SN Computer Science (2026) 7:349
https://doi.org/10.1007/s42979-026-04931-8

ORIGINAL RESEARCH

Design Tools for Gateway Interface Ecosystems: A Socio-Ecological Approach

Rotem D. Guttman[1] · Lauren Herckis[1,2] · Sabrina Culyba[3] · Kathryn Hymes[4] · Jessica Hammer[1]

Received: 23 September 2025 / Accepted: 21 March 2026

Abstract

Science gateways provide different interfaces to the same underlying toolset based upon the needs of different members of a specific community. However, as the aperture of the targeted community widens and we seek to address the challenges facing science across all of modern society, this approach becomes untenable. No single interface, no matter how intelligent, can serve the needs of every community in every context. In this paper we show how the creation of **science gateway interface ecosystems**—groups of intelligent interfaces that together form a mutually reinforcing collective—can address these challenges. Further, we present a methodology for creating such interface ecosystems *without the need for coordination* between the designers of the constituent interfaces. As a demonstration of this approach, we present a set of case studies in which interfaces are created for different audiences and contexts. Each case is examined through the lens of the design tools identified in our methodology. We show that despite being created by designers from different organizations, with different objectives, audiences, and contexts, these interfaces form a cohesive and mutually reinforcing pathway that guides the community to deepen their engagement with researchers and practitioners in the subject area.

Keywords Learning · Ecosystems · Science gateways · Cybersecurity

Introduction

Science gateways provide shared resources within a scientific community, such as access to computational services, data repositories, and software [1]. However, different members of a community have different needs when engaging with these shared resources. A first-year student may struggle to understand the basic workflow of a scientific process, while an expert practitioner might want extensive customizations. Science gateways are typically designed to provide remote access to high-performance computing resources, but the same design choice allows different front-end interfaces to connect to the same back-end infrastructure.

In this paper, we explore the concept of *gateway interface ecosystems*: a set of diverse interfaces for back-end resources that each serve a different audience, but that *together* form a mutually reinforcing collective. Each interface can be tailored for the needs of the audience and the context where it is deployed. For example, an interface for students could use progressive disclosure to help students understand core concepts step by step, while an interface for professionals might show many options for customization. However, the ecosystem approach considers these differences as part of a larger whole. By aligning different learning experiences to target the same core concepts, we can create a mutually reinforcing network that guides participants into deeper engagement.

As we will demonstrate below, this design philosophy has the potential to transform STEM education, helping learners grow over time by engaging with a range of science gateways within the same field, each of which is appropriately designed for their abilities and the context in which it

Lauren Herckis and Jessica Hammer have contributed equally to this work.

✉ Rotem D. Guttman
rguttman@andrew.cmu.edu

1 Human-Computer Interaction Institute, Carnegie Mellon University, 5000 Forbes Ave, Pittsburgh, PA 15213, USA

2 Global Health Workforce Development Institute, TruMerit, 3600 Market Street, Suite 400, Philadelphia, PA 19104, USA

3 Ludoliminal, Pittsburgh 15213, PA, USA

4 Oxford Internet Institute, University of Oxford, Wellington Square, Oxford OX1 2JD, UK

Published online: 10 April 2026

is deployed. Learners can "graduate" from one experience in a learning ecosystem to a more complex one, or explore complementary approaches to deepen their understanding.

To better understand what this might look like, consider the trajectory of someone learning to code. A child might begin with a board game like *Robot Turtles* that teaches computational concepts, then advance to a block-based coding system such as Scratch. As they get older, they might engage in informal learning activities like a game jam with community members and practitioners, or they might choose to take formal computer science classes. While each component of this example already exists, the transitions between them are typically left for individuals to navigate. Which board games prepare students effectively for block-based coding? Does the game jam help them build connections with practitioners, or are they just working in the same room? How can learners translate their prior experiences to be legible in the classroom? These are the challenges that a gateway interface ecosystem can help address, by making the learning goals of each experience *explicit*, so that they can be shared, reflected upon, and linked together into a range of different pathways.

While the benefits of this approach are clear, developing bespoke interfaces for each target audience that maintain alignment between interventions is a challenging design problem. In this paper, we therefore present a set of *design tools for science gateway ecosystems*, along with a case study showing how they can support learners at varying levels of expertise.

For our case study, we chose the problem of cybersecurity. We made this choice for three reasons. First, there is a pressing need for effective cybersecurity professionals. The most recent ISC2 survey places the gap between the number of cybersecurity professionals available and those needed to meet organizational needs worldwide at over 4.7 million, an increase of nearly 20% just since the previous year. However, traditional recruitment strategies, awareness building, and educational interventions have so far failed to address this gap [2]. A successful intervention in this domain promises to have substantial real-world impact. Second, a science gateways approach is especially important in the cybersecurity domain, as many schools lack access to cybersecurity labs and infrastructure. However, by utilizing lightweight interfaces—starting with analog experiences that are aligned with future digital interface experiences—we can expand the reach of cybersecurity education. Finally, we identified cybersecurity as a complex socio-technical problem, where knowing how to perform technical tasks is insufficient to improve cybersecurity within organizations. We see this evidenced in practice as even well-understood security measures such as multi-factor authentication, resource public key infrastructure or zero-trust architectures are slow to see widespread adoption [3–5]. Change is often seen as too costly to implement, too disruptive, or its need is not fully appreciated by decision makers [6–8]. Creating change in the face of organizational inertia requires a motivated staff with not only the technical skills to identify shortfalls and address them, but also the skills required to advocate effectively for meaningful change, even to a largely non-technical audience. An ecosystem approach allows designers to gain an appreciation for what may be otherwise viewed as disparate skill sets, and create interventions that support the integration of nontechnical skills in a technical context. Thus we can create not only technically capable practitioners but the perceptive change makers that the practice of cybersecurity so desperately needs. Science gateway interface ecosystems can be understood as mutually reinforcing, scalable collectives. They can be built for any domain. To advance such an ecosystem, a design team requires only an established set of desired outcomes, such as educational standards. Intentional use of the design tools described here enable a design team to contribute a new interface to the collective without needing to coordinate with previous or concurrent designers of other constituent interfaces.

Background

Cybersecurity Education

Cybersecurity education faces a myriad of challenges. Some of these challenges are common among STEM fields, such as lack of program funding, educator shortages, or resource disparities between communities. However, cybersecurity education faces the additional hurdle of a knowledge-implementation gap in the area of integrating technical and non-technical skills.

In order to better understand the reasons for this gap and its effect on workforce readiness it is important to understand the context in which this still-maturing field has been, and continues to generate, new professionals. In most post-secondary educational settings, cybersecurity has been taught in the context of computer science, computer engineering, information technology, information systems, or software engineering [9]. All of these fields are highly technical, and as such educators in this space have traditionally focused on technical skills [10]. However, as the field of cybersecurity has matured, there has been growing recognition of the need to broaden the skill set of its practitioners [11].

For cybersecurity professionals to be effective in the workforce they must engage in organizational decision making processes. Such processes require communication, collaboration, and negotiation skills combined with deep technical knowledge and an awareness of the business,

government or academic contexts of the organization. If cybersecurity professionals are unable to effectively utilize these skills in concert, change will not occur.

The most comprehensive document detailing the needs for cybersecurity workforce development are the "Cybersecurity Curricular Guidelines" created by the Joint Task Force (JTF) on Cybersecurity Education [9]. This task force represents a collaboration between all the major international computing societies with representatives from the Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). In this document these organizations attempt to provide prescriptive guidelines for developing cybersecurity training programs.

Even at its most basic level, the JTF guidelines recognize the need for the combination of both technical and non-technical skills, defining cybersecurity as:

> "A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. *It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management.*"(Emphasis added)

The JTF guidelines further note that to enable proficiency in the field graduates of a cybersecurity program should gain the "theoretical and conceptual knowledge essential to understanding the discipline, and opportunities to develop the practical skills that support the application of that knowledge," explicitly acknowledging the need for the combination of both technical and non-technical skills.

> Non-technical (sometimes called soft) skills are vital to the success of cybersecurity professionals. The ability to work in a team, communicate technical topics to nontechnical audiences, successfully argue for resource allocations, hone situational awareness, and operate within disparate organizational cultures are just a few of these skills.

Yet despite this recognition from academia and professional societies of the need to equip cybersecurity professionals with non-technical skills in order for them to be able to effect positive change, traditional cybersecurity programs continue to focus almost exclusively on technical skill development. However, by utilizing the tools presented in Section "Design Tools" we enable designers to account for the challenges faced by their target audience—both those unique to cybersecurity and those faced by the broader educational community, while accounting for the variety of factors needed to create effective cybersecurity practitioners.

Learning Ecosystems

Learning ecosystems borrow an ecological metaphor wherein learners are part of a larger, interconnected system of living and nonliving elements that interact in many complex ways, and in which a change or interaction in one part of the system may have effects throughout the system as a whole [12]. The ecosystem approach is favored in social sciences and in educational research and innovation to expose and explain the interplay among experiences of individuals, communities, and components of the broader environment. Learning ecosystems, by definition, incorporate diverse stakeholders such as learners, educators, families, school administrators, regulators, institutional bodies, professional associations and others. They also incorporate non-living elements such as educational tools and materials, supportive technologies, physical infrastructure, digital infrastructure, and an ever-growing variety of educational interventions [13, 14].

