Advances in Military Technology
Vol. 21, No. 2, 2026, pp. 513-526
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.02175

Integrating Practical Cybersecurity Skills and Leadership Through Collaborative Development

I. Klaban, D. Staněk*, A. Štefek, P. Františ, A. Coufalíková, T. Šlajs, T. Ráčil, P. Gallus, and V. Ondryhal

Department of Informatics and Cyber Operations, Faculty of Military Technology, University of Defence, Brno, Czech Republic

The manuscript was received on 24 July 2026 and was accepted after revision for publication as a case study on 1 November 2026.

Abstract:

This study examines a semester-long cybersecurity project built around a shared model information system in a military university program. The main educational contribution is the shared model information system, which connected the technical work of eight cross-year teams and gave senior students a concrete setting for peer leadership. Post-event surveys from 2024 and 2025 were analyzed separately because participation overlapped and the instruments differed. In 2025, the mean reported change in focal-area skill was 0.99 points on a seven-point scale; 43 respondents chose a higher rating, 23 the same rating, and three a lower rating. Leadership evaluations were positively associated with conflict resolution within both surveys. Future evaluations should collect prospective ratings, score technical work, and record stable team identifiers.

Keywords:

cybersecurity education, military education, DevSecOps, project-based learning, cross-year collaboration, peer leadership

1 Introduction

Cybersecurity education must connect software development, system operation, security analysis, and the coordination of specialized work. These demands are especially relevant in military programs where technical decisions are made within organizational and operational constraints [1]. Short laboratories remain useful for practicing individual

* *Corresponding author: University of Defence, Kounicova 156/65, CZ-662 10 Brno, Czech Republic. Phone: +420 973 443 394, Fax: +420 973 443 266, E-mail: dominik.stanek@unob.cz. ORCID 0009-0006-5141-3165.*

techniques, but sustained projects allow students to encounter dependencies between services, security roles, and team decisions [2].

This study examines a semester-long cybersecurity project embedded in a five-year military higher-education program. In two annual iterations, eight cross-year teams worked on complementary parts of a shared model information system. Their briefs covered system integration, configuration, and deployment; infrastructure attack and defence; monitoring; audit; documentation; and regulation. Senior students could lead or coordinate the teams, giving peer leadership a concrete technical setting rather than treating it as a separate classroom exercise.

The 2024 and 2025 post-event surveys address three research questions. RQ1a asks how 2025 respondents perceived changes in their focal-area skills. RQ1b asks how they rated organization, instructional clarity, support, and practical application. RQ2 asks whether leadership evaluation was associated with conflict resolution and related team processes within each annual survey. After the activity, the 2025 survey asked students to rate both their earlier and current focal-area skill. The difference between these ratings therefore reflects perceived change, not independently assessed performance. The instruments differed, and 56 of the 69 respondents in 2025 had also participated in 2024. We therefore analyze the surveys separately as overlapping cross-sectional datasets, not as independent cohorts or a replication.

The shared technical system is the study's main educational contribution. It gave specialized teams one system to develop, protect, audit, and document across study years, while senior students could lead or coordinate the teams. The surveys evaluate how students perceived this approach. Assessing technical outcomes would require direct performance measures.

2 Related Work

Cybersecurity curricula combine technical knowledge with design, communication, teamwork, ethics, and risk management. CSEC2017 and Computing Curricula 2020 place these capabilities within cybersecurity and computing education [3, 4]; current ABET criteria likewise include professional responsibility and effective participation as a team member or leader [5]. The NICE Framework complements these curricular perspectives with a vocabulary of cybersecurity work roles, tasks, knowledge, and skills [6].

Project-based learning provides a sustained task in which students can divide work, revise technical decisions, and integrate knowledge across subjects [2]. Its collaborative value depends on role clarity, communication, and the distribution of meaningful work [7]. Peer tutoring can support participation by less experienced students when their tasks contribute to a shared result [8]. Collaboration also varies across groups within the same course, making team conditions relevant to both instruction and evaluation [9].

Cybersecurity projects extend this logic by connecting classroom concepts with observable system behavior [10]. DevSecOps work emphasizes shared tools and responsibilities across development, security, and operations [11], while hands-on platforms can produce records that support feedback and assessment [12]. A shared system can therefore provide both a technical object and a reason for teams with different responsibilities to coordinate. However, teamwork and leadership still require explicit objectives and evidence; they cannot be inferred from completion of a technical artefact alone [13–15].

