Enhancing cyber security education in Romania: integrating cyber diplomacy concepts into universities curricula

Adrian-Victor VEVERA[1], Carmen-Elena CÎRNU[1], Ioana-Cristina VASILOIU[1, 2]

[1] National Institute for Research & Development in Informatics – ICI Bucharest,
8-10 Maresal Averescu Avenue, 1st District, Bucharest, Romania

[2] Bucharest University of Economic Studies,
6 Piata Romana, 1st District, Bucharest, Romania

victor.vevera@ici.ro, carmen.cirnu@ici.ro, ioana.vasiloiu@csie.ase.ro

Abstract: *In the digital age, cyber security is a critical field where an ever-evolving skill set is needed to combat increasingly sophisticated cyber threats. This article explores cybersecurity professionals' essential qualifications and skills, highlighting the need for comprehensive educational programs. With a focus on Romanian universities, the paper examines cybersecurity education's current state and identifies areas for improvement. A proposal to integrate cyber diplomacy concepts into cyber security curricula is introduced. Cyber diplomacy sits at the intersection of cybersecurity and international relations, significantly contributing to addressing cross-border cyber threats and fostering global cooperation. By integrating these concepts into university programs, institutions can better prepare students and increase the level of cybersecurity education in Romania. Analysing existing programs in detail, the article provides recommendations for teachers and decision-makers while responding to the need for a competent technical, non-technical and interdisciplinary workforce.*

Keywords: cybersecurity, cyber diplomacy, international relations, universities.

1. Introduction

The fast evolution of digital technology has transformed societies globally, making cybersecurity a critical aspect of national and international security. Romania, recognized for its robust IT sector and burgeoning digital economy, faces substantial cybersecurity challenges. Despite advances in technical education, there is a growing recognition of the need to incorporate cyber diplomacy into university curricula to prepare students for the complexity of modern cybersecurity threats (Asghar & Luxton-Reilly, 2020).

Cyber diplomacy refers to the use of diplomatic tools to resolve conflicts that may arise in cyberspace (cyber security, cyber terrorism, cyber crime) (Pierini, 2016). As cyber-attacks increasingly cross national borders, there is a need for cyber security professionals who are not only technically proficient but also knowledgeable about geopolitical, legal, and ethical dimensions. Integrating cyber diplomacy concepts into university-level education can equip future professionals with the skills to engage in international negotiations, formulate effective policies, and contribute to global cybersecurity governance.

https://doi.org/10.58503/icvl-v19y202405

In 2022, 27 universities in Romania offered students different programs and courses in cybersecurity (Vasiloiu, 2022). Institutions such as the Academy of Economic Studies, the National Polytechnic University of Science and Technology of Bucharest, the Technical University of Cluj-Napoca, the "Ovidius" University of Constanta and the University of Bucharest offer comprehensive programs that focus on the development of technical skills. However, these programs need a multidisciplinary approach that includes cyber diplomacy. Incorporating courses in international cyber law, cyber conflict and warfare, and diplomatic communication can give students a holistic understanding of this field.

By analyzing successful models from other countries and integrating cyber diplomacy into existing programs, Romanian universities can significantly improve their programs. For example, programs at Stanford University and the Massachusetts Institute of Technology offer a robust framework that combines technical training in cybersecurity with international relations and policymaking. Adopting similar approaches in Romania can prepare students to tackle both technical and strategic challenges.

In this regard, specific improvements are proposed for cyber security curricula by integrating cyber diplomacy concepts. The current state of cybersecurity education in Romania will be explored, gaps in existing programs will be identified, and strategies will be suggested to incorporate these new concepts. By doing so, the new generation of cybersecurity professionals will be properly equipped to meet the challenges of cyberspace.

2. Overview of cyber security programs in Romania

Cybersecurity education is essential in preparing the next generation of professionals to protect and secure the digital world. This subchapter provides a comparative examination of the cyber security curricula offered by several essential universities in Romania. Emphasis is placed on program content, practical training and research components.

The programs reviewed offer a wide range of courses and specializations in cybersecurity, addressing various facets such as cryptography, cybercrime, and machine learning. In the table below is a detailed overview of the key features of each program:

Table 1. Comparative analysis of cyber security programs

University	Program	Key topics	Practice	Research
Bucharest University of Economic Studies (ASE)	Cyber security	ICT security, cyber security, cryptography, security standards and protocols, blockchain, quantum cryptography, artificial intelligence, digital forensics, IoT	High emphasis	Medium emphasis

National University of Science and Technology Politehnica of Bucharest (UPB)	Advanced cyber security	Applied cryptography, securi-ty protocols, critical infrastructure security, mobile device security, cloud and grid computing security, incident management	Medium emphasis	High emphasis
University of Bucharest (UniBuc)	Security and applied logic	Cyber security, advanced cryptography, network security, database security, reverse engineering and vulnerability exploitation	Medium emphasis	High emphasis
Ovidius University of Constanta	Cyber Security and Machine Learning	Database Security, Machine Learning, Data Mining, Cryptography, Web Security, Digital Forensics, Software Security	High emphasis	Medium emphasis
"Dunărea de Jos" University of Galați (UGAL)	Combating cyber crime	International cooperation in the field of cyber crime, criminal psychology, security of computer systems, digital investigation techniques, investigations in Open-Source environments from the Internet	Medium emphasis	Medium emphasis
Technical University of Cluj-Napoca (UTC)	Security of information and computing systems	Source code security issues, reverse engineering and analysis of malicious software, big data systems and computer security, mathematical models for machine learning	High emphasis	High emphasis
Politehnica University of Timișoara (UPT)	Security of information and cyber systems	Modern cryptographic techniques, security of computer networks, security of mobile, web and cloud applications, security of industrial systems	High emphasis	High emphasis
Transilvania University of Brașov (UniTBv)	Cyber security	Cryptography, cyber security, incident management, network security, critical infrastructure security, industrial control system security, ethical hacking, data mining, IT forensics	High emphasis	High emphasis