Many educational interventions are designed to have a positive impact on learning under laboratory conditions, and much educational research explores the impact of interventions, pedagogy, or environmental factors, all else being equal. Authentic learning experiences do not, however, take place under laboratory conditions: they take place in classrooms and at dinner tables, on the job and through focused efforts to develop new schools, and among learners who each have unique histories, prior experiences, and predispositions. Learning may be the accidental result of misguided first attempts or cultivated through careful mentorship. An ecosystem approach enables education researchers and educational designers to account for many conditions and variables that impact the effectiveness, efficacy, implementation, and experiential qualities of an intervention.

An ecosystem approach to educational design has produced formal and informal learning opportunities that are positioned to positively impact multiple stakeholders within an ecosystem [15]. A well detailed example of this approach is presented in [16], where the authors show how IoT device-based systems can provide scalable systems that educators and other stakeholders can use and expand to meet individual learners, schools, and community needs. The authors utilize Singapore's National Science Experiment as a case study, detailing how an ecosystem approach focusing on the interactions between researchers and developers, pedagogical institutes, service providers, schools, teachers, students, funders, and government agencies to support the creation

of an ecosystem that promotes data driven thinking across the STEM audience. Extending this appraoch, designers and developers have sought to create interventions that are themselves ecosystems, providing pathways to learning and, at the same time, interacting by design in multiple and complex ways with the larger educational ecosystem in which they are embedded. The Synergies Project offers a useful case study of several interventions, designed using a learning ecosystem approach, that are mutually reinforcing and amplifying [17]. This project was built through a research-practice partnership in a specific neighborhood. Resulting innovations enabled stakeholders throughout the ecosystem to develop and access opportunities for training and to access educational technologies.

Design Tools

We use a combination of two design tools, the Transformational Framework and a socio-ecological model, to create human-centered science gateway interfaces that promote transformational learning and deep engagement with wicked problems. These tools, taken together, enable designers to address a complex problem such as cybersecurity workforce development and promote multiple, coordinated and mutually reinforcing outcomes. The Transformational Framework is a design process tool that is used to define critical features and desired impacts of transformational experiences. A socio-ecological model enables a holistic view of the problem space, in which we can systematically identify the targets of a given intervention beyond the individual.

The Transformational Framework

The Transformational Framework can be used to create an effective intelligent interface that drives a desired change, or desired changes, in an audience [18]. It presents a set of eight key areas for a design team to explore in order to align their collective vision and to document their process. The Transformational Framework process emphasizes collectively answering key questions about the audience being targeted for transformation and the contextual references being leveraged by the team to inform their approach to creating and evaluating that transformation. The design team uses this approach to guide and detail the design approach, and to set constraints for implementation.

Note that the Transformational Framework is typically used for the design of educational games; however, in this project, we adapt it for the design of educational interventions writ large. We will consider the elements of the Framework here, clustered into three groupings:

- Domain Concepts and Prior Work are tools for engaging domain knowledge in the design of the interface.
  - **Domain Concepts** asks "What is essential to include in the game to transform your players?" It leads teams to explore the various diverse aspects of the topical focus of their intervention and to evaluate what concepts should or could be embodied by their intervention given the scale of their project and the impact they hope it will have on players. In a non-game context, it can be applied to interface design or other types of learning interventions.
  - **Prior Work** asks "What can you learn from what others have done?" It guides teams to seek out related interventions or research, which can be evaluated by the team to inform their own project.
- Audience & Context, Player Transformations, and Barriers are tools for thinking holistically about the impact of interface design decisions.
  - **Audience & Context** asks "What is the ecosystem in which your game must create change?" It prompts teams to build a model of their players and the ecosystem in which the players will engage in the game itself as well as follow through with the goals of the intervention. In a non-game context, this item asks us to understand the direct users of a learning interface, as well as any other stakeholders in the experience.
  - **Player Transformations** asks "How should players be different after playing your game?" It has teams identify a focused set of specific impacts they hope to engender and measure in their players from their intervention. In a non-game context, this item is used to define the intended change from the learning experience.
  - **Barriers** asks "Why aren't your players already transformed?" It prompts teams to identify those things that stand in the way of the transformation of their audience, which their intervention may need to acknowledge and possibly address in order to successfully transform their players. In a non-game context, it means understanding the barriers faced by learners more broadly.
- High-Level Purpose and Assessment are tools for establishing what success looks like for the design of the interface
  - **High-Level Purpose** asks "Why is it important that your game transform players?" It leads teams

to establish a shared sense of what motivates the design's transformational success by centering a big-picture impact that the team's intervention should support. In a non-game context, it can be applied to any solution-based design or intervention where success is motivated at least in part by transformational impact.

– **Assessment** asks "How will you measure your game's impact?" It prompts teams to establish the criteria and methods that they will use to measure their project's transformational success.

As a brief illustrative hypothetical example of a transformational framework, consider a team seeking to create an intervention to encourage pursuit of math-related fields in college students. Through collaborative engagement with the Transformational Framework process, the team might center on a focused high-level purpose around helping students see math as relevant for their personal and professional use beyond school, which the team summarizes as "Math for Life." They look at prior works like case studies of academic interventions tackling a similar problem space. They consider existing expert research into what turns college students away from math-related pathways. Through this they create a shared map of barriers relevant to their purpose. Portions of this research indicate that students begin to lose interest in math-related fields by late secondary school, prompting the team to establish their target audience as 6th & 7th grade students with the intent that their intervention reduce this dropoff as their strategy for achieving their high-level purpose. Given this, they focus their targeted player transformations on students' beliefs about math relevance outside school—creating concrete reference points for students to call to mind common ways that math skills are useful for personal benefit in non-academic settings. The team establishes a bank of representative scenarios as the domain concepts key to their intervention design. Because they establish their audience as 6th & 7th graders but their high-level purpose is anchored on outcomes for college students, the team uses existing research on what beliefs or behaviors in secondary school have a predictive relationship with future math-engagement and use this information to design their assessment approach. It is important to note that this is an iterative process, and the result is a living document that is intended to evolve with the designers' understanding of the problem space as the project progresses, while still providing a guide to ensure the project proceeds in a manner aligned with their overall goals.

Socio-Ecological Modeling

Socio-Ecological Modeling (SEM) has been widely used in clinical research to better understand the multi-layered influences on a wide variety of complex systems, from colorectal cancer to bullying prevention. First formalized in the 1980's by Urie Bronfenbrenner [19, 20], Socio-Ecological Modeling was based upon his work over the previous decade to better understand the factors affecting human health [21]. His original socio-ecological model examined how health is affected by the interaction between the characteristics of the individual, the community, and the environment—including the physical, social, and political components. Subsequent work integrated the influence of policy.

As socio-ecological theory gained broader adoption, models were created to represent the multilayered influences that affect public health promotion, violence prevention, bullying among youth, dementia prevention, agricultural safety, and colorectal cancer [22–27]. More modern revisions of the model often represent the multilayered factors as concentric circles representing the individual, interpersonal, organizational, community, and policy spheres of influence.

Individual: Information about the attitudes, habits, and skills of an individual. May also include demographic information such as their age, gender, or race.

Interpersonal: The social network within which an individual resides–often this will be dominated by friends, family, and co-workers, but may also include any direct social connections.

Organizational: Institutions with rules and regulations that affect an individual or group. This level will often include schools or workplaces, but may also incorporate other less formal institutions such as artist collectives, agricultural partnerships, or criminal organizations.

Community: Relationships between different organizations, such as the relationship between a local high school and a community college, an environmental advocacy group and an oil producer, or any other inter-organizational relationship.

Policy: The social agreements which affect entities across the model. While these are commonly embodied in laws and regulations from the public policy sphere, cultural beliefs and social stigmas would also apply.

This representation serves to highlight the expanding sphere of influence of each layer of the model. As we move further away from the individual, the effect of each layer becomes more indirect, but is felt across all preceding layers.

While socio-ecological models have garnered some attention in the design community [28–30], they remain an underutilized tool for understanding the interplay of factors

affecting complex human systems. The lens of the socio-ecological model allows us to focus on a particular task-at-hand while still retaining the capability to account for the broader ecosystem within which that task exists. In this paper we present a methodology that leverages this strength of socio-ecological modeling to enable the creation of science gateway interface ecosystems, mutually reinforcing interfaces tailored for different tasks but serving a broader cohesive objective.

In Section "Methods" we will provide a demonstration of this methodology using an instantiation of the socio-ecological model within a specific domain, just as prior researchers have created instantiations related to public health promotion, bullying among youth, and dementia prevention [24, 25, 27]. We call this instantiation the Socio-Ecological Model of Change in the domain of Cyber Security (SEM-CCS). We will detail the elements in each layer of the SEM-CCS, moving from the individual level all the way up to the societal level, focusing our discussion at each level on the effects of identified elements on the potential for change to occur. Finally, we will examine how effects can propagate across levels of the model. In the subsequent section we will examine a set of design cases viewed through the lens of the SEM-CCS and transformational framework. We will examine how these cases can form a mutually reinforcing program that guides the target audience to further engage with the field of cybersecurity, without the need for coordination between the design teams to occur.

Methods

Below we will provide a detailed demonstration of the application of our approach for designing gateway interface ecosystems. We will take the general concepts discussed above of the transformational framework and socio-ecological modeling and detail their instantiation in this problem space. First, we will document the most recent iteration of the Socio-Ecological Model of Change in the domain of Cyber Security (SEM-CCS). This model will serve as the unifying basis for our discussion of interactions between all subsequent interface designs, as in each design engagement relevant elements of the SEM-CCS are extracted to create a usable, constrained subset for the current engagement. We will then document the iterative design process through which this subset of SEM-CCS elements is combined with other project specific information as inputs into the transformational framework and utilized to realize a bespoke intelligent interface.

