Research in Education: Case Cybersecurity Project

Ilkka Tikanmäki[1,2] and Jyri Rajamäki[1]
[1] Laurea University of Applied Sciences, Espoo, Finland
[2] National Defence University, Helsinki, Finland

ilkka.tikanmaki@laurea.fi
jyri.rajamaki@laurea.fi

Abstract: This action research investigates the integration of research into education through the Cybersecurity Project Course at Laurea University of Applied Sciences. The research period spans from spring 2022 to autumn 2024, during which the course produced research and development material for the DYNAMO project. The course, designed for bachelor-level students consists of 5 credits, and is aimed at preparing students with essential research skills in safety, security, risk management, and business information technology (cybersecurity). The study focuses on students' development in applying cybersecurity competence, project management, risk assessment, risk control, and communication skills. The research is focused on providing insights that can be used to optimise future educational programs in cybersecurity and risk management. The course utilises a structured module-based methodology to assess the efficiency of the study unit and its potential to influence the design of future security and risk management training programs. The learning platform, CANVAS, enhances students' learning experiences using various tools. This study focuses on evaluating the knowledge and contributions from the DYNAMO project. Collaboration between cybersecurity students and research, development, and innovation partners is enhanced through action research principles and empirical observation. The tasks in the course's six modules and orientation module help students develop their technical and soft skills. The findings show that students had a positive experience using platforms like Microsoft Teams for project management. Despite some finding the course more theoretical than expected, they valued the focus on writing scientific articles and understanding governance models. The course improved students' project management, risk assessment, and ethical considerations in cybersecurity, and led to the creation of several research papers for the DYNAMO project, offering valuable insights into cybersecurity governance, awareness, and threat intelligence. The study concludes that integrating research into cybersecurity education fosters a research culture, enhances flexibility, and prepares students for future projects. Collaboration with companies is crucial for addressing cybersecurity challenges. The course's structured approach and multi-sensory learning techniques provide an enjoyable experience, equipping students with valuable professional skills. These findings highlight the importance of including real-life research projects in the curriculum to improve students' learning and professional competence in cybersecurity.

Keywords: Cybersecurity Education, Research Integration, Project Management, Structured Learning, Peer Review

1. Introduction

The European Union/European Commission has created funding instruments for research in the European Research Area (ERA) through the EU Research and Innovation (R&I) programmes (European Commission Directorate General for Research and Innovation, 2022). Many organisations are increasingly relying on international R&I projects for their R&I investments. It is important for technology developers from all organisations, including industrial companies, small and medium-sized enterprises, research organisations, universities, government agencies, and others, to comprehend the functioning of the European innovation system (Rajamäki & Pirinen, 2022).

Teaching methods and content delivery have been shifted due to the rapid technological development and widespread digital transformation in higher education institutions (HEI). The use of digital technology in higher education has resulted in numerous benefits, such as better accessibility, collaboration, and efficiency. Cybersecurity challenges are part of the challenges with digitalisation in higher education. (Siphambili, 2024)

The project is implemented in teams using a defined process for research and development work. Students' skills in information security planning, development, and management in a target organisation/consortium are developed by implementing an information security project. Research work is carried out by the teams in Laurea's research, development, and innovation project DYNAMO. The project ends up with deliverables, including a technical solution that is demonstrable, a final project report, or a research paper that accurately demonstrates the results. Video presentations are used by the team or individual researcher to report on their progress.

The study's research questions are:

- What knowledge has the DYNAMO project contributed to the students?
- What have the students produced for the DYNAMO?

The introduction is followed by a literature review in Chapter 2, and the research methodology is presented in Chapter 3. Chapter 4 introduces the description of the study unit. The research findings are presented in Chapter 5, and Chapter 6 concludes with a discussion of future research requirements.

