Proceedings of 5th International Conference CNDGS'2026
ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / **https://doi.org/10.47459/cndcgs.2026.136**

From Theoretical Cryptology to Cybersecurity: Education and Research

Tomáš FABŠIČ[1], Viliam HROMADA[1], Milan VOJVODA[1]*, Pavol ZAJAC[1]

[1] Institute of Computer Science and Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava, Ilkovičova 3, 841 04 Bratislava, Slovakia

*Correspondence:*milan.vojvoda@stuba.sk*

Abstract

This paper traces cryptology and cybersecurity education and research at the Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava, from the late-1980s CRYPTO seminar to the 2024/25 launch of a Cybersecurity master's specialization. We outline the bachelor's and master's curricula, research supported by three NATO Science for Peace and Security projects on post-quantum cryptography, and student engagement through theses, the Locked Shields exercise, and the new Cybersecurity Competence Centre. Enrolment in security specializations grew from 15% in 2022 to 43% in 2026, suggesting the 2024 restructuring was well-timed.

KEY WORDS: *cybersecurity education, cryptology education, cybersecurity research, cryptology research*

Citation: Fabšič, T.; Hromada, V.; Vojvoda, M.; Zajac, P. From Theoretical Cryptology to Cybersecurity: Education and Research. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959, https://doi.org/10.47459/cndcgs.2026.136

1. Beginnings of Cryptology and Cybersecurity at FEI STU

The dynamic development of information and communication technologies during the second half of the 20th century brought exponential growth in security risks alongside undeniable benefits. Our institution, Faculty of Electrical Engineering and Information Technology of the Slovak University of Technology (FEI STU) in Bratislava, has played a significant role in training new engineers in fields such as computer science, robotics and cybernetics, electronics, power engineering, etc. In the late 1980s, Professor Grošek and his colleagues - Professor Štefan Prorubský, Associate Professor Ladislav Satko and Associate Professor Karol Nemoga - founded the CRYPTO seminar at the Department of Mathematics of FEI STU. They engaged in intensive study of the available literature and dedicated themselves to cryptology, particularly from a mathematical perspective — a natural fit given their backgrounds. In 1992, Otokar Grošek and Štefan Porubský published one of the first modern books on cryptology in the former Czechoslovakia [1]. The founders of the CRYPTO seminar offered bachelor and master theses for the students of the Informatics study programme, with topics covering mostly pseudorandom generators and sequences, ciphers and their cryptoanalysis. Professor Grošek created in 1997 a new course – Mathematical Introduction to Cryptology, that was optional for students from the whole faculty.

In 2000, the specialization in Security of Information Systems was created under the study programme Informatics. The specialization offered courses on Coding Theory (Satko), Introduction to Cryptography (Grošek), Security in Computer Networks (Nemoga), and Cryptanalysis of Ciphers (Grošek, Satko, Nemoga, Vojvoda). All the courses were focused on deep understanding of the principles, mainly from the mathematical point of view. Each course had 2-3 hours regular lectures every week, 2 hours seminars and homework assignments, in which the students solved appropriate tasks to demonstrate understanding of the issues. The diploma theses were also included in the study programme, focusing on more practical aspects of cybersecurity and cryptography engineering. The first team projects, that were in the curricula, as well, were devoted to statistical characteristics of the Slovak language, to the implementation of the statistical tests on pseudorandomness for binary sequences, later on factoring RSA modulus, where our students successfully repeated the factorization of RSA-100 and RSA-110 in 2002.

A significant milestone was October 1, 2003, when the Faculty of Informatics and Information Technologies (FIIT STU) was established. All staff of the Department of Informatics and Computer Engineering at FEI STU transferred to

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic

FIIT STU. However, FEI STU wanted to continue offering a study program in the field of Informatics. This was an opportunity for Professor Grošek to create a new study program at FEI STU - Applied Informatics - and to include subjects from selected areas of security at both the master's and the bachelor's degrees.