Utilizing the context of these processes, we will then examine a series of case studies. In each case study we will focus our attention on the design process steps, the resultant outputs, and their affects on elements identified in the SEM-CCS. Finally, we will show how the combination of these independently designed cases creates a mutually reinforcing collective, and how the resultant interface ecosystem can serve to guide learners to further engagement with the subject matter.

The SEM-CCS

The problem of enacting change in the domain of cybersecurity is especially well suited to the application of socio-ecological modeling due to the diverse set of interacting stakeholders, adaptive response behavior on the part of actors in the ecosystem, and the extremely tight coupling of human activity to the nature of the affected environment. This diverse set of stakeholders now encompasses most individuals, households, corporations, and government agencies present worldwide. Even those groups not actively engaged in the practice of cybersecurity can affect outcomes, as their behavior forms the risk environment in which cybersecurity decisions must be made. Similarly, the escalating arms race between threat actors and defenders in the cyber domain means that the behavior of each group actively responds to the other. Finally, it is the tight coupling of human activity with the affected environment which may be the most pronounced, as one would struggle to envision an environment more tightly coupled to human activity than that of cyberspace—a domain wholly created and maintained through human activity, and that without such activity would shortly cease to exist entirely.

In Section "Socio-Ecological Modeling" we identified the general elements present in most socio-ecological models. However, it is only by instantiating these elements within an ecosystem that the general model becomes useful [23]. The SEM-CCS, as with many Socio-Ecological models, does this by utilizing a multi-layered representation including the individual, interpersonal, organizational, community and policy layers. These layers are best visualized utilizing a set of concentric circles highlighting the key factors present at each layer as seen in Fig. 1. This representation highlights how the effect of factors at higher layers is more indirect, but more broadly felt across lower layers of the model.

At the **individual** level of the SEM-CCS we have identified three key change-enabling attributes, **Need Identification**, **Change Advocacy**, and **Implementation Capability**. If individuals in an organization cannot identify the need for change, secure permission to enact change, and ultimately have the capability to implement the needed changes then change will not occur.

At the **interpersonal** level of the SEM-CCS we have identified that the degree of **Connections with Practitioners**,

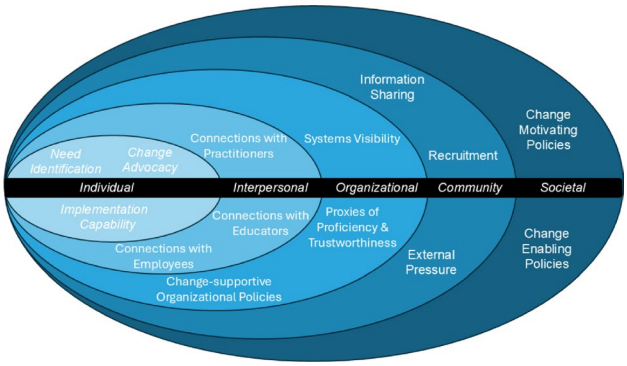

Fig. 1 A concentric circle representation of the SEM-CCS

Connections with Educators, and **Connections with Employees** are highly impactful in enabling change. An individual's connections with other cybersecurity practitioners positively affects their ability to enact change in the field, not only as a source of ongoing domain-relevant information but also as role models and career guides. Of particular note in this category is that connections need not be with a more senior practitioner; our research indicates that connections with peers or even more junior practitioners can yield significant benefits. Similarly, close connections with cybersecurity educators enable highly targeted support, tool-specific enrichment opportunities, and magnify the ability of early-career practitioners to advance into impactful roles. Finally, social connections to existing employees of an organization allow practitioners to more easily secure a cybersecurity position with that employer, and employees with a rich network within the organization were more likely to move into positions that allowed for change to be enacted. Notably, it does not appear to be the case that these social connections need to be with employees in a cybersecurity role.

At the **organizational** level of the SEM-CCS we have identified three key attributes, **Systems Visibility**, **Change-supportive Organizational Policies**, and **Proxies of Proficiency & Trustworthiness**, which affect cybersecurity change. Organizations with policies that prevent visibility into the state of all systems involved in a vulnerability will obscure the ability to detect that change is needed. Similarly, organizations with a culture that is supportive of challenging the status quo make it easier for individuals and groups to advocate for change, including in the cybersecurity domain. Organizational cultures that tend to punish "the squeaky wheel" make it unlikely that employees will feel comfortable calling out the need for change. Finally, many organizations note that their greatest hiring challenge is filling mid-level cybersecurity roles. These positions are advanced enough that employees must be trusted with carrying out core cybersecurity activities that require an elevated level of privilege. Without proxies of proficiency and trustworthiness employers are reluctant to allow individuals they perceive as novices to fill these roles due to the damage that they could cause—either through malicious action or incompetence.

At the **community** level of the SEM-CCS the degree of **Information Sharing**, **Recruitment**, and **External Pressure** impact the ability for cybersecurity change to occur. Organizations with strong relationships to other organizations in their sector who engage in information sharing are better able to enact change when responding to cybersecurity challenges. These relationships can be either producer/consumer such as organizations subscribing to threat feeds or purchasing consulting services, or they can be peer-facing, such as participation in sector specific consortiums, task forces, and fusion centers. Similarly, strong relationships between talent producers and consumers tend to allow organizations to meet their staffing needs and are thus better able to support change. Finally, inter-organizational relationships themselves can serve as sources of change, either through voluntary solicitation of change (external penetration tests, audits, work-study partnership projects), or through involuntary connections such as when organized groups apply external pressure. This external pressure can be enacted via legal avenues, such as awareness raising campaigns, boycotts, or shareholder advocacy or by employing less legal means such as those seen in the organized cyber-protests which utilized 4chan's Low Orbit Ion Cannon (LOIC) and associated website defacement campaigns.

The **policy** level of our model includes both **Change Motivating Policies** and **Change Enabling Policies**. Regulatory compliance or legal requirements are often a driver of enacted change as these change motivating policies can shift the incentive structure, encouraging organizations to take action where they may not have otherwise. Change enabling policies are distinct in that they have a direct bearing on the ability to enact change in cybersecurity. This could be through enabling individuals to acquire skills through education (FAFSA funding, NSF's Scholarship for Service program, and DoD's Cyber Service Academy scholarship), or by directly supporting organizations ability to enact change. An excellent example of direct organizational support policies are the Cybersecurity and Infrastructure Security Agency's Automated Indicator Sharing (AIS) program, Assessment Evaluation and Standardization (AES) program, CyberSentry Program, Joint Cyber Defense Collaborative (JCDC), Coordinated Vulnerability Disclosure Process, and Joint Ransomware Task Force (JRTF). These programs all provide information, methodologies, frameworks, and/or processes to enable organizations to enact cybersecurity changes within their organizations.

It is important to note the web of interconnections created by effects at high levels of the SEM-CCS upon lower levels.

Change Enabling Policies which support individual's education increase the pool of talent available for **Recruitment** at the community level, while educational attainment can create proxies of **Proficiency and Trustworthiness** to enhance the ability to enact change at the organizational level, create **Connections with Educators** at the interpersonal level, and enhance individuals abilities for **Need Identification**, **Change Advocacy**, and **Implementation Capability**. Similar interconnections exist across nearly all attributes of the SEM-CCS, and it is this high-degree of interconnectedness that can make designing in this domain so challenging. By utilizing the SEM-CCS we can identify the targets of a specific intervention at each level of abstraction and focus our intervention while still accounting for inter-dependencies across all levels.

Design Cases

We will now examine this process, its effects on the resultant interfaces and their impact. In the following examples the domain will remain constant and thus the Domain Concepts and much of the Prior Work will be similar, yet the Audience & Context, Transformations, and Barriers will vary between each application of this methodology and thus will result in wildly different interfaces. Despite the diversity of resulting designs, which were created by project teams that often never spoke to one another, the unifying underlying model ensured that the interfaces form a cohesive and mutually reinforcing program—one that guides the target audience to ever deeper levels of engagement with the field.

Engaging New Learners: Three Envelopes

We begin by presenting *Three Envelopes*, created to engage middle school students with cybersecurity as a precursor to considering cybersecurity careers. We were specifically interested in students who lacked access to cybersecurity education. Through our preliminary research, we found that not only were these students unfamiliar with cybersecurity, but they often lacked any knowledge of programming or computer networks, and in some cases did not even possess basic computing skills. Furthermore, the schools attended by our target population often lacked access to a computer lab, or had facilities that could not support cybersecurity training due to lack of computational resources, storage, or internet connectivity. Even outside the school context, many students in this population had no access to a digital device of any kind.

Our analysis of the audience and the barriers they faced suggested the design constraint of an *analog* intervention. Analog computer science education may seem paradoxical, but programs such as CS Unplugged have demonstrated their effectiveness at teaching core computational concepts [31, 32]. Currently, no comparable program exists for the domain of cybersecurity. We therefore needed to define the desired transformational outcomes ourselves, including any learning goals.

Middle school students would be the ones transformed by our intervention, and they typically do not belong to organizations in roles where they can make cybersecurity-relevant change. In defining our transformational goals, we therefore focused on the individual and interpersonal aspects of the SEM-CCS rather than the organizational, community, and societal layers. We already knew that access to computers was a barrier for our audience, so Implementation Capability was out. Similarly, it would be difficult to connect middle school students with practitioners or employees. However, Connections with Educators (interpersonal), Need Identification (individual), and Change Advocacy (individual) were all possible transformational targets.