2. Literature

The purpose of cybersecurity is to safeguard computer systems and Internet networks from information disclosure, theft, or damage (Cambridge Learner's Dictionary, 2025; Sareen & Jasaiwal, 2021). Cybersecurity involves defending hardware, software, and electronic data from disruption or misdirection in their services.

In today's job market, it is important to possess soft skills (Coghlan & Brannick, 2015; Ruoslahti et al., 2021) such as teamwork, communication, professionalism, and ethics (Rajamäki et al., 2024). Collaboration with companies offers students the benefits of research activities, including developing structured problem-solving skills, acquiring in-depth knowledge, improving teamwork, and improving communication skills (Schefer-Wenzl & Miladinovic, 2022). Incorporating research into the curriculum fosters a culture of research, increases research flexibility, and allows for the recognition and reward of good student performance (Schefer-Wenzl & Miladinovic, 2022). Research projects have made students more prepared for future research projects. Supervisors were more cautious, even though they acknowledged the advantages. However, the research experience was satisfactory for both students and supervisors according to research. (Rajamäki et al., 2024)

The Learning by Developing (LbD) pedagogical model is a fundamental principle that provides a foundation for linking Research, Development and Innovation (R&D&I) projects to cybersecurity education (Raij, 2007). The LbD model emphasises the significance of genuine learning experiences, active involvement in research, creativity, and establishing strong partnerships (Pirinen, 2009; Rajamäki & Pirinen, 2022). The LbD model enhances students' learning experience and prepares them for the realities of cybersecurity by actively involving them in international Research and Development (R&D) projects during their studies (Rajamäki et al., 2024).

Learning is linked to applied R&D projects and a development culture when higher education, externally funded research and development are integrated (Rajamäki, 2018). (Ruoslahti et al., 2018, p. 11) identified three roles when integrating learning into R&D: "1) the responsible teacher, who integrates learning development objectives with research and development activities, 2) the teacher preparing lecture materials, who integrates teaching with research and development activities, and 3) the student, who integrates learning with research and development activities".

Collaboration with companies is essential for cybersecurity universities. This method provides students with knowledge about the current state of the industry. Both teachers and practitioners believe that close collaboration with companies allows for a practical perspective (Bulai et al., 2019). Cybersecurity education poses several challenges. The level of knowledge among teachers, a lack of expertise, funding, and resources are among the issues (Rahman et al., 2020).

3. Method

This study utilised the principles of action research and empirical observation to enhance an applied research methodology. Action research aims to improve specific practices or situations using planning, action, observation, and reflection in an iterative process (Bouki, 2007; Coghlan & Brannick, 2015; Zydney et al., 2002). The study aims to enhance the collaboration between research, development, and innovation (RDI) and work-life partners of cybersecurity students. Figure 1 outlines the practical steps to implement a cybersecurity program module, showing a simplified model depicting the typical action research cycle, where planning, acting, observing, and reflecting are the four steps of each cycle.

Figure 1: Process steps of the study. Adapted from (Susman & Evered, 1978).

The goal of action research is to improve a specific practice or situation through a series of planning, action, observation, and reflection (Coghlan & Brannick, 2015). In this instance, the researchers aim to enhance cybersecurity students' learning experiences and professional competence by employing appropriate R&D&I projects in the degree curriculum. The main objective of action research in real-life situations is to solve real-life problems. Action research is often selected when there is a need for human participation (O'Brien, 2001). Through change and reflection during an ongoing problem, action research combines theory and practice (and researchers and practitioners) under a mutually acceptable ethical framework. The action research process involves researchers and practitioners working together in a specific action cycle, which includes problem diagnosis, action intervention, and reflective learning. (Avison et al., 1999)

4. Research Material

Since 2022, two cybersecurity project courses have been organised twice a year. Implementing cybersecurity project courses in spring 2022, autumn 2022, spring 2023, autumn 2024, and ongoing course in spring 2025 have been commissioned for the DYNAMO project. The materials from previous courses, including students' reports, are accessible and can be used for students' work. The background materials given to students comprised conference papers, DYNAMO public documents, other cybersecurity-related sources and material from previous courses.

