Human Systems Engineering and Design (IHSED2025), Vol. 198, 2025, 396–408
https://doi.org/10.54941/ahfe1006793

Exploring Barriers in Cybersecurity Training: A Socio-Technical Perspective on Cross-Organizational Portability and Inclusion

Ala Sarah Alaqra and Farzaneh Karegar

Karlstad University, Karlstad, Sweden

ABSTRACT

Cybersecurity training and practical exercises such as cyber-range and Capture-The-Flag (CTF) events are increasingly used to build organisational resilience. However, challenges remain in reusing and adapting these exercises across organisational and national boundaries. This paper explores two key aspects that affect the long-term sustainability and impact of cybersecurity training: cross-organisational portability and inclusivity. Drawing on a cross-border workshop with participants from Sweden and Norway, we identify technical, organisational, and pedagogical barriers that hinder the reuse of cybersecurity training and exercises, including the lack of shared packaging standards, mismatched legal frameworks, hidden infrastructure dependencies, and divergent learning objectives. We argue that portability is not only a technical issue but also a socio-technical challenge requiring clearer communication and aligned expectations. The paper also investigates how inclusivity is understood and implemented in cybersecurity education, highlighting promising practices, such as diverse learner pathways, multilingual materials, and community-led efforts, alongside persistent structural limitations. Based on these findings, we propose the use of lightweight, machine-readable manifests to improve scenario portability and call for more structured institutional support for inclusive training environments.

Keywords: Cybersecurity training and exercises, Barriers, Cross-organizational, Portability, Inclusivity, Sweden, Norway

INTRODUCTION

There is a growing and persistent gap between the increasing demand for cybersecurity professionals and the limited supply of individuals equipped with the necessary qualifications (Crumpler and Lewis, 2022). This skills gap is driven by multiple factors, including the rapid pace of technological evolution, the dynamic nature of cybersecurity roles, and the diverse range of skills required across technical and organizational domains. Traditional education systems often struggle to keep pace with these demands, necessitating faster, more targeted up-skilling approaches for both current and prospective members of the workforce. As a result, cybersecurity training has become a strategic priority for a broad spectrum of stakeholders,

including academic institutions, critical infrastructure operators, and public-sector agencies. Practical learning approaches are increasingly adopted across sectors to provide realistic, skills-centered training that goes beyond traditional lecture-based formats. Examples include: Capture-the-Flag (CTF) competitions, ethical hacking labs in academia, and scenario-driven cyber-range exercises for companies and crisis-management teams. Generally, each sector customizes content, tools, and learning outcomes to fit its specific constraints, such as public-sector regulations or commercial service-level requirements, resulting in a diverse but fragmented cybersecurity training landscape. For instance, in Wahsheh and Mekonnen (2019), the training exercises discussed are highly tailored to specific organizations, which limits generalizability and broader use.

Cybersecurity incidents often transcend national and organizational boundaries, yet training ecosystems are typically developed in isolation. Frameworks like Capture-the-Flag (CTF) competitions and cyber-range simulations often lack reusability and interoperability, limiting their effectiveness across contexts. When scenarios can't be scaled or adapted, the benefits of cross-border collaboration, such as knowledge sharing and infrastructure reuse, are lost. Equally important is access to these trainings. Without intentional inclusive design, scaling efforts may reinforce existing inequalities, excluding individuals with disabilities, non-technical backgrounds, or underrepresented groups. This undermines global efforts to close the cybersecurity skills gap and build a resilient, diverse workforce. These concerns lead us to the following research questions:

RQ1: What challenges do practitioners face when designing, deploying or re-using cybersecurity training and exercises in Norway and Sweden, particularly in cross-organisational settings?

RQ2: How do practitioners define, implement and experience inclusivity within these training frameworks, and which factors hinder or support their inclusivity efforts?

