding-security-cooperation-oct-24.pdf (Accessed: 6 February 2025).

U.S. Government Accountability Office. (2023). *Cybersecurity: Launching and Implementing the National Cybersecurity Strategy.* Available at: https://www.gao.gov/assets/830/827189.pdf (Accessed: 6 February 2025).

U.S. Government Accountability Office. (2024). *Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy.* Available at: https://www.gao.gov/products/gao-24-106916 (Accessed: 6 February 2025).

U.S. Government Publishing Office. (2022). *10 U.S.C § 333.* Available at: https://statecodesfiles.justia.com/us/2022/title-10/subtitle-a/part-i/chapter-16/subchapter-iv/sec-333/sec-333.pdf (Accessed: 6 February 2025).

Updyke, D. D., Dobson, G. B., Podnar, G. T., Osterritter, L. J., Earl, B. L., & Cerini, A. D. (2018). *GHOSTS in the Machine: A Framework for Cyber-Warfare Exercise NPC Simulation.* Software Engineering Institute.

Updyke, D. D., Podnar, T. G., Yarger, J., & Huff, S. (2024). *Self-Assessment in Training and Exercise.* Software Engineering Institute.

Welle, A., & Bumanglag, K. (2019). *Moodle.* Available at: https://moodle.com/wp-content/events/mootglobal19/VirtualCyberExerciseswithMoodle.pdf (Accessed: 6 February 2025).