5. Study Units' Description

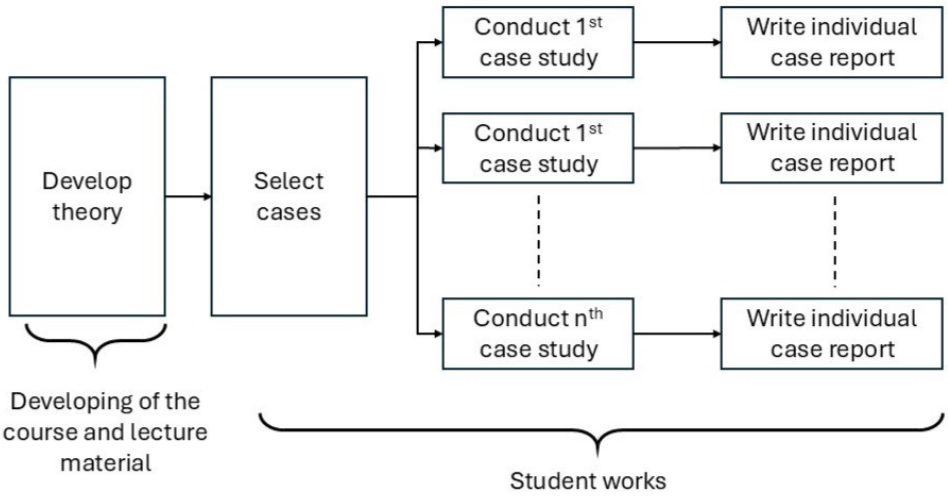

Figure 2: A learning-based approach. Modified from (Modified from Yin, 2009).

The openness principle (Open Science, Open Access, and Open Data) is used: Most assignments (Word documents, PowerPoint presentations, and videos) prepared and presented during this study unit will be open for all participants and future study units. Certain materials may be confidential and for internal use by DYNAMO

Project partners. A student must sign a light non-disclosure agreement (NDA) before releasing such material to them.

5.1 Targets of the Study Unit

In this study unit, students and teachers work as part of an international research consortium that produces new knowledge and other research results using methodological continua, such as understanding, innovating, demonstrating, building, testing, improving, fictionalising, transforming, experiencing, evaluating, implementing, and disseminating. The overall goal of the study module is to understand the European innovation system and how to operate as part of it. Another goal is to apply case studies, design science or service innovations and design tools, and be aware of the latest know-how and cybersecurity knowledge.

Learning objectives of the course are:

- Recognise research gaps and research focus
- Apply chosen information security framework in the project work
- Identify the most significant information security risks in the target organisation
- Find needed controls for identified information security risks
- Present the results of the project both in writing and orally
- Work in the project
- Compose a project plan
- Compose a WBS (work breakdown structure)
- Plan resource allocation
- Compose project updates and report frequently
- Present project results to other groups
- Use project management tool
- Make both self and peer-to-peer evaluation
- Work independently and within a team to reach the required solution

The study unit targets students who can recognise the research gap and research focus by applying the chosen information security framework in the project work. Students should also identify the most significant information security risks in the target organisation and find needed controls for identified information security risks. Students should be capable of presenting the project's results in writing and orally and know how to work on the project. Working on a project consists of composing a project plan and a WBS (work breakdown structure), planning resource allocation, composing project updates, and reporting frequently. Presenting project results to other groups, making self and peer-to-peer evaluations, independently working, and working within the team are learning objectives.

The course is designed for students to identify research gaps and focus on having the ability to apply the selected information security framework in project work. The course is designed to teach students how to present project results in writing and orally, create a project plan, work on projects, and conduct both self- and peer-review. Teachers provided guidance when necessary. Multi-sensory learning and diverse learning materials, such as videos, were utilised in the course. The course was structured into six modules and an orientation module. To receive credit, students are required to complete assignments and reflections in the course.