Survey measures address a different part of the evaluation. Retrospective before-and-after ratings may help respondents apply a common understanding of the skill to

both judgements, but the recalled baseline remains vulnerable to memory, consistency, and response-shift effects [16, 17]. Such ratings can describe perceived change when a prospective baseline is unavailable, but they do not replace direct assessment. The present study therefore reports survey evidence about perceived focal-area skill and team processes while treating technical performance as a separate outcome for future evaluation.

3 Program Context and Activity Design

3.1 Program Setting and Organization

The activity formed part of a continuous five-year university cybersecurity program preparing military and civilian specialists for defense-sector work. It ran during the summer semester in 2024 and 2025. At the start of each iteration, students were assigned to eight cross-year teams, each responsible for a topic connected to the same model information system. Teams developed their work throughout the semester and presented and discussed their outputs in an intensive closing session.

Senior students could lead or coordinate the work, while other students contributed through development, testing, documentation, system configuration, and project coordination. This structure linked leadership to decisions about a real technical object: teams had to allocate work, manage dependencies, explain changes, and communicate risks across topic boundaries. The available data record respondents' reported roles. Fig. 1 traces coordination from faculty mentors to senior student leaders and mixed-year teams. It also shows the daily synchronization, retrospectives, and monitoring reviews used during the project.



Fig. 1 Cross-year mentoring and coordination structure

3.2 Topics and Team Work

Course records list eight cross-year teams in both 2024 and 2025. Both years used the same eight briefs: information-system lifecycle documentation; infrastructure attack (Red Team); infrastructure protection (Blue Team); reporting (SIEM); information-system audit; NIS 2 and the new Cybersecurity Act (ZoKB); significant information systems (VIS); and Green Team work. Tab. 1 summarizes the briefs used in both years, with representative outputs and the main dependencies between teams.

Students prepared technical or administrative outputs appropriate to their brief, but their decisions could affect other teams. Infrastructure changes influenced deployment and monitoring; audit findings created work for development and defense; regulatory requirements shaped documentation and system controls. Team leaders organized tasks and communication within their groups, and teams discussed their outputs together at the end of the semester.

Tab. 1 Annual team briefs, outputs and dependencies

Area	**Brief and representative output (2024 and 2025)**	**Main dependency**
Lifecycle documentation	Information-system lifecycle documentation; technical and lifecycle records	Technical or regulatory changes
Infrastructure attack	Red Team; attack findings	Blue Team and information-system audit
Infrastructure protection	Blue Team; protection changes	Green Team and SIEM reporting
Security reporting	SIEM reporting; monitoring reports and dashboards	Deployed services and metrics
Information-system audit	Information-system audit; system and application findings	Red/Blue findings and remediation
Regulatory compliance	NIS 2 and new ZoKB; requirements mapping	Documentation and controls
Significant information systems	VIS; classification and requirements	Documentation and controls
System integration	Green Team; configuration and deployment	Services and monitoring

3.3 System Architecture and Technologies

The shared model information system had a React front end, GraphQL interfaces, and three Python services with separate PostgreSQL stores, all deployed in Docker containers. The Green Team configured, integrated, and deployed the system. The Red and Blue Teams examined infrastructure and application security, and the information-system audit team reviewed system and application issues. The reporting team used Prometheus and Grafana for security-event monitoring. The available project records do not identify a separate SIEM platform or its configuration. The regulatory brief covered NIS 2 [18], the new Cybersecurity Act, and requirements for significant information systems.

Fig. 2 shows the main component path and where the team briefs contributed to or monitored the system. The arrows show operational dependencies, not a complete data-flow model. A change to a service or interface could affect deployment, monitoring, audit, or documentation. Audit and regulatory findings could in turn require changes by development and infrastructure teams.

The retained records do not include versioned attack scenarios, control configurations, or deployment scripts. The article can therefore describe the educational architecture, roles, interfaces, and representative outputs.