2. Security of Information Systems Specialization at Bachelor's Degree

In its present form, the Applied Informatics bachelor's programme covers the standard core courses in mathematics, programming, and computer science — including Calculus, Discrete Mathematics, Linear Algebra, Statistics, Logic Systems, Introduction to Programming, Programming in C, Programming Techniques, Object-Oriented Programming, Introduction to Database Systems, Artificial Intelligence, Analysis and Complexity of Algorithms, Operating Systems, Software Engineering, and Development of Applications, among others. At the start of the third year, students choose one of two specializations: Security of Information Systems or Intelligent Software Systems. The Security of Information Systems track includes Classical Ciphers, Computer Crime, and Fast Algorithms, providing a foundation for both master's-level focus areas — mathematical cryptology and cybersecurity.

The Classical Ciphers course introduces students to the theoretical and practical foundations of historical ciphers, along with the historical context of their development and deployment. It also strengthens students' programming skills. The syllabus covers modular arithmetic, permutations, steganography, transposition and substitution ciphers, cipher machines, cryptanalysis (basic, computer, and advanced), and the statistical properties of languages.

The Computer Crime course examines the various forms of computer crime and the countermeasures available against them. Students learn how these offences are classified under the Slovak Criminal Code and the relevant regulations of the Slovak Republic and the European Union. Through practical exercises, they also gain hands-on experience with the techniques associated with each form. The syllabus includes an introduction to computer crime, hacking, social engineering, internet security, phishing, malware, botnets and spam, cracking and pharming, warez, spoofing and cybersquatting, legislation, and combined forms of computer crime.

The teaching includes regular lectures, seminars, and homework assignments. Students gain practical experience with cryptanalysis of classical (old) ciphers and deciphering cryptograms. An interesting challenge is always the final exam in the Classical Ciphers course, where students have 24 hours to decipher a message encrypted with one of the old ciphers using available tools.

The traditional academic model — comprising lectures, seminars, assignments, and exams — functions as a deliberate progression through the hierarchical levels of Bloom's Taxonomy. Lectures establish the groundwork by targeting Lower-Order Thinking Skills (LOTS) such as Remembering and Understanding, while seminars and practical exercises shift the focus toward Applying and Analyzing information in controlled settings. This cognitive journey culminates in independent assignments and final examinations, which challenge students to reach Higher-Order Thinking Skills (HOTS) like Evaluating and Creating. By aligning each instructional phase with these levels, the curriculum ensures that students transition from passive comprehension to an integrated, professional mastery of the subject matter.

Bachelor's and Master's theses, along with Team projects, serve as the definitive application of Problem-Based Learning (PBL), effectively bridging the gap between classroom theory and professional reality. By shifting the focus from passive instruction to active inquiry, these projects challenge students to identify real-world technical gaps and navigate the entire lifecycle of a solution—from initial analysis to final synthesis. While individual theses cultivate deep analytical rigor and self-directed research, Team projects introduce the essential complexities of collaboration, communication, and system integration. Ultimately, this project-driven approach ensures that students move beyond rote memorization to master the Higher-Order Thinking Skills (HOTS) required to tackle the messy, unpredictable challenges of the modern landscape.

3. Security of Information Systems Specialization at Master's Degree

The Applied Informatics master's programme builds directly on the bachelor's, deepening students' theoretical foundations and providing focused specialization in their chosen area.

The first year combines compulsory subjects — Introduction to Computer Security, Logic, Machine Learning and Neural Networks, Algorithms and Data Structures, Automata and Formal Languages — with a structured set of semi-compulsory and elective courses through which students profile their specialization. Several of the courses that lie at the core of the Security of Information Systems specialization are described in more detail below.

In the Introduction to Computer Security course, students gain a working understanding of the practical information security problems they will encounter as developers and learn how to address them. The course is built around the topics that every programmer and software developer should be familiar with, combining theoretical foundations with hands-on homework assignments that students must defend in order to qualify for the exam. The syllabus covers basic security concepts and terminology, threat modelling (STRIDE), confidentiality protection through symmetric and asymmetric encryption, integrity protection via hash functions, message authentication codes and electronic signatures, and user authentication including passwords, password storage, one-time passwords, multi-factor methods, and biometrics. Further topics include authentication and authorization using cryptography, key management, OAuth, and PKI; secure coding and the handling of malicious input such as format-string attacks and injection; operating-system security and malware; network security (link-layer protection, secure channels, IPSec, VPN, TLS, Tor); web security (client-state

manipulation, CSRF, JavaScript-based attacks, OWASP); applied protocols underlying cryptocurrencies and blockchain technologies; and current topics in the field, including the security implications of artificial intelligence, and security auditing.