The working method is to conduct research/development work in teams. A clearly defined process facilitates the project's implementation. Implementing an information security project enhances students' abilities in planning, developing, and managing information security in a targeted organisation/consortium. Research work is carried out by teams in conjunction with Laurea's research, development, and innovation project in this course for the DYNAMO project (DYNAMO project, 2024). Academic work is combined with real industry needs and innovation projects during the course. Integrating an international research project into the curriculum is a method to promote research culture in higher education. In a lively learning environment, students acquire valuable experience and, aside from technical skills, gain significant soft skills such as communication, teamwork, and respect for diversity. (Rajamäki et al., 2024) In this project-based learning, students participated in the development of an international project.

5.2 Course Modules and Assignments

The project results in deliverables, e.g. a demonstrable technical solution, a final project report or a research paper that demonstrates the results appropriately. The teams report and present their progress through video presentations.

The modules are based on the themes, and studies are divided into six modules and an orientation module, as described in the following table.

Table 1: Course modules and schedule.

Module #	The Subject of the Module	Period
Orientation	Basic information about the course	
1	Introduction to the topic and forming of research teams	Weeks 34-36
2	Determination of the RDI problem	Weeks 37-39
3	Project idea focusing and project plan	Weeks 39-42
4	Project work	Weeks 42-45
5	Reporting and sharing results	Weeks 46-50
6	Project finalising	Weeks 51-52

The orientation module had basic information on how to proceed with the study unit, including evaluation criteria and background material on cybersecurity. Module 1 consisted of an online Zoom meeting introducing the study unit and the key concepts of the DYNAMO project. Research teams were formed during Module 1. Module 1 had two assignments: familiarising DYNAMO key concepts and team formations. In Module 2, students planned preliminary research ideas and iterated research ideas according to peer review suggestions. In Module 3, teams made project plans and peer-reviewed other teams' plans. Mid-presentations were introduced, and peer reviews were given in Module 4. The module contained final presentation videos and peer reviews for them. Students wrote draft extended abstracts for the conference and peer-reviewed other teams' draft abstracts in Module 5. The final extended abstract was written and peer-reviewed, and self-assessment was given during the Module. A Work-in-progress (WIP) paper as a final report was written during the module. Project finalising consisted of self-evaluation of project management and teamwork.

The course is divided into 18 assignments. Student earns 3-40 credits from the assignments, depending on the scope of the assignment (Table 2).

Table 2: Assignments and points.

Assignment Name	Points	Assignment Name	Points
1: Familiarising with DYNAMO key concepts	3	2: Formation of teams	0
3: Preliminary research idea	3	4: Research idea peer review	3
5: Iterated research idea	3	6: Opponent team's peer review	3
7: Project plan	20	8: Project plan peer review	3
9: Mid presentation	5	10: Mid-presentation peer review	3
11: Final presentation videos	5	12: Peer review of the final presentation	3
13: Draft extended abstract	15	14: Peer review of draft extended abstract	3
15: Final extended abstract + self-assessment according to the ICCWS/ECCWS criteria	15	16: Final report (WIP) paper	40
17: Self-evaluation of project management and teamwork	5	18: Extra peer reviews of final abstracts	3

Evaluation is based on point gain during the study unit: 80 points are required to complete the course, with the maximum score being 134 points. The course used the digital workspace CANVAS and included lecture materials, recorded videos, presentations, and additional learning materials. Modules were the basis for the course's

structured learning objectives. The course consisted of an orientation period and 6 modules, taking 12 weeks to complete. The instructors could be contacted through a discussion forum. The course employed multi-sensory learning techniques along with a variety of learning materials, such as videos and reading materials. Assignments had to be returned within two (2) to five (5) weeks for each of the six modules in the course.