Based on the core premise of the intervention, we began with a dispositional outcome:

1. Students increase their awareness of and interest in cybersecurity careers.

In order to meet this goal for our audience we chose to adopt a game-based learning strategy due to several factors. First, games provide an opportunity for consequential participation, that is, taking knowledgeable action while acting in a role and context that may have been previously foreign [33]; Creating such opportunities can be difficult to accomplish in schools through other means [34]. Second, game play can serve as an avenue for social permission to engage with a subject in which a community has not historically engaged, while also serving as an opportunity to build a self-identity that includes such participation [35, 36]. Finally, game-based learning strategies have proved effective as preparation for future learning, magnifying the impact of subsequent educational interventions [37].

As discussed above, the constraint of an analog intervention was required. Analog games are typically multi-player, which provided us with an easy strategy for building both Change Advocacy (individual) skills and Connections with Educators (interpersonal). If students were playing in teams, it would provide a context for them to make arguments to their teammates about what they should do. If the game could be deployed in a classroom, then educators could facilitate and engage with these conversations, even if they were not cybersecurity experts themselves.

2. Students can argue persuasively for a course of action to be taken with regard to cybersecurity.

3. Students can evaluate the persuasive value of other's argument's in the same space.
4. Students gain an appreciation for their teacher as a trusted party for seeking out information about cybersecurity.*Three Envelopes* uses a competitive-cooperative design to accomplish these transformational goals. Competitive-cooperative game designs have teams of players who cooperate with one another, and compete with other teams, similar to League of Legends, Charades, or even a trivia night. In the case of *Three Envelopes*, each team of players takes on the role of the board of directors of a company. Each turn, they must agree on what their company should do. This means they have to practice persuading their fellow teammates, as well as evaluating whether their teammates' own arguments are persuasive. Meanwhile, other teams are doing the same, competing against one another to run the most profitable business.

When students are not actively discussing choices among their team, teachers serve as facilitators—describing the choices that each team have made, reading event cards that affect all companies, and updating the scoreboard. This ensures that all students have visibility into the current state of the game, and can learn from and react to the choices made by other students' companies. However, when the students discuss their choices among the team, teachers provide advice and mediation support to help students guide their team's conversations to reach a consensus. This guidance serves as an opportunity for teachers to participate as a neutral third party, diffusing potentially adversarial situations and helping to build connections with individual students.

Finally, to improve their Need Identification (individual), we worked with cybersecurity practitioners to choose underlying concepts that would help students understand why cybersecurity is important. We identified the following knowledge outcomes:

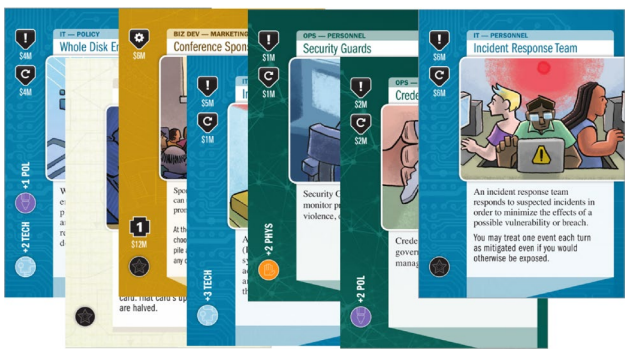

Fig. 2 Sample cards from Three Envelopes detailing choices of investments

5. Students can name different types of cyber attacks.
6. Students encounter broad classes of technology utilized in the practice of cybersecurity and how they relate to various attack types.
7. Students understand the difference between preventing, mitigating, and being exposed to an attack.

To accomplish these goals, we needed to design a system that would ask students to evaluate threats, identify possible technologies that could address those threats, and experience the consequences of preventing, mitigating, and being exposed to an attack. By connecting these to the decisions that teams had to make each turn, we could get students to discuss the risks and benefits of different strategies, reinforcing their Need Identification and supporting Change Advocacy at the same time.

In *Three Envelopes* as in the real world, students do not always know what threats are coming. Each turn, teams can choose to spend their money on cybersecurity-related investments, represented as cards (Fig. 2). These investments include things such as purchasing infrastructure, equipment and services, to implementing policies, or even hiring (and firing) staff. Each card includes information about what the card represents, its costs, aspects of cybersecurity it addresses (Technical Controls, Physical Security, Policies & Procedures, Workforce Security Awareness), and any special effects it may have on gameplay. At the end of each turn, the facilitator draws an event card, representing a cyber-attack. Each team evaluates how well their strategy protected them from the attack, which helps them draw connections between the technology and the attack types. Then the facilitator compares the outcomes of different teams, helping students see the different impact on companies that prevented, mitigated, or were exposed to the threat.

Three Envelopes has been deployed at several low-income schools in southwestern Pennsylvania, with several iterations of the game being played across multiple years at one middle school. This intervention has also been used across higher grade levels, from high-school to graduate school. Furthermore, *Three Envelopes* has seen use outside of the educational institution context that it was originally designed for, being adopted as a part of professional development activities providing continuing education credits for lawyers, to utilization as a workforce intervention during cybersecurity awareness month at a regional healthcare provider.

One event which the authors of this paper found particularly encouraging relating to the impact of *Three Envelopes* occurred while attending a graduation ceremony. A student who had played the game in previous years approached one of the authors to let them know that they had been accepted to college and intended to major in computer science with

a focus on cybersecurity, and stated that their interest in the field had been sparked by playing the game.

Providing Classroom Support: Cognitive Tutors

Once students are interested in cybersecurity careers, how might we support them in gaining technical skills? To answer this question, we looked at a common context where students first encounter hands-on cybersecurity training: a cybersecurity module within a programming class in junior or senior year of high school, or during an introductory course in a community college cybersecurity program. In both of these contexts, students had reliable access to computing devices and were familiar with using them. Both contexts had an instructor who was familiar with cybersecurity topics and, often, had prior experience teaching a cybersecurity curriculum.

However, while students had access to general computing devices, they did not have the ability to utilize cybersecurity relevant tools on these devices. For obvious reasons, administrators are rarely comfortable with students scanning, attacking, and defending systems on the school network. Additionally, many schools lack the ability to provide students in these courses with access to a cyber-range, which is a simulated environment for cybersecurity training,

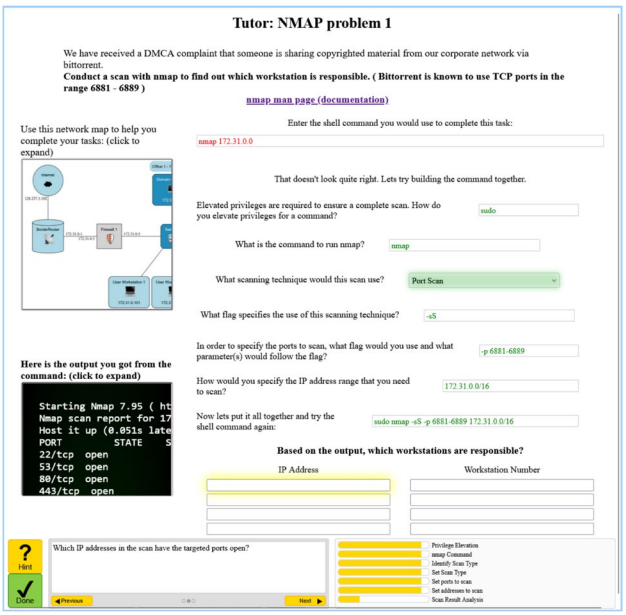

Fig. 3 An example of the tutor interface during a student interaction. The student's original attempt at specifying the nmap command (top, red) was incorrect and so the tutor provided additional scaffolding to walk the student through construction of the command (middle, green). Once the student was able to submit the complete command correctly (bottom, green), the output results appeared (bottom, left). The student then requested a hint in order to progress (bottom, yellow). Subsequent hint requests will provide increasingly specific guidance. Visible alongside this guidance is the current estimated mastery level of the student for each knowledge component (bottom, right)

where such tools can be used without risk to areas outside the range. Finally, although students all had a basic level of technology competence, they varied widely in prior cybersecurity knowledge and in their support needs. The high student-instructor ratio meant that students did not receive individualized support for these needs.

To address these barriers, we chose to explore a browser-based cognitive tutor. Delivering the learning intervention through the browser obviated the need for a cyber-range. The cognitive tutor uses a cognitive-behavioral approach, leveraging a model of the learner's mental state to provide feedback tailored to that learner's needs [38]. Cognitive tutors of this type have been shown to be more efficient than other teaching modalities when personalized human instruction is not feasible [39].

The technical skills addressed in the tutor had to be chosen such that they were relevant to both contexts, provided students with real actionable skills that they could take with them outside of the class context, and yet still did not have the potential to be misused (accidentally or maliciously). In order to simultaneously meet all these requirements we chose to focus on skills relating to nmap ("The Network Mapper"). This tool serves as one of the core tools in many cybersecurity professional's toolboxes [40], allowing its users to perform detailed scans of a wide variety of networks—locating systems, testing latency, checking configurations, and even identifying vulnerabilities can be accomplished. However, as actually exploiting vulnerabilities normally requires the utilization of different tools, the potential for misuse was limited.

Our browser based implementation, though, meant that actually utilizing the nmap tool would be impossible without the ability to connect to a cyber range. As such, our tutor provided a simulated interface to a fictitious computer, with procedurally generated output that mirrored what learners would see had they actually run the command within the network described in the problem on a computer with the appropriate cybersecurity tools installed (see Fig. 3).