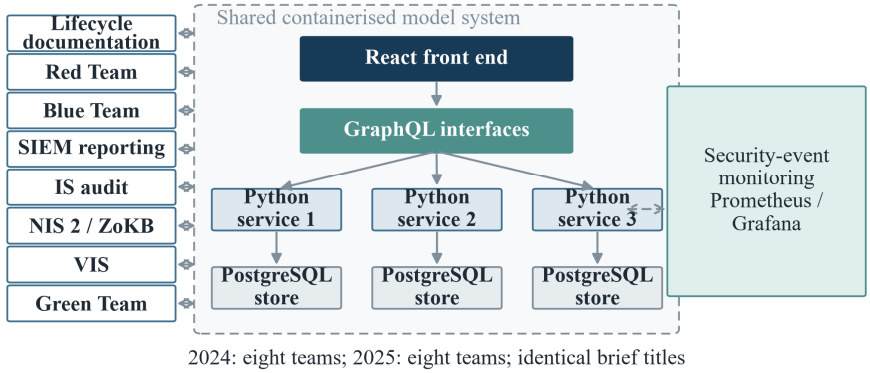


Fig. 2 Shared-system components and interfaces among project teams

4 Methods

4.1 Design and Participants

The study is a retrospective evaluation of two annual iterations of one curricular activity. Available survey records define the samples: 37 responses for the 2024 iteration and 69 for 2025. Among the 2025 respondents, 56 reported participating in the earlier iteration and 13 did not. Because the records are anonymous, returning respondents cannot be linked to any response they may have provided in 2024. The annual samples are therefore neither independent cohorts nor linked longitudinal observations. For these reasons, the two annual datasets cannot serve as an independent replication and cannot support valid estimates of year-to-year change.

In the 2024 sample, study years 1 and 2 were combined (n = 5), while years 3, 4, and 5 contributed 14, 8, and 10 responses. In 2025, years 2 to 5 contributed 16, 10, 26, and 17 responses. Available records do not contain a verified eligibility denominator, recruitment or nonresponse information, or a complete team roster. Response rates and team sizes cannot therefore be calculated. Instrument wording and administration procedures also differed between iterations, so all analyses are conducted within year.

Tab. 2 summarizes the composition of the available survey samples.

Tab. 2 Composition of the Survey Samples

Characteristic	**2024**	**2025**
Survey records	37	69
Study-year composition	Years 1–2 combined: 5; year 3: 14; year 4: 8; year 5: 10	Year 2: 16; year 3: 10; year 4: 26; year 5: 17
Prior-iteration participation	Not collected for linkage	Yes: 56; no: 13
Role-percentage allocation	Not collected	Valid: 42; invalid: 27

4.2 Questionnaires and Measures

The study team designed both questionnaires specifically to evaluate the activity after it ended. The items covered organization, technical application, cross-year teamwork, leadership, and self-assessment. The 2025 questionnaire also asked about retrospective

focal-area skill, role allocations, team processes, and prior participation. Neither questionnaire was adapted from an established psychometric scale. The available records document no formal pilot testing, cognitive interviewing, or psychometric validation. Most analysed constructs were represented by separate single-item measures rather than multi-item scales, so internal-consistency coefficients were not applicable.

Both questionnaires were administered in Czech. Author-prepared English translations preserved the order of questions and response categories; no independent translation check or back-translation was documented. This lack of verification adds uncertainty to the measurements.

The 2024 questionnaire addressed organization, instructions, technologies, documentation, practical application, collaboration, leadership, conflict resolution, cross-year knowledge sharing, and perceived benefits. The 2025 questionnaire covered related themes with nonidentical wording and added retrospective before-and-after focal-area skill ratings, role percentages, team-process items, and prior participation.

The principal 2025 measure asked respondents to rate their skill in their team's focal area before and after the activity on a scale from 1 (lowest) to 7 (highest). Both ratings were collected after the activity. Their difference is reported as perceived focal-area skill change. Because the recalled-before rating was not a prospective baseline, the measure may be affected by recall and response shift. Respondents also rated different technical or regulatory areas, so equal numeric changes do not necessarily represent the same content.

RQ1b used 2025 ratings of organization, instructional clarity, support, and practical application. RQ2 used leadership evaluation and conflict resolution because conceptually corresponding items appeared in both questionnaires. Cross-year knowledge sharing and perceived benefit, available only in 2024, were included as exploratory team-process variables. These choices were not preregistered. The 2024 conflict-resolution responses (Low, Average, Good, and Very good) were encoded from 2 to 5; adding a constant does not alter a Spearman rank correlation. Tab. 3 summarizes the analyzed constructs. Annual correlations were not pooled because item wording and response formats differed.