To explore the linked challenges of cross-organizational portability and training inclusivity, we held a structured workshop in February 2025. Participants included Swedish university educators using CTF labs in ethical hacking courses, and Norwegian practitioners and academics involved in designing and delivering cyber-range simulations for crisis management and organizational preparedness. This study is part of a cross-border cyber capacity (CBCC) project that aims to build a sustainable innovation ecosystem for cyber and societal security through joint training, cross-organisational collaboration, and knowledge exchange. Our work contributes to developing cybersecurity competence and strategic cooperation by supporting cross-border training environments, fostering knowledge transfer between education and practice, and promoting inclusive, reusable training models.

Design, Deployment, and Cross-Organisational Challenges

Despite the growing importance of cybersecurity training and exercises in both organisational and cross-organisational contexts, the literature

remains limited in identifying specific challenges and proposing solutions related to the design, development, and reuse of such training, especially in collaborative settings. Some studies, however, highlight key obstacles, including technical and infrastructure limitations (Pfaller et al., 2024; Glas et al., 2023), pedagogical and usability issues (Krinickij and Bukauskas, 2023; Glas et al., 2023), gaps in competencies and trainer availability (Glas et al., 2023), and limited reusability and customization (Glas et al., 2023; Kokkonen et al., 2023). In cross-organisational settings specifically, additional barriers arise, including communication and collaboration difficulties (Line & Moe, 2015; Krinickij and Bukauskas, 2023), policy and trust concerns (Krinickij and Bukauskas, 2023; Kokkonen et al., 2023), technical interoperability issues (Kokkonen et al., 2023), and strategic or resource misalignment (Line and Moe, 2015; Glas et al., 2023).

Cyber-range exercises (CRXs) demand high time, cost, and expertise (Glas et al., 2023; Pfaller et al., 2024), but many organisations lack the infrastructure to support them (Glas et al., 2023). Manual orchestration limits scalability (Pfaller et al., 2024), and complex systems are hard to replicate (Glas et al., 2023). Feedback, assessment, and standardisation are often missing (Krinickij & Bukauskas, 2023; Glas et al., 2023), with many CRXs focusing on tool-specific skills over general concepts (Glas et al., 2023). Trainer shortages, missing role-specific pathways, low reusability, and few modular components add to the challenge (Glas et al., 2023; Kokkonen et al., 2023). Departmental silos, poor coordination, confidentiality, legal barriers, technical incompatibility, and differences in organisational maturity further limit collaboration (Line & Moe, 2015; Krinickij & Bukauskas, 2023; Kokkonen et al., 2023). Competing operational demands and limited budgets constrain training (Line & Moe, 2015; Glas et al., 2023), and CRX participation is rarely recognised like formal certifications (Glas et al., 2023). This study explores these challenges in Sweden and Norway.

Inclusivity Challenges

Accessibility in cybersecurity education training and exercises is essential for ensuring equitable participation. Excluding individuals with disabilities or underserved communities risks deepening existing inequalities (Renaud and Coles-Kemp, 2022). Inclusive training not only empowers more people to protect themselves online but also strengthens the cybersecurity workforce by introducing diverse perspectives needed to address complex threats (Shillair et al., 2022). Early, accessible educational programs (e.g., those introduced in K–12 settings) are particularly effective at breaking down barriers for marginalised populations and fostering long-term engagement with cybersecurity (Triplett, 2023). To build societal resilience and address the global cybersecurity skills gap, strategies must prioritise inclusive and accessible learning initiatives (Renaud and Coles-Kemp, 2022; Shillair et al., 2022; Triplett, 2023). In this work, we examine accessibility strategies and perspectives in cybersecurity training. Specifically, we explore how inclusivity is understood and implemented by cybersecurity educators and practitioners in Sweden and Norway.

METHOD

To explore challenges in cross-organisational reuse and inclusivity in advanced cybersecurity training, we held an online workshop in February 2025 using Zoom and a Padlet board for collaborative documentation. This exploratory, qualitative session gathered preliminary insights from seven practitioners and educators in Sweden and Norway, including university instructors running CTFs and hacking labs, cybersecurity engineers managing cyber-range exercises, and researchers in cybersecurity education. Participants were recruited through the project for their direct experience in training delivery, tool development, and educational design.