The Cryptography course teaches students the fundamental principles behind modern symmetric and asymmetric cryptosystems and the mathematical apparatus on which they rest. They become familiar with the cryptographic primitives most widely used in practice and understand the role these primitives play in securing communication, as well as the assumptions on which the security of these systems depends. The course also addresses the rapidly growing interest in post-quantum cryptography, introducing students to the reasoning behind this shift and to the operating principles and underlying mathematics of selected prominent post-quantum cryptosystems. The syllabus covers an introduction to cryptography, stream ciphers, the Advanced Encryption Standard (AES), public-key cryptography (the RSA cryptosystem, cryptosystems based on the discrete logarithm problem, and elliptic curve cryptosystems), digital signatures, hash functions, and post-quantum cryptography.

In the Network Encryption course, students learn to use cryptographic tools to achieve secrecy, integrity, authentication, and non-repudiation across networks, and to recognise the most common attacks against cryptographic protocols and the techniques used to prevent them. They study selected protocols for authentication and key establishment in depth, becoming able to analyse whether a given protocol delivers properties such as forward secrecy, strong entity authentication, the good-key property, and key confirmation, and they become acquainted with the central design principles for such protocols. The course also introduces the concept of provable security together with its limitations, surveys software tools for protocol verification, and covers several cryptographic primitives essential to modern systems — commitment schemes, secret sharing, secure multi-party computation, and zero-knowledge proofs. The syllabus opens with cryptographic goals and primitives (encryption schemes, hash functions, message authentication codes, and digital signatures), public-key certificates and PKI, freshness mechanisms (nonces, timestamps, counters), and the main classes of attack on cryptographic protocols (eavesdropping, message modification, replay, reflection, and denial of service). It then turns to the goals and design principles of authentication and key-establishment protocols, provable security and protocol-verification tools, protocols based on symmetric cryptography (Needham–Schroeder Shared Key, Kerberos) and asymmetric cryptography (Needham–Schroeder Public Key), key-agreement protocols and their attacks (man-in-the-middle and small-subgroup attacks on Diffie–Hellman, MTI, STS), TLS 1.2 and 1.3, and the Signal protocol. The course concludes with commitment schemes, zero-knowledge proofs (Schnorr identification, the Fiat–Shamir transform, Schnorr signatures, and general-purpose ZKPs), key management (rotation, revocation, and threshold-based decentralisation), threshold cryptography (Shamir's secret sharing, multi-signature schemes), and secure multi-party computation.

Through the Practical Information Security course, students become familiar with the processes and procedures used to secure information systems in everyday practice. The course is built around hands-on application: lectures alternate with laboratory work, and students complete several smaller assignments together with a larger written project. It is organised into four thematic blocks — formal security (security standards and security management), network security (architecture, components, and secure communication), systems and applications security (authentication and authorization, trusted systems, and malware), and privacy (web and email privacy, anonymity, and the techniques used to protect personal information online).

Building on the foundations laid in Cryptography, the Design and Cryptanalysis of Ciphers course gives students a deeper view of how modern cryptographic systems are designed and how they are attacked. The course's homework assignments are also designed to develop research skills, training students to work with primary literature, carry out their own investigations, and present the results. The syllabus begins with the role of cryptography in information security, computational models of cryptographic primitives, perfect block and stream ciphers, hash functions, and an overview of asymmetric cryptography. It then covers generic attacks (brute force, meet-in-the-middle, Hellman's attack, and time–memory trade-offs); Boolean functions and the Shannon design principles of confusion and diffusion as realised in product ciphers and substitution-permutation networks; the linear and differential cryptanalysis of SPN; and block-cipher design culminating in AES (wide-trail strategy, performance and security analysis, modes of operation, and concrete attacks on CBC and SSL). The remainder of the course is devoted to stream ciphers (LFSR-based designs, RC4, and attacks against them), hash functions and MACs (construction, use, and attacks), asymmetric cryptography with selected algorithms (RSA, DSA, ECDSA) and the corresponding attacks and security analysis, post-quantum cryptography, and side-channel attacks.