4.3 Role Classification and Data Quality

The 2025 questionnaire contained percentage fields for team leader, developer, tester, project manager or coordinator, documentation specialist, and other work. Missing or non-numeric entries were set to zero. Each value had to fall between 0 and 100. A total from 99.5–100.5 % was accepted. An impossible value invalidated the allocation even when the total was within this range. Equal percentages in different role fields were permitted because the fields represented different types of work.

Twenty-nine respondents entered a nonzero team-leader allocation; a project-manager or coordinator allocation alone did not define leader status. Of these, 14 of the 29 leader-role reports had invalid percentage allocations, including the sole report from a first-time participant. Among the 42 valid allocations, 15 reported team-leader work and all 15 were returning participants. Raw leader-role presence is retained only as descriptive context. Invalid allocations were excluded from percentage-derived summaries, and no leader versus non-leader outcome comparison is reported.

The analysis converted allowed response labels to numeric values and set out-of-range values to missing. Analyses used pairwise-complete observations, so the denominator is reported for every inferential result. The analytic rules were defined before the results were calculated.

Tab. 3 Analyzed Constructs and Operational Definitions

Construct	Operational definition	Scale and use
Focal-area skill	Post-event ratings of skill before and after the 2025 activity in the area on which the respondent's team focused	Two ratings from 1 (lowest) to 7 (highest); paired difference for RQ1a
Activity context	Organization, clarity of pre-activity instructions, quality of supporting material, and practical application of cybersecurity principles	Four 1–7 items; descriptive results for RQ1b
Leadership	2024 evaluation of team leadership; 2025 rating that the leader set clear goals and provided support	2024: 1–5; 2025: 1–7; within-year RQ2 correlations
Conflict	2024 self-rating of ability to resolve disagreements; 2025 rating of constructive conflict resolution	2024: encoded 2–5; 2025: 1–7; within-year RQ2 correlations
Cross-year	2024 ratings of knowledge sharing and perceived benefit across study years	Two 1–4 items; exploratory RQ2 correlations
Prior participation	2025 report of participation in the 2024 iteration	Yes or no; sample-overlap disclosure and sensitivity analysis
Leader-role report	Nonzero percentage entered for team-leader work in 2025	Descriptive data-quality context; not used for an outcome comparison

4.4 Statistical Analysis

The 2025 focal-area outcome was the paired difference (after minus recalled before). A paired analysis was required because both ratings came from the same respondent. The mean difference answers the question of average perceived change, while Cohen's d_z expresses its magnitude relative to variation in the within-person differences [19]. The paired t test therefore tests mean change. Because the ratings were bounded and ordinal, we also report a two-sided wilcoxon signed-rank test as a rank-based sensitivity analysis. It omitted zero differences (the wilcox zero-difference convention) and used a normal approximation because of zeros and ties.

We used 10 000-resample percentile bootstraps (seed 0) for the mean and d_z so their 95 % confidence intervals did not rely only on normal theory.

Descriptive summaries include the available sample size, mean, standard deviation, median, interquartile range, and counts of higher, unchanged, and lower paired ratings. Means and standard deviations describe average level and spread; medians, interquartile ranges, and direction counts show the distribution without relying on the mean alone. Missing outcomes were not imputed; each result uses the available observations and reports its denominator. A post hoc two-sided Welch test compared mean change for returning and first-time participants because the groups were unequal in size and equal variances could not be assumed. We report returning minus first-time; this comparison is descriptive because the first-time group has $n = 13$.

Within each year, leadership and team-process items were examined using two-sided Spearman correlations. Spearman's coefficient was chosen because the items were

ordinal and the analysis concerned monotonic association rather than a linear relation between normally distributed scores. Pointwise 95 % percentile-bootstrap intervals used a 10 000-resample individual-record bootstrap (seed 0) to describe uncertainty in these exploratory associations. They are not multiplicity-adjusted and do not account for possible within-team dependence. Analyses used Python 3.12.10, NumPy 2.5.0, pandas 3.0.3, and SciPy 1.18.0.