A typical educational intervention with a cognitive tutor would focus primarily on gaining technical fluency, aligned with the Implementation Capability (individual) goal of the SEM-CCS. In turn, that might lead to transformational goals such as the following:

1. Students will learn how to operate the nmap scanning tool via the command line.
2. Students will learn how to utilize nmap to map out the state of a network.
3. Students will learn how to read scan output and identify changes needed to a network segment.

When first presented to a student the cognitive tutor displays a goal-directed task prompt which provides students with the relevant framing of the task they need to complete using nmap. Below this prompt is a link to the nmap 'man page' (short for manual). This 'man page' is the same documentation which would be available on a real system that had this utility, and which we frequently observed cybersecurity professionals consulting during cognitive task analyses conducted early in the development of the tutor.

Beneath the prompt and documentation link two items are presented side-by-side. An expandable network map, and a text entry area simulating a command prompt. This provides students with the opportunity to attempt to complete the task based upon the provided information. If a student inputs an nmap command that could be used to correctly complete the task, then they are immediately provided with simulated output that matches what their command would have produced, had it actually executed on a computer connected to the network in the diagram. This output is provided in an expandable window that replicates the look and feel of Linux terminal output.

However, if the student's first attempt was incorrect, the tutor system would provide them with a series of prompts which break down the construction of a correct nmap command into its components, and provide additional scaffolding. At each step the system provides the student with the ability to ask for one or more hints, each of which provides additional guidance on how to complete that step. Once the student has correctly input all the components of a correct nmap command, they are given another text entry area within which they may repeatedly attempt to enter a correct command, at which point they will receive the scan results described above.

Utilizing these scan results students can then attempt to complete the task they were given. Throughout this entire process each action a student takes, be it a correct entry, a mistake, or a request for a hint, is tracked by the system in order to provide feedback. Correct answers are highlighted in green, incorrect answers in red. Additionally, the system utilizes a Bayesian Knowledge Tracing (BKT) algorithm [41] to estimate the students' current mastery level over a set of knowledge components which are mapped to each of the transformational goals listed above (#1–3). An example run of the tutor is visible in Fig. 3. Additional problems can be provided until mastery is achieved for all components.

In addition to learners' *technical* ability to use nmap, we aimed to support their *self-efficacy* with nmap. Self-efficacy measures learners' belief in their own ability to solve problems. For example, learners with high cybersecurity self-efficacy believe that they have the tools they need to solve cybersecurity problems, and that they can use those tools successfully in practice [42]. We therefore also consider the following dispositional goal:

4. Students will increase their self-efficacy with using nmap.

By presenting actionable tasks in our tutor and guiding students to successfully complete them, we allow students to demonstrate to themselves their ability to complete these tasks. Subsequent tasks leverage the same knowledge components, allowing students to observe the improvement to their accuracy (correct answers) and fluency (speed at which they provide the correct answer), building their self-efficacy with the nmap utility. Similar tutoring systems in other domains have shown that such increases in accuracy and fluency within the tutor were associated with increases in student self-efficacy related to the tutored topic [43].

Beyond these individual transformations, we saw ways to augment our tutor to accomplish additional learning outcomes related to higher levels of the SEM-CCS. A standard "classroom" approach to nmap treats it as if the tool exists in a vacuum. However, in real-world contexts, organizations may provide limited visibility into their systems (Systems Visibility), and even a tool as apparently simple as nmap intersects with policy and regulatory issues (Change Motivating Policies). Could we train students to understand the limitations and opportunities around how nmap might be implemented in practice?

We translated these opportunities into two transformational goals:

5. Students will be able to map networks even when the associated network documentation is incorrect or incomplete.
6. Students will understand how policy and regulatory enforcement can be accomplished utilizing network scanning.

We realized that we could advance toward these goals by embedding nmap tutor use in *contextualized scenarios*, where students would operate as if they were in a real workplace. The traditional classroom examples were rewritten to provide additional context, giving students not only the "what" of the task, but also the "why". Importantly, as only the question prompt changed, no additional technical development costs were incurred in addressing these factors of the SEM-CCS.

By working backward from the incorrect documentation goal (transformation 5), we designed problem narratives that include the identification of rogue workstations which are on the network but do not appear in the company's documentation, implemented by simply removing some items

from the existing network map. While the policy and regulatory enforcement goal (transformation 6) was addressed with problem narratives including the identification of systems that are operating applications outside of those approved by management, or configured against regulations. For example, the example problem in Fig. 3 includes a DMCA complaint that has been received about copyrighted material being shared from within the corporate network, and relevant technical information about how such peer to peer file sharing would be exhibited on the network was provided. Students were then asked to identify the offending workstation(s).

Heuristic evaluations of the tutor have been completed by a group comprising both novice and experienced graduate students, as well as instructors of high school and community college cybersecurity programs. We are currently preparing for a full deployment which will be integrated into high school and college classrooms as a part of a study scheduled for the upcoming semester.

Creating Immersion: Battlefield Simulator

Classrooms are not the only learning opportunity for students to build their confidence with hands-on technical cybersecurity skills. Learners can also encounter cybersecurity in OST (out of school time) settings, such as afterschool programs or community events. In this case, we had the opportunity to work with a summer camp that offered a week-long cybersecurity program.

As with our cognitive tutors, this intervention was aimed at older teens and young adults. Learners traveled from all over the region to attend this camp. While this signaled high levels of interest in the topic, it also meant that many students did not know other participants, in contrast to our work in high-school and college environments. There was also higher variation in participants' prior knowledge, compared to students who were already engaged in traditional classroom instruction.

Given the similarities in the audience, we aimed to target the same elements of the SEM-CCS: Implementation Capability (individual), Need Identification (individual), and Systems Visibility (organizational). However, differences in the context meant we had to approach the design in a different way.

Fig. 4 A view of the immersive interface environment

Unlike the schools described above, the camp had access to a fully-featured and mature cyber-range thanks to a generous donation from a local organization with excess simulation capacity. Students also had access to a full virtual world, representing all the people, systems, and networks acting within the environment. However, the system was designed for experienced professionals, and could not be directly modified to meet the needs of the teenage learners. Any changes we made had to be in the form of supportive scaffolding *around* the cyber-range and associated simulation, rather than changing the system itself. This created a substantial interface design challenge.

Because we had so little flexibility in modifying the simulation, we analyzed what the *unmodified* simulation could provide for learners, without requiring them to spend the entire week struggling with incomprehensible and inappropriate interfaces. Based on this analysis, we identified the following transformations:

1. Participants will gain an appreciation for how porous unhardened computing systems can be.
2. Participants will learn basic security best practices for hardening a Windows system.
3. Participants will gain self-efficacy in their ability to execute such hardening activities.
4. Participants will gain an understanding of how cyber-physical effects can propagate from cyberspace into the real world, and vice versa.

Because of the summer camp context, we identified *immersive design* as a way to support students toward these learning goals. Immersive design uses physical props and narrative design to bring learners into a fictional environment, similar to an escape room. Because the camp had its own physical space, we had the resources needed to take this approach. We converted one of the camp's rooms into "FOB Kyle", a forward operating base supporting special forces operations. The room itself was augmented with camo netting, task-focused lighting, and ambient sounds being piped in to mimic an active forward operating base, including the sounds of equipment being moved and helicopters taking off and landing (see Fig. 4).

Participants were briefed on their tasking—secure critical systems and support the operations of a special forces team that has been dispatched to rescue an American citizen being held hostage abroad in the midst of an ongoing cyber attack.

In order to defend against the ongoing cyber attack participants received step by step instructions for hardening

the Windows systems that were being attacked, supporting transformation 2. In addition to the instruction packet, volunteer camp staff (who were themselves subject matter experts in cybersecurity and/or ISC2 members) were on-hand to provide support as needed. Participants were then able to see the effect of their hardening activities, as systems were able to resume operations, supporting transformation 3.

Participants coordinated with the fictional team of special operators "in the field" as they worked to secure the operation and provide ongoing support through the simulator. In support of transformation 1, we ensured that as a part of these support activities the participants needed to gain access to security camera feeds in order to find the hostage, and to compromise the building management system to gain control over the lighting systems. Similar step-by-step instructions and in-person support was available for these tasks, though due to the unhardened nature of the systems, the written instructions were sufficient in all cases without further assistance, showcasing how vulnerable such systems are.

Additionally, the participants had to pilot a virtual reconnaissance drone to guide the special operator's movements to avoid them encountering enemy forces. The control system for this drone was one of the systems the participants hardened. If not properly secured, the drone connection would be lost at a key moment in the simulation. Both this activity, and the utilization of the building's camera system and lighting for gaining advantage in the rescue operation showcased how effects can cross the cyber/real world border, supporting transformation 4.

Without the benefit of the immersive environment, the remaining simulation would have been a technical exercise that the participants walked through, without context or visibility into the repercussions or outcomes of their actions. By wrapping the exercise in a narrative and immersing the players in the environment, we could serve our transformational goals without modifying the digital cyber-range interface.

Transitioning to the Workforce: Cyber SimLab

Once students have an interest in cybersecurity and have developed their technical skills, they need support in becoming effective professionals. Community colleges are a particularly good target for this type of support, as students may either go directly to the workforce or continue their education in a four-year institution, depending on their career goals. We partnered with a local community college's cybersecurity program and identified that their capstone course was meant to serve this role, either helping students secure an entry-level position or transfer to another institution for further study. Because the ultimate goal was to prepare students for the workforce, we identified two audiences who needed to be served by our intervention: students and employers.