The workshop took place over approximately five hours, which included a lunch break and two smaller breaks. The workshop started with an introduction to the workshop, as well as the Padlet to be used. Participants were given some time to get familiar with the process of documenting their responses. The structure of the workshop included three main parts. The first part explored participants' organizational roles, training formats, tools, stakeholder backgrounds, and pedagogical goals. The second part focused on discussing experiences and challenges in cybersecurity training, highlighting shared issues and cross-border differences. The final part addressed inclusivity, with participants reflecting on accessibility, gender, and diversity in technical backgrounds within their training practices. Discussions were captured through real-time documentation by participants on the shared Padlet board, supplemented by notes. The main moderator conducted the entire workshop (A.S. Alaqra). However, for the discussions of Parts 1 and 2, a second moderator (F. Karegar) facilitated the breakout sessions when participants were divided into two groups in Zoom's breakout rooms. The qualitative data collected was subsequently organised thematically according to the workshop structure. No audio or video recordings were made to preserve participant privacy.

RESULTS

In total, there were seven participants in the session, four from the Swedish side (SWE1-SWE4) and three from the Norwegian side (NOR1-NOR3). According to the workshop's discussion, participants indicated that cybersecurity training frameworks in Sweden and Norway reflect a shared emphasis on experiential, practical learning, highlighting how cybersecurity education is tailored to national contexts and pedagogical goals. However, there was a difference in institutional focus and the scope of engagement.

Table 1: Categories of challenges surfaced in the workshop.

Challenge Type	Category
Technical/Infrastructure	Infrastructure robustness & continuity Scalability & resource capacity

Continued

Table 1: Continued

Challenge Type	Category
Organisational/Process	Cross-organisational portability & standardisation Stakeholder communication & requirement alignment
Pedagogical/Learner-centred	Pedagogical engagement & learner management

Cybersecurity Training and Exercises Challenges

Analysis of participants' comments on challenges they face when designing, deploying, and re-using cybersecurity exercises in Norway and Sweden yielded five categories that relate to three main areas, as shown in Table 1. There are five interlocking yet analytically distinct challenge categories that relate to three main areas, as shown in Table 1. The first, technical/infrastructure, refers to issues in the hardware and software backbone of exercises, from bugs in open-source engines and cloud-quota ceilings to rapid container/VM rollback needs and missing metadata standards. The second, organisational/process, involves frictions in human and institutional workflows, such as divergent regulations, planning miscommunications, unanticipated adaptation workload, and unclear ownership of outages or hand-overs. The third, pedagogical/learner-centred, covers factors shaping motivation, engagement and fairness rather than raw technology: minimal-overhead onboarding and workload management, varied learner backgrounds and reactions, learners' fairness during outage, and immersive narrative design.

Infrastructure Robustness, Continuity, & Scalability: Although fewer participants raised technical or infrastructure challenges than issues of portability or pedagogy, they highlighted how lapses in robustness, breaks in continuity, and scalability limits can undermine even well-planned exercises. Once cohorts exceed a certain number of concurrent users, cloud quotas and on-premise hardware quickly become bottlenecks. As one participant noted (NOR2), "If the number of students goes over 100 … we are limited concerning what we can use in the cloud," often forcing ad-hoc resource hunts mid-semester. Running a 4–6-month cyber-range for 400 learners, as another described, adds sustained compute demands and human-support overhead that strain narrowly provisioned environments and small operations teams. Robustness under adversarial load is another issue: most CTF and cyber-range platforms (whether open-source or commercial) are not designed to host intentionally broken or malicious services. As one participant said (NOR2), "none of them are considered for hosting broken or malicious services in mind," so when expert users probe them, latent bugs emerge and can crash entire challenges, leaving teams to scramble for fixes on the spot. When failures occur, continuity is disrupted further by delays in diagnosing whether the problem lies with a container, firewall, or another dependency. One participant described this as: "Is it our container or the campus firewall?" During this lag, learners react unevenly, scoreboard

integrity suffers, and a short outage can turn into an extended disruption that undermines trust in the exercise's reliability.