A broad range of technical skills and strong soft skills, such as communication, critical thinking, and problem-solving, are necessary for cybersecurity professionals. R&D&I projects are being incorporated into cybersecurity curricula by higher education institutes to meet this changing need. Several studies confirm that this strategic approach leads to a win-win situation for students, higher education institutes, and the industry. (Rajamäki et al., 2024)

6. Results

This chapter first discusses the students' viewpoint on the study period. Then, it analyses the added value the course has provided to the DYNAMO project.

6.1 Students' Perspective

The teamwork experience in the course was generally positive for students. Microsoft Teams and other platforms were commonly used by groups for projects and planning materials. Their success was largely attributed to their regular meetings and open communication. The teams were successful in meeting deadlines and producing high-quality work despite some scheduling challenges and occasional absences. According to one student, "Everyone contributed to the project consistently, and I have no negative feedback for any team member."

The course was perceived to be more theoretical than some students anticipated. The emphasis on writing scientific articles and understanding governance models was appreciated by some, but others were looking forward to more hands-on, practical cybersecurity work. According to one student, "The course was more about writing theories in the context of cybersecurity. It's not always a negative thing, but it's not what I thought it would be".

Even though they faced obstacles, students believed that they had acquired valuable skills and knowledge. Project management, risk assessment, and the importance of ethical considerations in cybersecurity were topics they learned about. They were able to enhance their teamwork and communication skills through the course. According to a student's reflection, 'This project taught me a great deal about the importance of balancing technical solutions with ethical considerations, especially in sensitive areas like cybersecurity.'

Teams had different approaches to project management. A week-by-week plan was followed by some teams, while others prioritised the overall project from the start. Teams were able to meet deadlines and produce quality work despite their different approaches. Project management was perceived as very loose by one student. One team conducted a week-by-week assessment and then assessed what was required for the next deadline.

7. Benefits for the DYNAMO Project

The courses have led to the creation of research for the DYNAMO project. The conference papers for the DYNAMO project, which came from the Cybersecurity Project course, are presented in Table 3 below.

Table 3: Articles produced for DYNAMO.

Title	Author(s)	Publication
Governance and management information system for cybersecurity centres and competence hubs	Jyri Rajamäki, Janne Lahdenperä	22nd European Conference on Cyber Warfare and Security
Improving the Cybersecurity Awareness of Finnish Podiatry SMEs	Rajamäki et al.	WSEAS Transactions on Computers
Implications of GDPR and NIS2 for Cyber Threat Intelligence (CTI) Exchange in Hospitals	Rajamäki et al.	WSEAS Transactions on Computers

Title	Author(s)	Publication
E-EWS-Based Governance Framework for Sharing Cyber Threat Intelligence in the Energy Sector	Jyri Rajamäki, Asfaw Feyesa and Anup Nepal	European Conference on Cyber Warfare and Security (2024)
DYNAMO and the EU AI Act: Balancing Innovation and Regulation	Tikanmäki et al.	International Conference on Cyber Warfare and Security (2025) In press
Navigating the Cyber Resilience Act: Implications for the Dynamo Horizon Project	Rajamäki et al.	European Conference on Cyber Warfare and Security (2025) In press
AI Governance: Achieving EU AI Act Compliance in the Dynamo Project	Tikanmäki et al.	European Conference on Cyber Warfare and Security (2025) In press
MISP Management Models for Effective Threat Intelligence in Cybersecurity	Tikanmäki et al.	European Conference on Cyber Warfare and Security (2025) In review
Cyber Threats in Hospitals: GDPR and NIS2 Regulations in Preventing USB Injections	Tikanmäki et al.	International Conference on Cyber Warfare and Security (2025) In press
A CTI Governance Framework for Enhanced Resilience in Critical Infrastructure Sector	A Nepal et al.	European Conference on Knowledge Management (2025) In review
AI Governance: Achieving EU AI Act Compliance in the Dynamo Project	Burns et al.	European Conference on Cyber Warfare and Security (2025) In press
Enhancing Risk Management on IoT Medical Devices	Tikanmäki et al.	European Conference on Cyber Warfare and Security (2025) In review
AI and Cyber Threat Intelligence Management in the Energy Sector	Rajamäki et al.	European Conference on Knowledge Management (2025) In review

The table presents an in-depth analysis of recent and upcoming cybersecurity research, emphasising topics such as GDPR, NIS2 regulations, AI governance, cyber threat intelligence, and risk management in various sectors, such as healthcare and energy. The authors are teachers and students, who have written for multiple conferences and journals.