4.5 Ethics and Data Availability

The survey formed part of a curricular activity. Responses were anonymous, and no monetary incentives were offered. The full questionnaire, cleaned datasets, and de-identified responses containing potentially sensitive context are available from the corresponding author upon reasonable request and institutional approval.

5 Results

5.1 RQ1a: Perceived Focal-Area Skill Change

The 2025 analysis contained 69 complete retrospective focal-area pairs. The mean recalled-before rating was 3.17 (standard deviation SD = 1.41), and the mean after rating was 4.16 (SD = 1.50). The mean within-person difference was 0.99 points (95 % bootstrap confidence interval [CI] 0.68–1.29). Cohen's d_z = 0.77 (95 % bootstrap CI 0.53–1.08). The paired t test gave $t(68) = 6.41$, $p < 0.001$, and the Wilcoxon test gave $W = 68$, $p < 0.001$.

Of the 69 paired responses, 43 (62.3 %) were higher after the activity, 23 (33.3 %) were unchanged, and 3 (4.3 %) were lower. The median change was one point, with an interquartile range from zero to two. Fig. 3 shows both the paired transitions and the distribution of within-person differences. In total, 26 respondents reported no positive change in perceived skill: 23 selected the same rating and three selected a lower rating. Perceived benefit was therefore not uniform.

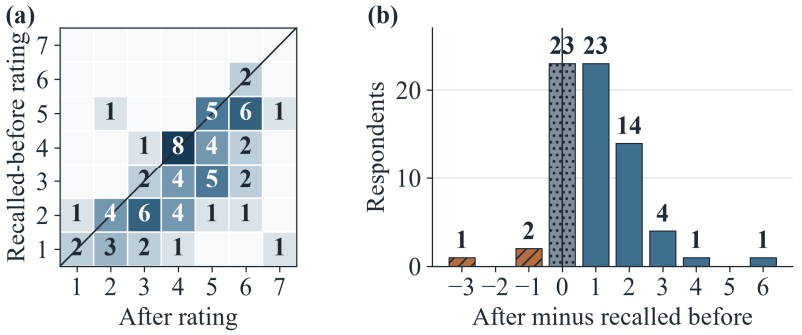


Fig. 3 Retrospective focal-area skill ratings in 2025

The mean perceived change was 1.00 point among the 56 respondents who reported 2024 participation and 0.92 points among the 13 first-time respondents. The estimated difference was 0.08 points (returning minus first-time; 95 % CI −0.90–1.05), with Welch $t(15.62) = 0.17$, $p = 0.869$. The wide interval includes differences of about one scale point in either direction, so the result does not establish equivalence.

5.2 RQ1b: Activity Evaluation

All 69 respondents rated organization, instructional clarity, support, and practical application. Instructional clarity and practical application had medians of 5, while organization and support had medians of 4 (Tab. 4). Each measure was a single item, and the items do not form a validated comparative scale. We therefore interpret the results descriptively.

Tab. 4 Activity-context ratings in 2025

Measure	**Mean**	*SD*	**Median**	**IQR**
Organization	4.20	1.69	4	3–5
Instructional clarity	5.09	1.70	5	4–6
Support quality	4.38	1.33	4	4–5
Practical application	4.80	1.44	5	4–6

All measures used seven-point scales and have n = 69. SD, standard deviation; IQR, interquartile range.

5.3 RQ2: Leadership and Team Processes

In 2025, leadership evaluation was positively associated with conflict resolution (Spearman ρ = 0.35, individual-record bootstrap 95 % CI 0.11–0.56, nominal p = 0.003, n = 69).

Leadership evaluation in 2025 had a mean of 6.04 (SD = 1.48), a median of 7, and an interquartile range of 6–7. Conflict resolution had a mean of 5.45 (SD = 1.41), a median of 6, and an interquartile range of 4–7.

In the 2024 records, leadership evaluation and conflict resolution had ρ = 0.38 (95 % CI 0.01–0.70, nominal p = 0.029, n = 33). Leadership evaluation and cross-year knowledge sharing had ρ = 0.41 (95 % CI 0.08–0.67, nominal p = 0.018, n = 34). The estimate for perceived cross-year benefit was ρ = 0.32 (95 % CI −0.02–0.61, nominal p = 0.069, n = 34). Tab. 5 reports the four exploratory results.