Cross-Organisational Portability & Standardisation: This category includes challenges when cybersecurity exercises are reused across organisations, whether by handing over ready-made scenarios or developing them together. While participants mainly discussed reusing existing packages, many of the same issues such as hidden assumptions, different goals, and lack of shared standards also affect co-creation. A "scenario" usually includes infrastructure configurations, challenge artefacts and tasks, instructions, narratives, scoring rules, and supporting files. Although these seem self-contained, they are often tied to the original host's policies, infrastructure, and unstated assumptions. The lack of standard formats, a common taxonomy for challenge types (like Web, Crypto, Forensics) and hosting setups (such as on-premises virtual machines or containers), and missing metadata about target groups and learning goals make simple reuse difficult.

Every organisation operates under its own rules; how it defines "critical services", who must report a data breach, and what counts as acceptable incident-handling. For example, a scenario designed for a Swedish authority suddenly may become non-compliant when run by a Norwegian partner, and then the exercise should be fitted within local legal requirements and their scope. As a result, the scenario cannot be simply copied. It means that despite the availability of the self-contained exercise package, several things must be adapted and even rewritten, including, for example, challenge artefacts and tasks, scoring rules, and briefing content to match the receiving organisation's requirements and scope. What one country defines as a "critical service" or "personal-data asset" may fall outside another's legal framework, forcing entire evaluation metrics to be redefined rather than reused. Not only differences in rules and scopes, but also hidden infrastructure assumptions lead to partial reuse of the "scenario" shared. In other words, hidden assumptions make an exercise seem portable on paper but fail in practice. A hidden assumption is any tacit, undocumented detail that the author of an exercise takes for granted. So when the exercise is moved to a new environment, it mysteriously breaks. These dependencies don't surface in the instructions or packaging. Therefore, the receiving team only discovers them during setup and must then rebuild or prune the affected parts. As one practitioner (NOR3) put it: "A ready CTF challenge is not necessarily transferable between different parties...there are lots of invisible assumptions involved when it comes to implementations."

Practitioners often noted that sharing a ready-made CTF or cyber-range exercise today is like handing over a black box of files. Without a clear structure or metadata, the recipient must unpack everything, figure out what each piece does, and decide which artefacts are generic and which are context-specific. This informal packaging, combined with legal rework and hidden dependencies, creates three main burdens: 1) High adaptation overhead: since there is no manifest to separate generic elements from sector-specific or national content, planners spend more time decoding and pruning than creating new exercises from scratch. As one participant (NOR3) said, it is often "quicker to create a new exercise" than untangle another organisation's

bundle. Even reusable parts still need extra adaptation work. 2) Incompatible taxonomies: different organisers use their own naming for challenge types, scoring, and deployment settings. Automated imports often fail, so files must be renamed manually to match local conventions. 3) Barrier to reuse and benchmarking: without a shared, machine-readable format, it is hard to filter artefacts by scope or align scoring rubrics, KPIs, and regulatory contexts. This prevents reliable comparison of outcomes and makes sharing best practices or aggregating learning results across teams nearly impossible.

Participants also stressed that clearly stating the main learner group and learning objectives is vital for smooth sharing. When this metadata is missing, planners must extract it manually and retrofit scripts, scoring, and narratives for the new audience. This extra work often exceeds the effort of building a fresh scenario.

Stakeholder Communication and Requirement Alignment: Our workshop participants reported that the "technical" hiccups in CTFs and cyber-range exercises stem from breakdowns in early-stage communication and misaligned expectations. In the planning phase, organisers and their counterparts may fail to establish a shared understanding: initial requirements briefs are often unstructured or incomplete, and critical details such as expected exercise deliverables, system dependencies and success criteria go unstated, which leads teams to talk past one another. As one participant (NOR3) remarked, "Miscommunication in the planning phase" highlights how unclear early coordination can undermine exercise preparation.