4. New Specialization at Master’s Degree: Cybersecurity

The contemporary geopolitical landscape is increasingly characterized by continuous hybrid warfare [2], where cyberspace has firmly established itself as a primary domain of global conflict. The critical national infrastructure, military communications, and sovereign supply chains are routinely targeted by various attacks [3]. Traditional IT and software engineering education is no longer sufficient. The restructuring of the Applied Informatics study programme was necessary. The initiator of these changes was our graduate Michal Ďorda (Security of Information Systems specialization, IT security auditor). The aim was to integrate the already established advanced cryptology and cybersecurity, tailored for the operational demands of national defense as well as the new business needs. This effort resulted in the creation of the Cybersecurity specialization under the study programme Applied Informatics at master's level in the academic year 2024/25.

This means that from the academic year 2024/25, master's students in Applied Informatics can choose from two

information-security-related specializations: the original Security of Information Systems specialization and the newly established Cybersecurity specialization. Alternatively, they can choose the Artificial Intelligence specialization or the Intelligent Software Systems specialization. The establishment of the Cybersecurity specialization was accompanied by the creation of several new courses. The core of this specialization is formed by three courses shared with the Security of Information Systems specialization (Introduction to Cryptography, Introduction to Computer Security and Practical Information Security) and three newly established courses which are described in more detail below.

The IT and Security Audit (ITSA) course gives students a comprehensive view of information-systems auditing and are prepared for the professional roles available in security and audit practice. Lectures introduce the main areas — the foundations of information-systems security, security standards and regulations, security policies and procedures, identification and authentication, and security testing — and devote dedicated attention to network security, cloud auditing, and the legislative framework specific to IT and security audit. Students also examine the different types of audit, the tools used to support them, and the ethical aspects of the auditor's role, with practical case studies bringing the theoretical material into a real-world setting. The syllabus covers an introduction to IT and security auditing, the types of IT and security audits, the auditor's profile and professional development, the audit object (assets) and associated risks, the audit process and its management, the auditing of procedural and organisational measures, audits assessing compliance with security standards and legislation, the auditing of technical measures, supporting tools, supply-chain auditing, audits in modern technologies (cloud and AI), and practical aspects of security audit. The final examination for the ITSA course offers a unique and immersive experience, as students are required to defend the audit reports they had meticulously developed throughout the semester before a panel of Chief Information Security Officers (CISOs) from major IT companies and banks. This high-stakes setting allows these industry leaders to probe deep into the students' technical reasoning, providing a rigorous validation of their understanding while offering invaluable practical insights from the front lines of cybersecurity. By experiencing this live defense process, students not only prove their expertise but also gain a realistic preview of the professional pressures and communication standards expected at the executive level.

The Incident Response Management (IRM) course provides students with a working knowledge of cyber threats and security incidents, and of the techniques available for responding to them. The course is organised around the full incident-response life cycle, training students to manage an incident from initial identification, through containment and prevention of its spread, to the restoration of normal operations. The syllabus covers the incident-response process, the creation of incident reports, the management of cyber incidents and the frameworks used to structure incident response, cyber risks and the attack life cycle, network security, the detection and identification of events, preventing the spread of an incident, the resumption of operations afterwards, threat intelligence, threat hunting, and practical examples drawn from the field.

The Digital Forensic Analysis (DFA) course equips students with practical knowledge they can apply to the investigation of security incidents, learning the methods used to recover, preserve, and interpret digital evidence. The course is organised around the full forensic workflow, from securing the integrity of evidence at the point of collection, through detailed examination of storage media, file systems, and operating-system artefacts, to the production of formal forensic reports. The syllabus opens with the foundations of digital forensic analysis, the preservation of digital evidence, and the processing and analysis of storage media; continues with file-system analysis, the analysis of Windows artefacts (in two parts), and the analysis of Windows physical memory; and concludes with forensic timelining, an introduction to mobile-device analysis, an introduction to malware analysis, automated data-analysis procedures, and the safe handling of forensic material and reporting. The final examination for the DFA course is uniquely delivered as a Capture The Flag (CTF) competition, where students tackle real-world forensic challenges that were directly integrated into the semester's curriculum. Rather than abstract theory, the exam utilizes authentic scenarios and datasets discussed during lectures, requiring students to apply their investigative skills to reconstruct actual digital events in real-time. This approach ensures that the assessment is not just a test of knowledge, but a practical validation of their ability to solve the same complex problems they will encounter in professional forensic practice.