Students entering the capstone had substantial technical training from their previous coursework in the program, emphasizing Need Identification (individual) and Implementation Capability (individual). However, students did not receive any training in how to deploy their technical skills effectively in an organizational context (e.g. Change Advocacy). While some students received instruction in persuasive argumentation and writing in English classes, at no point in the previous program were they able to exercise these skills in a technical context. Without opportunities to practice these skills, graduating students lacked the skills to communicate effectively to both other practitioners and to a non-technical audience. Additionally, the program did not offer internships or other opportunities to make contact with working professionals. Without these relationships, students struggled to secure initial placement in the cybersecurity field, potentially resulting in their abandonment of the pursuit despite already making significant investment.

Employers, on the other hand, found hiring effective cybersecurity workers to be risky and difficult. Cybersecurity workers have privileged access to a company's systems, and therefore have the potential to do significant damage, either accidentally or maliciously. Employers therefore must place significant trust in a candidate to offer them a cybersecurity position. Because they have only two years of training, students from a community college background are less likely to be considered for these roles. Even when they do manage to secure employment in these roles, they are often unfamiliar with how to operate effectively in an organizational context. It can be months or even years before they can effectively contribute to positive change within the organization, causing their careers to lag behind those of their peers.

We saw the opportunity to address these problems *together*. The capstone course had previously emphasized solely technical skills. We could work with instructors to redesign the capstone course to emphasize how those skills could be used for organizational change. At the same time, we could engage practitioners and employees of target organizations as a way of building trust in the students' skills. Framed in terms of the SEM-CCS, extending the interpersonal level in this way would help participants build connections that would help them secure employment or scholarship opportunities. Accounting for organizational factors such as Proxies of Proficiency & Trustworthiness, and Change-Supportive Organizational Policies would help address systemic challenges these students would otherwise face, while simultaneously helping to affect Recruitment

challenges at the community level. Even factors at the societal level, such as change motivating policies, were considered during the design of Cyber SimLab.

Combining these sets of barriers with the identified areas of focus in the SEM-CCS we can extract a set of applicable transformations for each audience. Applicable transformations for the student audience are:

1. Students refine their technical skills at identifying vulnerabilities and addressing them.
2. Students learn to argue persuasively about technical topics in front of both technical and non-technical audiences.
3. Students learn to incorporate organizational context into technical arguments, matching their arguments to organizational priorities.
4. Students learn to operate within the established policies and procedures of an organization.
5. Students create connections with local employees and practitioners.

While the transformations applicable to the employees of regional cybersecurity employers are:

6. Employees will gain a more favorable perception of the cyber capabilities of community college students.
7. Employees will generate new connections with community college members.

To address these goals, we combined a technical platform with a novel pedagogy. Students engaging with Cyber SimLab were provided with access to the (virtualized) infrastructure of a fictional company—Secure Skies Inc. This fictional company was designed to replicate not only the network infrastructure but also the organizational realities of a real world company. From internal office politics to formalized policies and procedures, operating within the context of Secure Skies Inc would mirror operating in the real world. Students were tasked with conducting a penetration test with the goal of identifying potential vulnerabilities in the corporate network (transformation 1). However, rather than fix these vulnerabilities directly, as in most similar classes, students had to follow corporate policy and submit a formal change request, with an accompanying change management plan (transformation 4). The students would then present this plan to upper management and seek permission to enact the proposed changes (Transformation 2 & 3). Finally, after negotiating with upper management and coming to an agreement on which changes to enact, the students would return to the environment and implement the changes.

Critically, we recruited technical and non-technical managers from regional employers to take the role of Secure Skies Inc. upper management (Transformation 5 & 7). By attending these presentations, these employees could see the effectiveness and capability of the community college graduates in the context of challenges similar to those faced by their organizations (transformation 6). Not relegated to mere passive viewers of the presentation, by engaging in the active negotiation with the students about what actions to take, we further support transformations 5–7.

These presentations served as opportunities to build connections not only between the capstone students and practitioners, but also as an organizational bridge, connecting organizations across the community with cybersecurity recruitment needs into the talent pipeline represented by the community college. However, what about organizations who could not send representatives to the capstone class? To create a proxy of proficiency and trustworthiness to employers beyond those directly involved in the presentations, we designed a new certificate for students completing the program. The top-line branding includes the name of one of the most well respected research universities in the cybersecurity space, and beside the student's name appears the seal of the federally funded research and development center which arguably helped to define the modern field of cybersecurity. The certificate itself is co-signed by both a senior researcher from the above institutions as well as the course instructor from the community college partner.

The initial cohort of Cyber SimLab has completed the course and graduated from the program. Of the cohort, half of the students transitioned to a four year degree program, with at least one of the students securing a prestigious scholarship which included an employment clause in the field post-graduation. This compares with the previous cohort which included no students which, to our knowledge, continued to a four year degree program or received job offers in the field. By participating in the Cyber SimLab experience students are more likely to transition into a career in the field, and better equipped to identify, advocate, and implement change where it is needed. Similarly, based upon the result of subsequent interviews with the participating employees, they believe that their organizations are better able to identify talent that meets their needs, and more likely to allow this broader talent pool the opportunity to enact change.

Discussion

In this paper, we argue that using the Transformational Framework together with Socio-Ecological Modeling can help designers create intelligent interfaces to *different*

underlying systems that together form a mutually reinforcing, integrated collective. The cases described here involved dozens of stakeholders, including instructors, curriculum designers, game designers, employers, and, of course, researchers. Our design tools helped us stay aligned on the ultimate goals of our *ecosystem* of interventions, even when contributors had different professional positions, languages, disciplinary or theoretical perspectives, motivations, and resource contexts. The same toolkit that helped our diverse teams create innovative, well-targeted interventions also enables designers who never interact with one another to identify and account for interdependencies and to build on one anothers' efforts (see Fig. 5).

The design cases we describe above may, on the surface, seem very different from one another. *Three Envelopes* is an analog game for middle schoolers, while Cyber SimLab is a semester-long capstone class for community college students. The nmap cognitive tutor helps learners master a single tool using a browser, while the summer camp had access to a full cyber-range and associated simulation. However, we argue that these differences in fact reflect the strengths of an ecosystem approach. Wicked problems, such as transforming the cybersecurity workforce, call for solutions that address different parts of the problem while creating pathways for deeper exploration, engagement, and connection. Different interfaces within an ecosystem can use multiple approaches to learning design, support learners at different levels of proficiency, and be accessible to many types of learners through personalized learning pathways.

One strength of this approach is for designs within the same ecosystem to embody different theories of learning. For example, cognitive approaches to learning emphasize the underlying mental representations and processes of the learner. As suggested by the name, cognitive tutors take a primarily cognitive approach. They provide structured opportunities for problem-solving, use learner input to hypothesize about the learner's underlying mental model, and provide targeted feedback to help learners build more appropriate representations and processes [44]. Our nmap tutor sits squarely within this tradition. On the other hand, *Three Envelopes* emphasizes constructivist learning, where players collaborate to weigh the strengths and weaknesses of various approaches and, together, build a deeper understanding of the technologies used in cybersecurity and their relevance to different types of attacks [45]. Cognitive approaches to learning typically do not ask learners to participate in collaborative meaning-making, while constructivist learning experiences generally do not scaffold learners in building new mental representations. Of course, many learning experiences incorporate aspects of multiple theories. For example, our immersive simulation incorporates humanist confidence-building interventions alongside

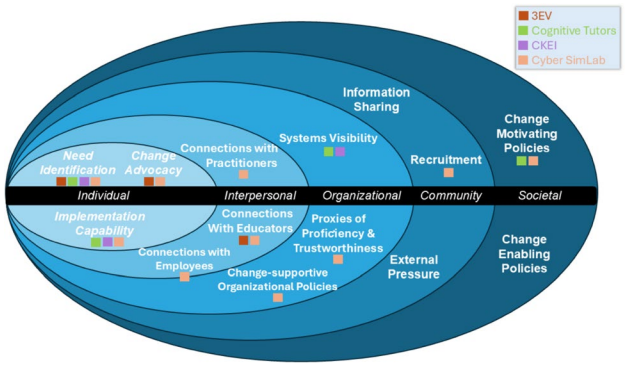

Fig. 5 Design cases as mapped to the SEM-CCS

connectivist designs to facilitate acquisition and sharing of knowledge through interaction with cyber-human networks [46, 47]. In the long term, however, being able to build learning pathways that *link* experiences focused on different learning theories supports learners in developing a range of outcomes, such as motivation, interest, excitement; cognitive or procedural learning; proficiency in specific skills; socioemotional learning; or deeper engagement with learners' metacognition, values, peers, community, and broader socio-technical context.

The integrated application of the Transformational Framework and Socio-Ecological Modeling can also be used as an analytical toolkit. Educators and educational systems frequently identify existing resources, many of which were not originally designed as learning interventions, and leverage them to promote learning. Found assets such as games and illustrations can enhance students' learning experiences, but educators are often overwhelmed by the sheer number of resources available to them. The Transformational Framework and SEM can be used to analyze existing interfaces on multiple scales in order to determine whether a given intervention is a good fit for a particular context of learning or cohort of learners, or alternatively to identify best-fit opportunities for implementation. In this paradigm, the evaluator would first consider the specific motivation for adopting the intervention by identifying the transformation or transformations that are desired. By working through the Framework, we can think holistically about the impact of specific features of the intervention. The SEM can then be used to identify and distinguish the projected impacts of the intervention at multiple levels throughout the broader learning environment and make a well-informed decision about adoption *or* a well-designed plan for implementation. It is important to note that the transformation guiding the choice of SEM should be focused on the desired end-outcome, not the process by which it is achieved, and thus need not even be directly focused on learners as an end goal. For example, the SEM-CCS chosen for this paper's analysis is focused on creating organizational change in the domain of

cybersecurity, and as a result effects on learners are an artifact of this process but not its goal.