Miscommunication in the planning phase makes the requirement-elicitation process a big problem. Contact points in organisations come with widely varied backgrounds, from non-technical managers to seasoned network engineers, so they struggle to articulate what they need an exercise to achieve, which infrastructure it must run on, or which systems to inject faults into. Proper requirement elicitation is important to bridge the gap between what an organisation wants from an exercise and what they achieve at the end. Participants reported that finding an organisation's requirements often involves numerous back-and-forth iterations, "several updates needed" (NOR1), before the exercise design team fully understands what to build, and noted that while academic CTFs can be reused more straightforwardly, enterprise exercises demand extensive adaptation to match each organisation's maturity and processes. In academic CTF contexts, it is more probable on paper, although it may not be true in real-world deployment, that contact points (typically teaching or lab assistants) share a well-defined execution environment. As a result, the mentioned challenges can be lifted, and exercises can be reused with minimal adjustment. Compared to university-style CTFs, company-run exercises take a lot more work because businesses have different approval processes and rules to follow, often use custom systems that don't match the standard setups, and set tighter safety controls, so every step has to be negotiated and tested. Therefore, running exercises in real organisations means more back-and-forth and custom tweaking than in a school lab, which makes requirement elicitation and communication in planning a crucial step.

Underlying both of these challenges is a profound trust and common-language gap. Clients and exercise designers often use different jargon, conceptual frameworks and even national terminologies, so critical constraints remain unstated or perhaps obscured. Moreover, participants noted that even when stakeholders understand their own problems, they may hesitate to disclose them openly, and this further compounds misalignment. As a result, essential details, such as data-classification labels, incident-response roles, dependencies in the systems and infrastructure, and existing problems to induce crisis (if expected), stay hidden until painful surprises emerge during deployment. Only a shared glossary and transparent dialogue can surface these concealed expectations early.

Pedagogical Engagement & Learner Management: From the discussion, cybersecurity training frameworks across Sweden and Norway share similarities in learner engagement, experiential learning, and real-world alignment. However, learner-centred challenges were identified, particularly around diverse learner profiles, motivation, time management, and equitable access to resources. Below are detailed accounts of the aforementioned.

Participants from both countries noted that students arrive with varying levels of technical knowledge, motivation, and expectations. For instance, SWE3 described student responses in emotional stages: from initial confusion and denial to eventual engagement and enjoyment. Therefore, highlighting the need for emotionally aware instructional design. Similarly, SWE2 and SWE4 acknowledged that even technically skilled participants may need structured onboarding to grasp complex infrastructures or course expectations. In Norway, NOR2 and NOR3 emphasised the importance of aligning scenarios with specific learner groups (e.g., IT staff vs. crisis management teams), as mixed audiences may lead to confusion or reduced impact.

Some instructors recognise the need for greater flexibility in assignment timelines. Although not all participants explicitly endorsed deadline extensions, SWE1 and SWE3 indicated that iterative review and adaptation, for both of course content and infrastructure, are built into their workflows. This eventually may support more responsive scheduling in the future. Furthermore, several Swedish instructors reported that students tend to postpone practical assignments until deadlines approach, limiting deep engagement. SWE2 noted that poor time management reduces learning effectiveness and increases stress. In Norway, delayed engagement was similarly observed, and instructors stressed the importance of having support across the training period to keep learners on track.

In regard to motivation, sustaining student motivation was identified as a key concern. SWE3 and NOR1 both noted that motivation levels vary significantly, with some students underestimating the effort required. In response, educators have employed strategies like Discord channels for peer discussion, gamification elements, and competitive moments to boost engagement. NOR1 also reported that 10% of students typically fall behind, reflecting the challenge of keeping learners on pace, especially in long-duration or self-paced formats.