All three newly established courses received excellent student evaluations in the 2024/25 academic year, as shown in Table 1. Students are generally motivated to complete anonymous course evaluations because doing so gives them the opportunity to create their schedules for the next semester earlier. The lower participation rate in the evaluation of the DFA course can likely be explained by the fact that this course is taught in the final year of study. In the following semester, students only attend diploma thesis consultations, which are arranged individually with their thesis supervisors, so the incentive of earlier schedule creation is no longer relevant for them. **S**tudent evaluations of courses are in Table 1.

Table 1. **S**tudent evaluations of courses.

Course	ITSA	IRM	DFA
Total students	17	28	22
Respondents	12 (70.59 %)	23 (82.14 %)	6 (27.27 %)
Lecture attendance	8 x 100 %, 4 x ≥ 75 %	10 x 100 %, 9 x ≥ 75 %	5 x 100 %, 1 x ≥ 75 %
Lecture grade	1.13	1.17	1.00
Seminar grade	1.13	1.20	1.16

Notes: IT and Security Audit (ITSA), Incident Response Management (IRM) and Digital Forensic Analysis (DFA) in the academic year 2024/25. Grades on a 1–3.5 scale, 1 = best.

Students particularly appreciated the practical focus of the new cybersecurity courses, including the large number of real-world examples, the connection of assignments to practical industry contexts, and the greater flexibility in solving tasks. On the other hand, it is necessary to improve the overall organization of these courses, especially since they are taught by external instructors, as well as provide better support for working with the academic information system.

5. Increased Student Interest in Information-Security-related Specializations

The introduction of the Cybersecurity specialization in 2024 led to increased interest in information-security-related specializations among bachelor's and master's students in Applied Informatics, as demonstrated in Table 2. We believe that the incentive of finding an interesting job was crucial. Furthermore, the original specialization Security of Information Systems was focused more on cryptographic primitives, which requires a deep knowledge in mathematics and that was a deterrent for many students. A third advantage for the Cybersecurity specialization was an intensive cooperation with experts from government institutions: The Cyber Defence Center of the Slovak Republic, The Ministry of Defence of the Slovak Republic, The National Security Authority of the Slovak Republic; and from business: enigMMA, IstroSec, Binary House, Binary Confidence, Citadelo, ALISON Slovakia, EMM, etc.

Table 2. Interest in information-security-related specializations among students in the Applied Informatics bachelor's and master's study programmes.

Year	Percentage of bachelor's students choosing an information-security-related specialization	Percentage of master's students choosing an information-security-related specialization
2026	42,65%	Not known yet
2025	36,69%	30,21%
2024	19,43%	29,73%
2023	16,19%	22,11%
2022	15,02%	21,98%

Interest in information-security-related specializations among students in the Applied Informatics bachelor's and master's study programmes at Faculty of Electrical Engineering and Information Technology of Slovak University of Technology in Bratislava (Table 2).

6. Plans for Future Improvements in Information-Security-related Specializations

We are moving toward a strategic integration of the Security of Information Systems together with the Cybersecurity specialization. This merger is driven by the natural synergy between these disciplines, allowing us to create a more cohesive curriculum and significantly broaden the range of elective courses available to our students. This consolidation also responds to current enrollment trends and student perceptions. While the Security of Information Systems has seen lower numbers due to concerns over its rigorous mathematical foundation, the Cybersecurity track is increasingly favored for its direct practical application and excellent career prospects. By merging these paths, we aim to demystify the technical requirements and provide a more balanced, career-oriented educational journey that meets the demands of the modern job market.