Tab. 5 Exploratory within-year team-process associations

Year	**Variables**	ρ	**95 % CI**	p	n
2024	Leadership evaluation and conflict	0.38	0.01–0.70	0.029	33
2024	Leadership evaluation and cross-year sharing	0.41	0.08–0.67	0.018	34
2024	Leadership evaluation and perceived cross-year benefit	0.32	−0.02–0.61	0.069	34
2025	Leadership evaluation and conflict	0.35	0.11–0.56	0.003	69

Two-sided Spearman correlations used pairwise-complete records. Pointwise percentile-bootstrap intervals resample individual records. ρ, Spearman's rank correlation; CI, confidence interval. The p values are nominal and not cluster-adjusted or multiplicity-adjusted.

On the 2024 ordered scales, leadership evaluation had a median of 4 (interquartile range, IQR, 3–5; n = 34), and conflict resolution had a median of 4 (IQR 3–5; n = 36). Cross-year knowledge sharing had a median of 2 (IQR 2–3), and perceived cross-year benefit had a median of 3 (IQR 2–4), both with n = 37. These summaries are not compared numerically with 2025 because item wording, scales, and administration conditions differed.

No role-based outcome comparison was estimated because all 15 valid leader-role reporters were returning participants, confounding reported role with prior participation.

6 Discussion

6.1 Perceived Skill and Activity Experience

The principal 2025 result was a positive shift in retrospective focal-area ratings. Nearly two thirds of respondents selected a higher rating after the activity, while one third reported no change and three reported a lower rating. The mean difference, its confidence interval, and the distribution of individual responses give a consistent account of perceived change, although they do not show that every participant had the same experience.

Both skill ratings were made after the activity. Respondents may have used knowledge gained during the semester to reinterpret their earlier level or may have sought consistency between the two answers. The estimate is therefore best understood as a retrospective judgement of change rather than a direct measure of learning. The sensitivity comparison by prior participation was also too imprecise to distinguish returning from first-time respondents because the first-time group contained only 13 participants.

The activity-context ratings complement this result. Instructional clarity and practical application had higher medians than organization and support, suggesting useful areas for curricular review. Because these were separate single items rather than a validated comparative scale, the differences should guide questions for the next evaluation rather than rank the quality of activity components.

6.2 Peer Leadership and Cross-Year Team Processes

Within both annual surveys, favorable leadership evaluations were associated with favorable conflict-resolution ratings. The 2024 association between leadership and cross-year knowledge sharing also accords with the intended coordinating role of senior students. This pattern is consistent with project-based learning research that treats communication and role organization as conditions for effective collaboration [7], but the annual estimates are not replications of a common measure because item wording and response scales differed.

The correlations do not establish a direction of influence. Effective coordination may support constructive conflict management; teams experiencing fewer conflicts may evaluate their leaders more positively; and a generally favorable team experience may raise both ratings. The ceiling in the 2025 leadership item and the use of same-respondent measures add further uncertainty. A direct comparison by reported leadership role was not feasible because, among valid role allocations, every respondent reporting leader work had also participated in the previous iteration.

6.3 Implications for Activity Design

The shared architecture is the central instructional feature of the activity. It turns coordination into part of the technical task: service changes, security findings, monitoring requirements, and regulatory decisions must cross team boundaries. Peer leadership therefore has a practical object, and cross-year collaboration is organized around work

that contributes to a common system. This design principle is more important than any single technology in the stack and can be adapted as tools change. The team structure can also absorb new technical tasks without changing the basic organization of the activity. A recurrent-neural-network approach to hash-function generation [20] would give the integration team an implementation problem and the Red, Blue, audit, and documentation teams a common artefact to test and document. A controlled exercise in malware development assisted by large language models [21] would similarly connect attack construction with defensive analysis, monitoring, and regulatory review. In each case, the technical topic matters because it creates work across team boundaries.

Assessment should reflect the same structure. A short common security task could evaluate reasoning shared across teams, while topic-specific rubrics could assess development, infrastructure, monitoring, audit, documentation, or regulatory outputs. Together, these measures would retain the breadth of the project without collapsing distinct technical areas into one self-rating. Explicit role descriptions and a verified roster would also distinguish team leadership from project coordination, development, testing, and documentation.