Efforts by educators in both countries include the adopting of gamification strategies to enhance motivation and peer interaction. For example, NOR1 incorporated social platforms and reward mechanics to maintain interest, and SWE1 explored immersive, interconnected challenge environments to simulate real-world security narratives. Participants indicate that these approaches also encourage collaborative problem-solving. In addition, educators expressed a desire to provide more coherent and immersive experiences through narrative-based training. SWE1 described building layered, interdependent exercises within a single virtual environment to mimic real-life scenarios. This pedagogical strategy aims to improve contextual understanding and sustain learner interest over time.

In an attempt to include more learners, educators aim to reduce barriers to entry for students with lower levels of preparation or organisational ability. SWE2 framed this as a challenge of "low-overhead onboarding," particularly for students not accustomed to hands-on cybersecurity work. This has been addressed through in-class walkthroughs, detailed documentation, and the involvement of guest experts to contextualise assignments. However, ensuring fairness was a key concern, particularly when unexpected issues arise. SWE3 cited hardware compatibility issues (e.g., outdated ports, improperly flashed devices) and variable internet access as common barriers. These disruptions risk creating inequitable learning conditions. To address this, NOR2 stressed the importance of robust technical support and pre-session dry runs, though miscommunication during setup phases still presents challenges.

Perspectives on Inclusivity in Cybersecurity Training

Overall, participants indicated that inclusivity in cybersecurity training across Sweden and Norway is addressed through a mix of structural adaptations, pedagogical awareness, and ongoing experimentation. However, challenges remain in fully bridging the gap between intention and practice, especially when it comes to the complexity of inclusion.

Participants from both Sweden and Norway highlighted the multilayered nature of inclusivity in cybersecurity education and training. They touched on accessibility, gender balance, cultural diversity, and varying technical competencies. SWE1 emphasised economic inclusivity through open-source tools and free resources. SWE1 also indicated inclusivity in the sense of providing multiple solution paths for exercises to accommodate diverse thinking styles and backgrounds. SWE2 and SWE3 further elaborated on gender and cultural representation, referencing exchange student inclusion, neurodiversity considerations, and hybrid/online delivery modes to increase access. In Sweden, the physical environment of training spaces, such as the hacking lab at Karlstad University, was also critically discussed in terms of how it is perceived by female students.

Norwegian participants (NOR1, NOR2, NOR3) highlighted formal efforts to promote inclusive learning environments. Similarly, in Sweden's universities, there are formal standards to accommodate the special needs of students for their education. At xx University, in Norway, pedagogical

training is mandatory to support inclusivity, and standardised accessibility accommodations for students with disabilities are in place. NOR3 noted the importance of using inclusive language in documentation and instructional materials, recognising how phrasing can either engage or alienate different user groups. NOR3 stressed the importance of individual responsibility and reflection for conducting inclusive behaviour.

Gender inclusion was a recurring challenge across both contexts, with efforts to achieve gender balance. NOR3 discussed recruitment for national cybersecurity teams, noting that reframing CTF challenges to emphasise creative problem-solving over technical skill significantly improved female participation. Feedback revealed that many women initially felt excluded due to the perception that strong IT skills were a prerequisite. SWE3 reinforced this point by stressing the importance of incorporating female role models in events and designing challenge scenarios (to include organizationally relevant with problem-solving aspects), which tend to attract a broader demographic.

The discussion also included ongoing tensions between inclusivity aspirations and structural constraints. SWE1 acknowledged that individual accommodations may be limited by curriculum design, assessment formats, and learning objectives. A Swedish example involving a student with a speech impediment during an assessed presentation highlighted the complexities of equitable evaluation. Although some participants suggested adaptive tools like text-to-speech could improve accessibility, these are not yet systematically implemented.