Table 4 below contains conference papers written for the DYNAMO project based on or as part of the thesis.

Table 4: Thesis or part of thesis-based articles.

Title	Author(s)	Publication
Implementation of OSINT for Improving an International Finance Sector Organization's Cybersecurity	Tiitta & Rajamäki	Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS
Utilisation and Sharing of Cyber Threat Intelligence Produced by Open-Source Intelligence	McMenamin & Rajamäki	Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS)
Governance for Cyber Threat Intelligence (CTI) Exchange Across the DYNAMO Resilience Cycle	Nepal & Rajamäki	European Conference on Cyber Warfare and Security (2025) In review
Enhancing Cyber Threat Intelligence (CTI) Exchange: A Governance Model for the DYNAMO Platform	Rajamäki, Nepal and Chalkias	European Conference on Cyber Warfare and Security (2025) In review

As Table 4 indicates, four conference papers were written either based on the thesis or as part of them. Conference papers that contribute to the DYNAMO project and thesis are highlighted in this table. The focus is on implementing and governance cyber threat intelligence (CTI). These papers address different aspects of CTI, such as the utilisation of open-source intelligence (OSINT) and governance models for efficient CTI exchange. The research is designed to enhance cybersecurity in various sectors using the DYNAMO platform.

8. Discussion

Students and teachers need cybersecurity awareness to identify cybercrimes and cyber threats. In preventing cybersecurity threats, it is crucial to have education or training. To be safe, it is important to be aware of the

potential risks. Education, teacher knowledge level, and expertise are among the challenges that cybersecurity poses. People's mindsets can be changed through cybersecurity education. A lack of knowledge about cybersecurity's importance and implications is the cause of a person's lack of cybersecurity awareness. Increasing safety and security can be achieved through the incorporation of cybersecurity into education in educational institutions and by raising awareness.

The students deemed the course a bit distant and hoped for more face-to-face classes where they could converse with teachers and other students about course-related matters. The students suggested improving the study unit by providing more feedback on their assignments. Students sought more detailed information about the purpose and functioning of academic conferences. One student had expected the course to be more practical in terms of cybersecurity, not theoretical. The course's unclear structure and tasks caused frustration among one group. Clear instructions on which issues should be considered were required for the self-assessment task. Several students claimed that full-time work sometimes hindered their ability to concentrate on their studies. The course was considered interesting and useful for learning how to write scientific articles and learning about the DYNAMO project. It was desired to have a complete view of the entire course so that students could start with a clear understanding of what is being done and why. Due to the course schedule being too tight, the schedules often did not work, and it was anticipated to change.

“While this assignment seemed confusing in terms of the actual practical application of cybersecurity to the project framework, I was surprised to see it as a thorough exposure experiment for writing real-life research papers”.

The course examined a structured module-based approach to evaluate the effectiveness of the study unit and what insights it can provide for the design of future security and risk management training programs. The course content was well-received by students, with topics like cyberattacks, business continuity management (BCM), and threat intelligence. Valuable insights were gained from the DYNAMO project and other materials. According to one student, learning the connection between cyberattacks, BCM, Echo-Early Warning System (E-EWS), and threat intelligence has been extremely beneficial.