Organization and support deserve particular attention when the activity is repeated. Standardized onboarding, clear role expectations, and planned exchanges between dependent teams would reduce ambiguity without removing student autonomy. In a military-education setting, these practices also connect technical work with the communication and responsibility expected across specialized cyber roles.

6.4 Priorities for Future Evaluation

A stronger design would collect prospective and post-activity measures using stable self-generated identifiers. Pseudonymous team identifiers would permit cluster-aware analysis, while a verified count of eligible participants would make response rates and possible nonresponse visible. The questionnaire should retain a fixed core of focal-area skill, activity context, leadership, conflict resolution, cross-year knowledge sharing, and role clarity, with consistent wording, anchors, administration procedures, and independently checked translation.

Technical evidence should also be specified before the activity. A common scored security task, topic-specific output rubrics, and privacy-reviewed system indicators would allow reported experience to be compared with observed performance and participation. This combination would test whether favorable leadership and conflict-resolution ratings correspond to stronger team processes or technical outputs rather than relying on same-source correlations.

7 Limitations

All survey responses in both years were collected after the activity. In 2025, both the recalled-before and after focal-area skill ratings were collected after the activity. The recalled-before rating may be affected by memory, response shift, consistency, and demand effects. Students worked in different technical areas, but all rated their skills on the same scale. Without an objective technical assessment, the reported difference is perceived skill change, not demonstrated competence.

Most questionnaire constructs were measured with a single item. The available materials provide no formal reliability or validity evidence. The statistical confidence intervals do not account for this measurement uncertainty.

Of the 69 respondents in 2025, 56 had also participated in 2024, but their anonymous responses cannot be linked across years. The annual datasets are therefore neither independent cohorts nor longitudinal records and should not be treated as a replication. Any differences may reflect sample overlap or changes in wording, scales, or administration. We therefore made no inferential comparison between years.

8 Conclusion

The study's main pedagogical contribution is its shared technical system. It allowed specialized cybersecurity teams to collaborate across study years and work with peer leaders on the same system. The surveys evaluate students' perceptions of this approach. In 2025, 43 of 69 respondents reported a higher retrospective focal-area rating, 23 the same rating, and three a lower rating. Together, the unchanged and lower ratings mean that 26 respondents reported no positive change in perceived skill. This result warrants follow-up.

Leadership ratings were positively associated with conflict-resolution ratings in both surveys. However, these associations do not show that students' technical skills improved or that leadership caused the results. Future iterations should collect prospective measures, score technical tasks, verify participation records, use stable team identifiers, and ask follow-up questions when students report no positive change.

Acknowledgement

This work was developed as part of a research project DZRO-FVT21-KYBERSILY funded by the Ministry of Defence of the Czech Republic.

References

[1] KRASZNAY, C. and B.P. HÁMORNIK. Human Factors Approach to Cybersecurity Teamwork – The Military Perspective. *Advances in Military Technology*, 2019, **14**(2), pp. 291–305. DOI 10.3849/aimt.01296.

[2] HELLE, L., P. TYNJÄLÄ and E. OLKINUORA. Project-Based Learning in Post-Secondary Education – Theory, Practice and Rubber Sling Shots. *Higher Education*, 2006, **51**(2), pp. 287–314. DOI 10.1007/s10734-004-6386-5.

[3] *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity* [online]. New York: Association for Computing Machinery, 2020 [viewed 2026-09-05]. ISBN 1-4503-8919-8. Available from: https://doi.org/10.1145/3184594

[4] *Computing Curricula 2020: Paradigms for Global Computing Education* [online]. New York: Association for Computing Machinery and IEEE Computer Society, 2021 [viewed 2026-09-05]. ISBN 1-4503-9059-5. Available from: https://doi.org/10.1145/3467967

[5] *Criteria for Accrediting Computing Programs* [online]. 2025 [viewed 2026-09-05]. Available from: https://www.abet.org/2026-2027_cac_criteria/

[6] PETERSEN, R., D. SANTOS, M.C. SMITH, K.A. WETZEL and G. WITTE. *Workforce Framework for Cybersecurity (NICE Framework)* [online]. 2020 [viewed 2026-09-05]. DOI 10.6028/NIST.SP.800-181r1. Available from: https://doi.org/10.6028/NIST.SP.800-181r1

[7] BORREGO, M., J. KARLIN, L.D. MCNAIR and K. BEDDOES. Team Effectiveness Theory from Industrial and Organizational Psychology Applied to Engineering Student Project Teams: A Research Review. *Journal of Engineering Education*, 2013, **102**(4), pp. 472–512. DOI 10.1002/jee.20023.