This analytical approach may be used to develop experimental interventions which are ready for translation for use in practice. Proven educational interventions may be well-designed to test principles and demonstrate impact on learners [48] but may not be designed nor evaluated for use under real-world conditions. Research has consistently shown that educators struggle to implement proven tools effectively once the developers or researchers move on to the next project [49], and educators, learners, and school systems are left with a functional intervention and without the support to deliver the interventions consistently and effectively [50, 51]. This challenge is more acute when the intervention is technologically complex [52]. In recent years, some efforts to narrow the research-practice gap have included rubrics to evaluate evidence-based interventions for use in school contexts [53] and to assess student readiness for educational technologies [54]. The toolkit described here can be used by researchers to identify barriers to, and opportunities for, implementation by highlighting stakeholders and interdependencies that are critical for adoption of an educational intervention into any new context of use. As researchers and developers pursue experimental aims, the integrated toolkit can indicate documentation and foundations that enable translation from a research intervention to use in broader practice.

Additionally, we note that the cases we have presented can be chained together for a longer-term learning experience. Younger audiences exposed to Three Envelopes gain a broad understanding of cybersecurity, and their interest may encourage them to seek out further learning opportunities such as a summer camp or cybersecurity elective. These experiences in turn prepare them for formal training, where an approach like Cyber SimLab can help them make this pursuit a reality by securing their employment in the field. However, we believe that there are also unexplored opportunities to design *specific* transitions within a learning pipeline. While this has been beyond the scope of our work to date, we see that aspects of the SEM-CCS could be linked to existing strategies for helping learners navigate a complex ecosystem, such as microbadging [55]. We envision, for example, a site where learners can search for cybersecurity learning opportunities based on which elements of the SEM-CCS they foster. The system might also make recommendations to learners about experiences that pair well together. For example, game-based learning is good at giving learners a space to develop their intuitions about a field, but often needs support beyond the game to help players translate what they learn into explicit and formal knowledge [56]. Learners who engage a cybersecurity system through a game-based interface might be recommended to watch a video where a cybersecurity professional plays the game and discusses how the material connects to their job, or to a class that covers similar topics.

Finally, a significant strength of this toolkit is its role as a entry point to designing for a learning ecosystem. Designers in many roles, disciplines, and learning contexts can replicate this approach, create novel interfaces that contribute to a gateway interface ecosystem, and extend the impact of each specific educational resource far beyond its utility as a stand-alone product. To do so, designers apply the Transformational Framework process by answering a series of questions to guide development of design constraints based on desired learner outcomes. In answering these questions, the team applies a socio-ecological lens to assist in identifying the appropriate audience and context, desired player transformations, applicable barriers, and the relevant domain concepts. This may entail developing a SEM for their domain, or identifying a SEM created by others. In concert, this design toolkit enables the creation of novel learning experiences that complement, mutually reinforce, and amplify the impact of other learning experiences within the ecosystem. Though the cases described in this paper were designed by different teams that each engaged dozens of stakeholders, we present them because the authors have been involved in their design. The Transformational Framework and Socio-Ecological Model can enable other designers to work in this problem space, build innovative designs that our teams would not have dreamt of, and add new interventions in support of learning and development that are amplified, integrated, and reinforced through their integration with our cases and the larger learning ecosystem.

Conclusion

In this paper, we argued that an *ecosystems approach* to science gateways can help designers create personalized, intelligent interfaces that support learning in very different contexts and for very different audiences. We shared two design tools that, in tandem, can help accomplish this goal: the Transformational Framework and Socio-Ecological Modeling. We show how these tools can be used to design interventions in the domain of cybersecurity, where there is both an acute need for trained professionals and a lack of successful interventions to address this need. We first presented the SEM-CCS, an example of how a socio-ecological approach can be applied to a specific knowledge domain. We then shared four case studies with highly divergent learner populations and contexts of deployment. For each case, we showed how the transformational framework and the SEM informed the choice of platform and the execution

of the educational intervention. Finally, we show some of the long-term benefits and opportunities of this approach.

Author Contributions All authors whose names appear on this submission have made substantial contributions to the work; participated in the writing and revision process; approved the version to be published; and agree to be accountable for all aspects of the work. Guttman, Hammer, and Herckis participated in the design and deployment of one or more of the case studies described in this paper, as well as the cross-case synthesis and analysis. Culyba, and Hymes provided critical intellectual background for framing the work, and contributed to the development of the ecosystems approach described in the paper.

Funding Open Access funding provided by Carnegie Mellon University. Classroom utilization of Three Envelopes and Cognitive Tutors discussed in Sections "Engaging New Learners: Three Envelopes" and "Providing Classroom Support: Cognitive Tutors" were conducted as unfunded STEM outreach projects. The summer bootcamp discussed in Section "Creating Immersion: Battlefield Simulator" was hosted by ISC2, with volunteer staff and donations provided by ISC2 member organizations. Cyber SimLab, discussed in Section "Transitioning to the Workforce: Cyber SimLab", was funded by the National Science Foundation award FW-HTF-R: A New Bridge to the Digital Economy: Integrated AI-Augmented Learning and Collaboration.

Data Availability Not applicable.

Materials Availability Not applicable.

Code Availability Not applicable.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

Ethical Approval and Consent to Participate This paper describes the design of interventions, not human subjects research. Outside of the scope of this paper, all studies conducted with the interventions described have been approved by the lead author's IRB.

Consent for Publication Not applicable.

References

1. Wilkins-Diehr N. Special issue science gateways–common community interfaces to grid resources. Concurr Comput Pract Exp. 2007;19(6):743–9. https://doi.org/10.1002/cpe.1098.
2. Global Cybersecurity Outlook. Insight Report, World Economic Forum (January 2025). https://www.weforum.org/publications/global-cybersecurity-outlook-2025/. Accessed 19 Sep 2025.
3. Gartner Survey Reveals 63 % of Organizations Worldwide Have Implemented a Zero-Trust Strategy. 2024. Accessed 20 Sep 2025.
4. Gilad Y, Cohen A, Herzberg A, Schapira M, Shulman H. Are we there yet? On RPKI's deployment and security. In: Proceedings 2017 Network and Distributed System Security Symposium. Internet Society, San Diego, CA. 2017. https://doi.org/10.14722/ndss.2017.23123.
5. Cyber Readiness Institute: Unlocking MFA Adoption: Why Small and Medium-Sized Businesses Must Act Now to Strengthen Their Cybersecurity. 2024. https://cyberreadinessinstitute.org/resource/unlocking-mfa-adoption-why-small-and-medium-sized-businesses-must-act-now-to-strengthen-their-cybersecurity/. Accessed 15 Jan 2025.
6. Samotshozo LB-P. Examining factors hindering cybersecurity professionals from effectively implementing security controls for federal information systems. D.Sc.: Capitol Technology University, United States—Maryland; 2020.
7. Gale M, Bongiovanni I, Slapnicar S. Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. Comput Secur. 2022;121:102840. https://doi.org/10.1016/j.cose.2022.102840.
8. Wessels M, Brink P, Verburgh T, Cadet B, Ruijven T. Understanding incentives for cybersecurity investments: development and application of a typology. Digital Bus. 2021;1(2):100014. https://doi.org/10.1016/j.digbus.2021.100014.
9. Joint Task Force On Cybersecurity Education: cybersecurity curricula 2017: curriculum guidelines for post-secondary degree programs in cybersecurity. ACM, New York, NY, USA 2018. https://doi.org/10.1145/3184594. Accessed 28 Dec 2024.
10. Cabaj K, Domingos D, Kotulski Z, Respício A. Cybersecurity education: evolution of the discipline and analysis of master programs. Comput Secur. 2018;75:24–35. https://doi.org/10.1016/j.cose.2018.01.015.
11. Dawson J, Thomson R. The future cybersecurity workforce: going beyond technical skills for successful cyber performance. Front Psychol. 2018;9:744. https://doi.org/10.3389/fpsyg.2018.00744.
12. Chigbu BI, Ngwevu V, Jojo A. The effectiveness of innovative pedagogy in the industry 4.0: educational ecosystem perspective. Soc Sci Hum Open. 2023;7(1):100419. https://doi.org/10.1016/j.ssaho.2023.100419.
13. Bocking S. Visions of nature and society: a history of the ecosystem concept. Alternatives. 1994;20(3):12–18.
14. Bandyopadhyay S, Bardhan A, Dey P, Bhattacharyya S. Bridging the education divide using social technologies: explorations in rural India. Singapore: Springer; 2021. https://doi.org/10.1007/978-981-33-6738-8. (**Accessed 2026-02-04**).
15. Falk JH, Dierking LD, Staus N, Wyld J, Bailey D, Penuel W. Taking an ecosystem approach to stem learning: the synergies project as case study. Connect Sci Learn. 2016;1(1):12420441.
16. Benita F, Virupaksha D, Wilhelm E, Tunçer B. A smart learning ecosystem design for delivering data-driven thinking in STEM education. Smart Learn Environ. 2021;8(1):11. https://doi.org/10.1186/s40561-021-00153-y.
17. Falk JH, Dierking LD. Viewing science learning through an ecosystem lens: a story in two parts. In: Corrigan D, Buntting C, Jones A, Loughran J, editors. Navigating the changing landscape