The overall impression was that the course was both demanding and rewarding. The chance to work on real-life research projects allowed students to feel proud of their achievements. Their positive experience was attributed to the collaborative environment and the support from teammates, which were highlighted as key factors. One student summarised, "Overall, this course was a great opportunity to improve technical and teamwork skills. I am proud of how our team worked together and the quality of the project we delivered."

8.1 Teamwork

The work in the group was evenly distributed, and all members contributed: “We support each other in our work and provide feedback. We similarly work on tasks and can rely on each other's judgement when it comes to editing, etc”. Some teams had previous experience working together, and thus, they felt it was easy to divide the responsibilities. One team selected a project manager from among them, whose task was, among other things, to book common working times and assign tasks for each team member. The team's working methodology was to work independently before meeting once a week to bring together various areas.

The importance of teamwork and collaboration was consistently emphasised by students. Microsoft Teams and WhatsApp were used by many groups to communicate and manage projects. The key to their success was having regular meetings and open communication. A student mentioned that we all worked in unison to bring the project to a productive conclusion, and we gained a lot from each other.

8.2 Challenges and Limitations of the Study

A complete view of the entire course was sought to provide a complete understanding of what happens and why from the start. The schedules did not always work because the course schedule was considered too tight, and it was hoped to change. The technical limitations made it difficult to co-edit the documents. A few students mentioned areas in which the course could be improved. They proposed more contact lessons to facilitate conversations with peers and instructors. Common requests were for teachers to provide clearer instructions and more detailed feedback. Some students admitted they were uncertain about what the assignments demanded of them. Some of the instructions were not easy to follow or seemed incomplete.

9. Conclusion

The findings indicate that students had a positive experience with a course integrated into an international R&D project. Students appreciated using similar platforms like Microsoft Teams in studies as companies use in the workplace. Although the course was more theoretical than expected, students valued the emphasis on writing scientific articles and understanding governance models. The course improved students' skills in project management, risk assessment, and ethical considerations in cybersecurity. Additionally, the course resulted in the creation of several research papers for the DYNAMO project, providing valuable insights into cybersecurity governance, awareness, and threat intelligence.

The study highlights that integrating research into cybersecurity education fosters a research culture, enhances flexibility, and prepares students for future projects. Collaboration with companies is crucial for addressing cybersecurity challenges. The course's structured approach and multi-sensory learning techniques make it an enjoyable learning experience, equipping students with valuable professional skills

As a follow-up study, the career development and professional success of students who have completed the course should be tracked over the long term. It could be investigated whether exposure to international research and development activities during their studies has influenced their career paths.

Acknowledgements

This study has received funding from the Developing Cybersecurity Education and Related Cooperation in Higher Educational Institutions project granted by the Ministry of Education and Culture. The views expressed are those of the author(s) only and do not necessarily reflect those of the funder. The granting authority can be held responsible for them.

Ethics Declaration

Ethical clearance was not required for the research.

AI Declaration

The paper's spelling was verified using the artificial intelligence tool.

References

Avison, D. E., Lau, F., Myers, M. D., & Nielsen, P. A. (1999). Action research. *Communications of the ACM*, *42*(1), 94–97. https://doi.org/10.1145/291469.291479

Bouki, V. (2007). Undergraduate Computer Science Projects in UK: What is the point? *Proceedings of Informatics Education Europe II (IEEII 2007) Developments in South East Europe*, 176–184.

Bulai, R., Țurcanu, D., & Ciorbă, D. (2019). Education in Cybersecurity. *Central and Eastern European eDem and eGov Days*, *335*, 33–44. https://doi.org/10.24989/ocg.v335.2

Cambridge Learner's Dictionary. (2025). *cybersecurity noun—Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com*. Cybersecurity. https://dictionary.cambridge.org/dictionary/english/cybersecurity

Coghlan, D., & Brannick, T. (2015). *Doing action research in your own organization* (2nd ed., Vol. 12). SAGE Publications Ltd. https://kyptraining.com/wp-content/uploads/2020/05/DOING_ACTION_RESEARCH_IN_YOUR_OWN_ORGANI.pdf