To further strengthen our offering, we are working on introducing specialized subjects focused on the two pillars of digital protection: Offensive Security and Defensive Security. The first one will focus on the attacker's mindset, teaching students how to proactively identify and exploit vulnerabilities to secure a system. This approach will provide invaluable hands-on experience in ethical hacking, ensuring graduates can anticipate and mitigate threats before they are exploited by malicious actors. The Defensive Security will be devoted on the architecture of protection, covering monitoring, incident response, and the implementation of robust security controls. It will equip students with the essential skills to design resilient infrastructures and maintain the integrity of organizational data against sophisticated cyberattacks.

7. Research Excellence: Post-Quantum Cryptography and NATO projects

Higher education plays a crucial role in preparing the experts needed for national defence. Genuine expertise is acquired not only through coursework but also through participation in university research. In this section we overview our research related to national security and defense.

The security research at our institution was initially devoted mainly to mathematical cryptography and cryptanalysis. The approaching era of practically viable quantum computers poses a critical threat to current asymmetric cryptographic standards. We recognised early on that research into new cryptographic primitives resistant to quantum attacks was required (so called Post-Quantum Cryptography, PQC). Our PQC research is closely intertwined with our educational activities [4].

Our research activities in this area have received strategic and financial support from the prestigious grant schemes of the North Atlantic Treaty Organization (NATO), specifically three grants within the Science for Peace and Security

program: Secure Implementation of Post-Quantum Cryptography (NATO SfP 984520), Secure Communication in the Quantum Era (NATO SPS Project G5448), and Secure Communication via Classical and Quantum Technologies (NATO SPS Project G5985). Participation in these international consortia not only pushes the boundaries of our fundamental research but also directly contributes to building the resilience of alliance networks [5].

The new Cybersecurity specialisation has also opened up research opportunities in intelligent-malware and threat analysis, currently focusing on explainable AI. Rapid advances in artificial intelligence, particularly in large language models (LLMs), are opening up further opportunities for research and for collaboration between AI and cybersecurity teams.

Finally, our research tries to address various practical defence needs within the Slovak Republic. In cooperation with the Institute of Nuclear and Physical Engineering, we are working on AI-based detection of suspicious objects in X-ray scanner imagery, with applications at airports, government buildings, and other critical-infrastructure sites.

8. Student Involvement and Connection to Real-World Deployment

As a research university, we focus on integrating research with education. Many bachelor and diploma theses are based on the research problems we are currently working on. Furthermore, we use Team projects to promote research participation in smaller student groups. Students were highly successful in our NATO projects, as well as our cybersecurity research. Theses and projects allow students to work on real and significant research tasks, participate in project workshops and gain valuable international experience. As an example, one master's thesis supervised in our department [6] focused on implementing and experimenting with a quantum-secure group authenticated key establishment protocol. This protocol was subsequently incorporated into a chat application [7] that served as a proof-of-concept for NATO SPS Project G5448 in which our department participated. The student also presented his findings at two project-related workshops, giving him valuable opportunities to refine his presentation skills and build connections within the research community.

The pinnacle of practical preparation and the integration of students into the real cyber defense ecosystem is their participation in the international Locked Shields exercise organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) [8]. This is the world's most complex cyber defense exercise, allowing our students to become integral members of national "Blue Teams". Under immense time pressure and facing real (simulated) cyberattacks, students train in the protection of military and civilian IT systems and critical infrastructure. This experience bridges academic education and operational practice. While in previous years only 1–3 students participated in the Locked Shields exercises, the introduction of the cybersecurity specialization significantly increased student interest and involvement, with participation rising to as many as 19 students.

We also reach out to younger generations of students — secondary-school pupils. As part of the TACTICON project [9], supported by the Ministry of Defense of the Slovak Republic, more than 100 secondary-school students developed physical fitness and strategic thinking, while connecting these activities to technology and esports. They also broadened their knowledge through lectures on cybersecurity and artificial intelligence.