of formal and informal science learning opportunities. Cham: Springer; 2019. p. 9–29. https://doi.org/10.1007/978-3-319-89761-5_2.
18. Culyba S. The transformational framework: a process tool for the development of transformational games. Pittsburgh: Carnegie Mellon University; 2018.
19. Bronfenbrenner U. Ecology of the family as a context for human development: research perspectives. Dev Psychol. 1986;22(6):723–42. https://doi.org/10.1037/0012-1649.22.6.723.
20. Bronfenbrenner U. Ecological systems theory. In: Vasta R, editor. Six theories of child development: revised formulations and current issues. London: Jessica Kingsley Publishers; 1992. p. 187–249.
21. Bronfenbrenner U. Toward an experimental ecology of human development. Am Psychol. 1977;32(7):513–31. https://doi.org/10.1037/0003-066X.32.7.513.
22. CDC: Colorectal Cancer Control Program. Archived: 2024. https://www.cdc.gov/colorectal-cancer-control/index.html. Accessed 15 Jan 2025. http://medbox.iiab.me/modules/en-cdc/www.cdc.gov/cancer/crccp/sem.htm
23. Lee BC, Bendixsen C, Liebman AK, Gallagher SS. Using the socio-ecological model to frame agricultural safety and health interventions. J Agromed. 2017;22(4):298–303. https://doi.org/10.1080/1059924X.2017.1356780.
24. Mace RA, Cohen JE, Lyons C, Ritchie C, Bartels S, Okereke OI, et al. Socio-ecological barriers to behavior change-oriented dementia prevention: a qualitative study of healthcare professionals' perspectives. Aging Ment Health. 2024. https://doi.org/10.1080/13607863.2024.2430525.
25. Swearer SM, Espelage DL. Introduction: a social-ecological framework of bullying among youth. In: Espelage DL, Swearer SM, editors. Bullying in American schools. Routledge, pp. 23–34.
26. Riner ME, Saywell RM. Development of the social ecology model of adolescent interpersonal violence prevention (SEMAIVP). J Sch Health. 2002;72(2):65–70. https://doi.org/10.1111/j.1746-1561.2002.tb06517.x.
27. Wold B, Mittelmark MB. Health-promotion research over three decades: the social-ecological model and challenges in implementation of interventions. Scand J Pub Health. 2018;46(20):20–6. https://doi.org/10.1177/1403494817743893. (**PMID: 29552963**).
28. Hirsch T, Lim C, Otten JJ. What's for lunch? A socio-ecological approach to childcare nutrition. In: Proceedings of the 2016 ACM Conference on Designing Interactive Systems. DIS '16, pp. 1160–1171. Association for Computing Machinery, New York, NY, USA 2016. https://doi.org/10.1145/2901790.2901793. Accessed 24 Dec 2024.
29. Mohd Mohadis H, Mohamad Ali N. Using socio-ecological model to inform the design of persuasive applications. In: Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, pp. 1905–1910. ACM, Seoul Republic of Korea 2015. https://doi.org/10.1145/2702613.2732835. Accessed 24 Dec 2024.
30. Kapuscinska A, Bhujwala PM, Kalarchian M, Hammer J. A socio-ecological approach to activity games for girls. In: Proc. ACM Hum.-Comput. Interact. 2021;5(CHI PLAY):246–124628. https://doi.org/10.1145/3474673. Accessed 12 Jan 2025.
31. Battal A, Afacan Adanır G, Gülbahar Y. Computer science unplugged: a systematic literature review. J Educ Technol Syst. 2021;50(1):24–47. https://doi.org/10.1177/00472395211018801.
32. Thies R, Vahrenhold J. Back to school: computer science unplugged in the wild. In: Proceedings of the 2016 ACM Conference on Innovation and Technology in Computer Science Education, 2016;118–123. ACM, Arequipa Peru. https://doi.org/10.1145/2899415.2899442. Accessed 23 Jul 2024.
33. Gresalfi M, Barab S, Siyahhan S, Christensen T. Virtual worlds, conceptual understanding, and me: designing for consequential engagement. On the Horizon The Intl J Learn Futures. 2009;17(1):21–34. https://doi.org/10.1108/10748120910936126.
34. Barab S, Pettyjohn P, Gresalfi M, Volk C, Solomou M. Game-based curriculum and transformational play: designing to meaningfully positioning person, content, and context. Comput Educ. 2012;58(1):518–33. https://doi.org/10.1016/j.compedu.2011.08.001.
35. James DiSalvo B, Yardi S, Guzdial M, McKlin T, Meadows C, Perry K, Bruckman A. African American men constructing computing identity. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '11, pp. 2967–2970. Association for Computing Machinery, New York, NY, USA; 2011. Accessed 26 Oct 2023 https://doi.org/10.1145/1978942.1979381
36. DiSalvo B, Guzdial M, Meadows C, Perry K, McKlin T, Bruckman A. Workifying games: successfully engaging African American gamers with computer science. In: Proceeding of the 44th ACM Technical Symposium on Computer Science Education, pp. 317–322. ACM, Denver Colorado USA; 2013. Accessed 28 Aug 2023. https://doi.org/10.1145/2445196.2445292
37. Black JB, Khan SA, Huang S-CD. Video and computer games as grounding experiences for learning. In: Learning by playing: video gaming in education. Oxford University Press. https://doi.org/10.1093/acprof:osobl/9780199896646.003.0020.
38. Corbett AT, Koedinger K, Hadley WS. Cognitive tutors: from the research classroom to all classrooms. In: Goodman P, editor. Technology enhanced learning. Routledge; 2001. p. 26.
39. Steenbergen-Hu S, Cooper H. A meta-analysis of the effectiveness of intelligent tutoring systems on college students' academic learning. J Educ Psychol. 2014;106(2):331–47. https://doi.org/10.1037/a0034752.
40. Alhamed M, Rahman MMH. A systematic literature review on penetration testing in networks: future research directions. Appl Sci. 2023;13(12):6986. https://doi.org/10.3390/app13126986.
41. Corbett AT, Anderson JR. Knowledge tracing: modeling the acquisition of procedural knowledge. User Model User-Adap Inter. 1994;4(4):253–78. https://doi.org/10.1007/BF01099821.
42. Wee JMC, Bashir M, Memon N. Self-Efficacy in cybersecurity tasks and its relationship with cybersecurity competition and Work-Related outcomes. In: 2016 USENIX Workshop on Advances in Security Education (ASE 16). USENIX Association, Austin, TX; 2016. Accessed 04 Dec 2023 https://www.usenix.org/conference/ase16/workshop-program/presentation/wee
43. Bernacki ML, Nokes-Malach TJ, Aleven V. Examining self-efficacy during learning: variability and relations to behavior, performance, and learning. Metacogn Learn. 2015;10(1):99–117. https://doi.org/10.1007/s11409-014-9127-x.
44. Shute VJ, Zapata-Rivera D. Adaptive technologies ETS Research Report Series. 2007;2007(1):34. https://doi.org/10.1002/j.2333-8504.2007.tb02047.x.
45. Mayer RE. Designing instruction for constructivist learning. In: Reigeluth CM, editor. Instructional-design theories and models. Routledge; 1999 , pp. 141–159
46. Tangney S. Student-centred learning: a humanist perspective. Teach High Educ. 2014;19(3):266–75.
47. Goldie JGS. Connectivism: a knowledge learning theory for the digital age? Med Teach. 2016;38(10):1064–9.
48. Forman SG, Shapiro ES, Codding RS, Gonzales JE, Reddy LA, Rosenfield SA, et al. Implementation science and school psychology. Sch Psychol Q. 2013;28(2):77.
49. Hagermoser Sanetti L, Collier-Meek M. Applying implementation science to school psychology: theory & research to address the research-to-practice gap. J Sch Psychol. 2019;76(2019):33–47.
50. Dufrene BA, Parker K, Menousek K, Zhou Q, Harpole LL, Olmi DJ. Direct behavioral consultation in head start to increase

teacher use of praise and effective instruction delivery. J Educ Psychol Consult. 2012;22(3):159–86.
51. Mouzakitis A, Codding RS, Tryon G. The effects of self-monitoring and performance feedback on the treatment integrity of behavior intervention plan implementation and generalization. J Posit Behav Interv. 2015;17(4):223–34.
52. Granić A. Educational technology adoption: a systematic review. Educ Inf Technol. 2022;27(7):9725–44.
53. Shaw SR, Pecsi S. When is the evidence sufficiently supportive of real-world application? evidence-based practices, open science, clinical readiness level. Psychol Sch. 2021;58(10):1891–901.
54. Almulla MA. Investigating important elements that affect students' readiness for and practical use of teaching methods in higher education. Sustainability. 2022;15(1):653.
55. Varadarajan S, Koh JHL, Daniel BK. A systematic review of the opportunities and challenges of micro-credentials for multiple stakeholders: learners, employers, higher education institutions and government. Int J Educ Technol High Educ. 2023;20(1):13. https://doi.org/10.1186/s41239-023-00381-x.
56. Vrugte J, Jong T. Self-explanations in game-based learning: from tacit to transferable knowledge. In: Wouters P, Oostendorp H, editors. Instructional techniques to facilitate learning and motivation of serious games. Cham: Springer; 2017. p. 141–59. https://doi.org/10.1007/978-3-319-39298-1_8.