DISCUSSIONS

Facilitating Cross-Organisational Portability

Our findings highlight that organisations are willing to share cybersecurity exercises across other organisations, sectors, and even national boundaries. However, cross-organisational portability challenges hinder them from doing so. The absence of a common packaging and description standard imposes hidden adaptation costs. Planners, for example, must navigate divergent legal mandates, reverse-engineer embedded infrastructure dependencies, and adapt materials to meet specific training objectives and target groups before any scenario can run. As participants in our workshop noted, such efforts may exceed the cost of creating fresh content. This burden also risks undermining the collaboration that cross-organisational sharing aims to foster, as resource-constrained teams divert time from pedagogical innovation to tedious reconfiguration work. This aligns with known barriers in the literature, such as the lack of modular or configurable components, metadata standards, shared packaging conventions, and mismatches in legal frameworks and sector-specific definitions—such as the concept of "critical services"—that limit reusability and portability across contexts (Glas et al., 2023; Kokkonen, Paijanen and Sipola, 2023; Wahsheh and Mekonnen, 2019).

In Europe, the NIS2 Directive (Directive (EU) 2022/2555) strengthens cybersecurity requirements, governance, and cooperation but does not define technical or metadata standards for packaging or exchanging training exercises, leaving this to community efforts (European Parliament & Council,

2022). Similarly, ENISA's "Cross-Sector Exercise Requirements" report describes what cross-sector exercises should include (like roles, formats, and review artefacts)but does not specify how to package or share scenarios in a machine-readable way (European Union Agency for Cybersecurity, 2022).

Introducing a lightweight, machine-readable manifest (e.g., JSON), as proposed by our workshop participants, could help close this gap by enabling a predictable, scriptable portability workflow. Such a manifest could tag artefacts as general, sector-specific, or country-specific; declare the intended audience; and specify deployment parameters using a shared vocabulary, making implicit assumptions explicit. To support inclusivity, it should also include accessibility metadata (examples such as preferred languages, assistive technology compatibility, and diversity objectives) to ensure training is welcoming and aligned with accessibility or gender balance goals. Receiving teams could then disregard irrelevant parts and focus on adapting core materials instead of reverse-engineering them.

While communication and alignment challenges exist in any cybersecurity exercise, they become more acute across organisational or sectoral boundaries (Line & Moe, 2015; Krinickij & Bukauskas, 2023). Differences in culture, terminology, and infrastructure can create misalignment and friction, so clear stakeholder interaction (defining learner groups, objectives, or using shared glossaries) is vital for smooth transfer. As participants confirmed, portability is a socio-technical practice: even the best manifest depends on effective communication and shared expectations. Future work should test manifest prototypes in cross-organisational pilots and embed structured scoping and collaborative tools into routine practice. Combining a technical exchange format with a culture of transparency and coordination could strengthen resilience, inclusivity, and efficiency in cross-organisational exercise sharing.

Inclusive Approaches, Challenges, and Practices.

Our findings support the importance of inclusive design in cybersecurity education and training, as emphasised in prior work (Renaud et al., 2022; Shillair et al., 2022; Triplett et al., 2023). Participants across Sweden and Norway demonstrated awareness of various inclusivity dimensions, such as accessibility for individuals with disabilities, gender diversity, neurodiversity, and varied technical backgrounds, but concrete strategies for implementation remain a challenge.

Some educators considered inclusivity in their pedagogical planning (e.g., using gender-neutral language, accommodating neurodiversity, or incorporating flexible learning formats); however, these practices were often implemented on a case-by-case basis. This aligns with Renaud et al. (2022), who argue that without systemic integration of inclusive frameworks, marginalised groups may continue to be excluded from meaningful participation in cybersecurity training. Several respondents also noted challenges in meeting individual needs due to course structure or assessment constraints, suggesting a lack of institutional flexibility in supporting accessibility requests. Additionally, addressing learner diversity

and backgrounds is important. Participants recognised the need to accommodate students with varied technical backgrounds. Some educators responded by offering multiple solution paths or by designing challenges that emphasised creative problem-solving over technical mastery. One example from a national team recruitment event in Norway demonstrated that replacing traditional CTF tasks with creative-thinking exercises led to increased female participation, which is consistent with Triplett et al.'s (2023) call for earlier and more inclusive engagement in cybersecurity. Such adaptations help dismantle preconceptions about who belongs in the field and expand the pool of cybersecurity talent.