There is currently a significant shortage of cybersecurity experts. In response, the Government of the Slovak Republic has established cybersecurity competence centres in cooperation with universities. One of the established centres is Cybersecurity Competence Centre (CCC) at the Slovak University of Technology in Bratislava. The task of the centre is to educate experts in the field of cybersecurity for state and public administration and also to raise awareness of cybersecurity in society as a whole. Our graduate students can also join training activities of the centre as instructors, expanding their soft skills and building social connections. The existence of the CCC brought us the excellent cybersec platforms, developed by Binary Confidence. They represent the pinnacle of modern cybersecurity training environments, often referred to as a high-fidelity "cyber range". The platform serves as a sophisticated cyber range designed to simulate complex, real-world digital infrastructures where participants can face authentic cyber threats in a safe, controlled environment. By integrating advanced gamification elements with rigorous technical scenarios, the platform transforms traditional learning into an immersive experience that demands both tactical precision and strategic agility. It is an indispensable tool for stress-testing incident response teams, conducting talent-scouting competitions, and providing hands-on validation of a professional's ability to defend critical assets under pressure. Having access to such a home-grown, world-class platform is a significant strategic advantage; it bridges the gap between academic theory and the chaotic reality of the cyber frontline, fostering a community of elite security experts who are 'battle-tested' before the first real attack even occurs. The excellence of the cyber range lies in its ability to adapt to the evolving threat landscape, ensuring that the training remains relevant, challenging, and directly applicable to current industry needs.

9. Conclusions

Over the past two decades, the focus at FEI STU has expanded from the theoretical foundations of cryptology to a broad educational and research portfolio with international reach, including three NATO Science for Peace and Security grants and regular participation in the Locked Shields exercise. The growth of student interest in information-security specialisations — from approximately 15% of bachelor's students in 2022 to 43% in 2026 — suggests that the restructuring carried out in 2024 was well-timed. Together with the newly established Cybersecurity Competence Centre and ongoing cooperation with public-sector and industry partners, these developments position the Faculty to make a sustained contribution to building cyber resilience in Slovakia and across the alliance.

Acknowledgements. This research was supported in part by the NATO Science for Peace and Security Programme under Project G5985, and in part by the Slovak Scientific Grant Agency (Vedecká Grantová Agentúra MŠVVaŠ SR a SAV,Slovakia), Grant Number VEGA 1/0105/23.

References

1. Grošek O, Porubský Š. Šifrovanie – algoritmy, metódy, prax. Praha: Grada; 1992.
2. Giannopoulos G, Smith H, Theocharidou M. The landscape of Hybrid Threats: A conceptual model. Luxembourg: Publications Office of the European Union; 2021. doi:10.2760/44985.
3. Moschetta G, Winslow E, Buys W, Hayat K. Global Cybersecurity Outlook 2026, Insight Report. Geneva: World Economic Forum; 2026 Jan.
4. Fabšič T, Grošek O, Hromada V, Zajac P. Post-Quantum Cryptography Migration: Challenges in Education. In: Toward a Quantum-Safe Communication Infrastructure. Amsterdam: IOS Press; 2024. p. 13–23.
5. Colombo C, Vasco MIG, Steinwandt R, Zajac P. Secure communication in the quantum era: (group) key establishment. In: Advanced Technologies for Security Applications: Proceedings of the NATO Science for Peace and Security 'Cluster Workshop on Advanced Technologies', 17-18 September 2019, Leuven, Belgium. Dordrecht: Springer Netherlands; 2020 Jun. p. 65–74.
6. Malo P. Implementation of future-quantum group key establishment protocol [master's thesis]. Bratislava: Slovak University of Technology in Bratislava; 2020.
7. Abela R, Colombo C, Malo P, Sýs P, Fabšič T, Gallo O, et al. Secure implementation of a quantum-future GAKE protocol. In: Roman R, Zhou J, editors. Security and Trust Management. STM 2021. Lecture Notes in Computer Science, vol. 13075. Cham: Springer; 2021. p. 103–21. doi:10.1007/978-3-030-91859-0_6
8. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Locked Shields [Internet]. Tallinn: CCDCOE; [date unknown] [cited 2026 Apr 10]. Available from: https://ccdcoe.org/locked-shields/
9. Jeleň M. [TACTICON - bezpečnoť, stratégia, šport a ešport v praxi] [Internet]. LinkedIn. [2026 Jan] [cited 2026 Apr 10]. Available from: https://www.linkedin.com/posts/michal-jele%C5%88-phd-38aa38144_tacticon-esports-healthyesports-ugcPost-7423840049957437440-5OQS