[8] TOPPING, K.J. The Effectiveness of Peer Tutoring in Further and Higher Education: A Typology and Review of the Literature. *Higher Education*, 1996, **32**(3), pp. 321–345. DOI 10.1007/BF00138870.

[9] JOHNSEN, M.M.W., E. SJØLIE and V. JOHANSEN. Learning to Collaborate in a Project-Based Graduate Course: A Multilevel Study of Student Outcomes. *Research in Higher Education*, 2024, **65**(3), pp. 439–462. DOI 10.1007/s11162-023-09754-7.

[10] FRONTERA, P.J. and E.J. RODRÍGUEZ-SEDA. Network Attacks on Cyber-Physical Systems Project-Based Learning Activity. *IEEE Transactions on Education*, 2021, **64**(2), pp. 110–116. DOI 10.1109/TE.2020.3014268.

[11] PRATES, L. and R. PEREIRA. DevSecOps Practices and Tools. *International Journal of Information Security*, 2025, **24**, 11. DOI 10.1007/s10207-024-00914-z.

[12] ŠVÁBENSKÝ, V., J. VYKOPAL, P. ČELEDA and J. DOVJAK. Automated Feedback for Participants of Hands-On Cybersecurity Training. *Education and Information Technologies*, 2024, **29**(9), pp. 11555–11584. DOI 10.1007/s10639-023-12265-8.

[13] BIGGS, J. and C. TANG. *Teaching for Quality Learning at University: What the Student Does*. 4th ed. Maidenhead: Open University Press, 2011. ISBN 0-335-24275-8.

[14] SHUMAN, L.J., M. BESTERFIELD-SACRE and J. MCGOURTY. The ABET "Professional Skills" – Can They Be Taught? Can They Be Assessed? *Journal of Engineering Education*, 2005, **94**, pp. 41–55. DOI 10.1002/j.2168-9830.2005.tb00828.x.

[15] HALL, J.L. and A. RAO. Enabling Teamwork in Cybersecurity Courses. In: L.F. SIKOS and P. HASKELL-DOWLAND, eds. *Cybersecurity Teaching in Higher Education*. Cham: Springer, 2023, pp. 79–102. DOI 10.1007/978-3-031-24216-8_4.

[16] NOLTE, S., G.R. ELSWORTH, A.J. SINCLAIR and R.H. OSBORNE. The Inclusion of "Then-Test" Questions in Post-Test Questionnaires Alters Post-Test Responses: A Randomized Study of Bias in Health Program Evaluation. *Quality of Life Research*, 2012, **21**(3), pp. 487–494. DOI 10.1007/s11136-011-9952-1.

[17] DRENNAN, J. and A. HYDE. Controlling Response Shift Bias: The Use of the Retrospective Pre-Test Design in the Evaluation of a Master's Programme. *Assessment & Evaluation in Higher Education*, 2008, **33**(6), pp. 699–709. DOI 10.1080/02602930701773026.

[18] *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, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)* [online]. 2022 [viewed 2026-09-05]. Available from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[19] LAKENS, D. Calculating and Reporting Effect Sizes to Facilitate Cumulative Science: A Practical Primer for t-Tests and ANOVAs. *Frontiers in Psychology*, 2013, **4**, 863. DOI 10.3389/fpsyg.2013.00863.

[20] TURČANÍK, M. Using Recurrent Neural Network for Hash Function Generation. In: *2017 International Conference on Applied Electronics (AE)*. Pilsen: IEEE, 2017. DOI 10.23919/AE.2017.8053625.

[21] ADAMEC, M. and M. TURČANÍK. Development of Malware Using Large Language Models. In: *2024 New Trends in Signal Processing (NTSP)*. Demanovska Dolina: IEEE, 2024. DOI 10.23919/NTSP61680.2024.10726304.