Beyond curriculum design, participants reflected on how the learning environment itself can influence inclusivity. Examples included the physical layout and design of hacking spaces, concerns about visible gender imbalance in events, and the need for female role models. Shillair et al. (2022) argue that inclusive education must extend beyond content to include social cues, cultural representation, and psychological safety. Our findings also suggest that while isolated practices point toward growing awareness, more structural support is needed to institutionalise inclusivity.

CONCLUSION

This paper examined the challenges of cross-organisational portability and inclusivity in cybersecurity training, based on insights from a cross-border workshop involving practitioners from Sweden and Norway. While participants expressed interest in sharing and reusing training exercises, they highlighted substantial barriers, including missing packaging standards, hidden infrastructure dependencies, and divergent legal and pedagogical assumptions. These findings underscore that portability is not merely a technical issue but a socio-technical challenge requiring better coordination, transparency, and shared understanding. We propose the use of lightweight, machine-readable manifests to support more predictable and efficient adaptation across organisations.

In parallel, participants described a growing commitment to inclusivity, reflected in efforts such as varied challenge formats, inclusive language, and accessibility accommodations. However, these efforts remain largely individual and informal, constrained by institutional structures and a lack of systemic support. Taken together, our findings highlight the need for both technical infrastructure (such as standardised metadata for exercises) and systematic scaffolding (such as supporting policies and planning rituals) to realise more resilient and inclusive cybersecurity training ecosystems. Future work should focus on piloting tools for cross-organizational portability while embedding inclusivity strategies more deliberately from the beginning of training design.

ACKNOWLEDGMENT

The authors would like to thank the participants of this study. This work was funded by CBCC Interreg project.

REFERENCES

Crumpler, W. and Lewis, J. A., 2022. Cybersecurity Workforce Gap. Washington, DC: Center for Strategic and International Studies. Available at: JSTOR.

European Parliament and Council of the European Union, 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). Official Journal of the European Union, L 277, 30.12.2022. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj [Accessed 24 June 2025].

European Union Agency for Cybersecurity (ENISA), 2022. Cross-sector exercise requirements. ENISA report, March 2022. Available at: https://www.enisa.europa.eu/publications/cross-sector-exercise-requirements [Accessed 24 June 2025].

Glas, M., Böhm, F., Schönteich, F. and Pernul, G., 2023. Cyber range exercises: Potentials and open challenges for organizations. In: International Symposium on Human Aspects of Information Security and Assurance, pp. 24–35. Springer.

Kokkonen, T., Paijanen, J. and Sipola, T., 2023. Multi-national cyber security exercise, case Flagship 2. In: Proceedings of the 14th International Conference on Education Technology and Computers (ICETC '22). New York, NY: Association for Computing Machinery, pp. 292–298. https://doi.org/10.1145/3572549.3572596.

Krinickij, V. and Bukauskas, L., 2023. Challenges in cybersecurity group interoperability training. In: International Conference on Human Computer Interaction, pp. 273–278. Springer.

Line, M. B. and Moe, N. B., 2015. Understanding collaborative challenges in IT security preparedness exercises. In: IFIP International Information Security and Privacy Conference, pp. 311–324. Springer.

Pfaller, T., Skopik, F., Smith, P. and Leitner, M., 2024, June. Towards Customized Cyber Exercises using a Process-based Lifecycle Model. In Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (pp. 37–45).

Renaud, K. and Coles-Kemp, L., 2022. Accessible and inclusive cyber security: A nuanced and complex challenge. *SN Computer Science*, 3(5), p. 346.

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E. and von Solms, B., 2022. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, 119, p. 102756.

Triplett, W. J., 2023. Addressing cybersecurity challenges in education. International *Journal of STEM Education for Sustainability*, 3(1), pp. 47–67.

Wahsheh, L. A. and Mekonnen, B., 2019. Practical cyber security training exercises. In: 2019 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, pp. 48–53.