DYNAMO project. (2024, January 9). *DYNAMO Mission and Objectives*. https://horizon-dynamo.eu/about/

European Commission Directorate General for Research and Innovation. (2022). *European Research Area policy agenda: Overview of actions for the period 2022 2024.* (p. 25). Publications Office. https://data.europa.eu/doi/10.2777/52110

O'Brien, R. (2001). An Overview of the Methodological Approach of Action Research. In R. Richardson (Ed.), *Theory and Practice of Action Research* (pp. 1–13). Universidade Federal da Paraíba. http://www.web.ca/~robrien/papers/arfinal.html

Pirinen, R. (2009). Learning by developing. *International Journal of Emerging Technologies in Learning (iJET)*, *4*, 46–58. https://doi.org/10.3991/ijet.v4s3.1103

Rahman, N., Sairi, I., Zizi, N., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Raij, K. (2007). *Learning by developing*. Laurea University of Applied Sciences. https://www.theseus.fi/handle/10024/114677

Rajamäki, J. (2018). *Industry-university collaboration on IoT cyber security education: Academic course: "Resilience of Internet of Things and cyber-physical systems."* 1969–1977. https://doi.org/10.1109/EDUCON.2018.8363477

Rajamäki, J., & Pirinen, R. (2022). Resilient Learning as a Tool for Excellence: Laurea's Students in the ECHO H2020 Project during the COVID-19 Pandemic. *2022 IEEE Global Engineering Education Conference (EDUCON)*, 1889–1894. https://doi.org/10.1109/EDUCON52537.2022.9766796

Rajamäki, J., Rathod, P., Kämppi, P., & Pirinen, R. (2024). Integrating International Research-Innovation Projects and Working Life Partners into Cybersecurity Degree Programme. *2024 IEEE Global Engineering Education Conference (EDUCON)*, 1–9. https://doi.org/10.1109/EDUCON60312.2024.10578728

Ruoslahti, H., Coburn, J., Trent, A., & Tikanmäki, I. (2021). Cyber Skills Gaps – A Systematic Review of the Academic Literature. *Connections: The Quarterly Journal*, *20*(2), 33–45.

Ruoslahti, H., Rajamäki, J., & Koski, E. (2018). Educational Competences with regard to Resilience of Critical Infrastructure. *Journal of Information Warfare*, *17*(3), 1–16.

Sareen, D. A., & Jasaiwal, S. (2021). Need of cyber security education in modern times. *International Journal of Multidisciplinary Trends*, *3*(2), 188. https://doi.org/10.22271/multi.2021.v3.i2c.179

Schefer-Wenzl, S., & Miladinovic, I. (2022). Integrating Research Elements into Computer Science Degree Programs: Preparing Students to Engage in Research Projects. *2022 IEEE Global Engineering Education Conference (EDUCON)*, 1069–1073. https://doi.org/10.1109/EDUCON52537.2022.9766523

Siphambili, N. (2024). Exploring Cybersecurity Implications in Higher Education. *European Conference on Cyber Warfare and Security*, *23*(1), Article 1. https://doi.org/10.34190/eccws.23.1.2306

Susman, G. I., & Evered, R. D. (1978). An Assessment of the Scientific Merits of Action Research. *Administrative Science Quarterly*, *23*(4), 582. https://doi.org/10.2307/2392581

Yin, R. K. (2009). *Case study research: Design and methods* (No. 1; 4th ed., Vol. 14). Thousand Oaks, CA: Sage Publications. https://journals.nipissingu.ca/index.php/cjar/article/view/73

Zydney, A. L., Bennett, J. S., Shahid, A., & Bauer, K. W. (2002). Impact of Undergraduate Research Experience in Engineering. *Journal of Engineering Education*, *91*(2), 151–157. https://doi.org/10.1002/j.2168-9830.2002.tb00687.x