The course offerings at these universities cover a broad spectrum of subjects, ensuring a comprehensive preparation for students. The curricula are designed to equip students with extensive technical skills, covering areas such as cryptographic techniques, network security, mobile and web application security, and digital forensics. The table below lists some of the specific courses offered and indicates the universities that offer them:

Table 2. Comparative analysis of cybersecurity programs

Course	**ASE**	**UPB**	**UniBuc**	**Ovidius**	**UGAL**	**UTC**	**UPT**	**UniTBv**
Cryptography	✓	✓	✓	✓		✓	✓	✓
Security protocols	✓	✓						
ICT security	✓							
Cyber security	✓							✓
Database security	✓		✓	✓				
Network security	✓		✓			✓	✓	✓
Mobile security	✓	✓				✓	✓	✓
Web security	✓	✓		✓		✓	✓	
Digital forensics	✓			✓	✓	✓	✓	
Regulation of cybercrime					✓			
Research activities	✓	✓	✓	✓	✓	✓	✓	✓
Practice activities	✓	✓	✓	✓	✓	✓	✓	✓

All programs include foundational topics such as cryptography and cybersecurity principles, but each has unique offerings. For example, the Ovidius University of Constanta integrates machine learning, which is less emphasized in other programs, reflecting an interdisciplinary approach.

In terms of practical training, all universities offer high levels, but the Academy of Economic Studies in Bucharest stands out, with 280 hours allocated. This practical focus is essential in preparing students to deal with real-world cyber threats.

Each program offers specialized topics that address specific interests in cybersecurity. For example, the Bucharest Academy of Economic Studies addresses current topics such as blockchain, quantum cryptography, artificial intelligence and the Internet of Things (IoT).

Despite these strengths, there are gaps in existing educational programs. The lack of integration of cyber diplomacy concepts represents a substantial gap. While technical skills are essential, the ability to navigate the geopolitical, legal and ethical dimensions of cybersecurity is increasingly important in the globalized digital environment. "Dunărea de Jos" University in Galati has the only program that focuses on combating cybercrime and international cooperation, preparing students to ensure a safe and stable cyberspace.

The cybersecurity programs of the universities selected for analysis offer a diverse curriculum, focusing on various aspects of the field. Each university has unique strengths in practical training, research and specialist subjects, meeting the different needs of both students and industry. Given that as cyber threats evolve, so too should the curricula designed to combat them. By constantly adapting the curriculum to meet emerging threats and industry demands, these programs can equip graduates with the necessary tools to meet the challenges associated with cybersecurity.

3. Integrating cyber diplomacy concepts into the curricula of cyber security programs in Romania

In the age of digital transformation, cybersecurity is a critical area that supports the stability and security of global networks. However, the scope of cyber security extends beyond technical measures to include strategic, legal and diplomatic dimensions. Integrating cyber diplomacy concepts into cybersecurity programs is critical to preparing a new generation of professionals who can understand the complex landscape of international cyber relations. This subchapter focuses on the motivation for this proposal, highlighting the benefits of a multidisciplinary approach that combines technical expertise with diplomacy.

First, it must be taken into account that cyber threats are inherently global, transcending national borders and affecting international relations. State-sponsored cyber attacks, cyber espionage and transnational cybercrime (ENISA, 2023) are issues that require coordinated international responses. Traditional cybersecurity education, focused primarily on technical skills, often needs to address these threats' geopolitical and strategic implications. By integrating cyber diplomacy into the curriculum, universities can train students with the aptitudes and knowledge to understand and manage the international dimensions of cyber security.

International law and politics play a crucial role in shaping the cybersecurity landscape. States collaborate on issues and situations related to cyber security through the Budapest Convention and other treaties, conventions and agreements on international law applicable to cyber warfare (Vasiloiu, 2023). Integrating international cybersecurity law and policy courses would help students become familiar with the legal aspects of their field.

Universities can improve students' strategic and diplomatic skills by incorporating cyber diplomacy concepts into the curriculum. Courses in diplomatic communication, negotiation techniques, and conflict resolution provide students with practical tools to engage in international cyber policymaking and collaboration.

Effective cyber security requires international cooperation and collaboration (Kosseff, 2018). Cyber diplomacy plays an important role in building alliances, fostering trust and developing cooperative frameworks to combat cyber threats. By teaching students about the mechanisms of international cooperation, such as multilateral agreements and public-private partnerships, universities not only equip them for the field but also position themselves as key contributors to global cybersecurity efforts, thereby enhancing their reputation and influence.

4. Case studies on introducing cyber diplomacy concepts into cyber security program curricula

Examining case studies from other countries and institutions provides valuable insights into the benefits of integrating cyber diplomacy into cybersecurity programs. Leading universities such as Stanford University and the Massachusetts Institute of Technology (MIT) have developed courses combining cybersecurity training with international relations and policymaking.

4.1 Stanford University: Foundations of Policy and Cybersecurity

Stanford University's course, Foundations of Policy and Cybersecurity, is designed to provide students with an overview of the intersection of cybersecurity and international politics. This course covers the strategic, legal and ethical dimensions of cyber security, emphasizing the role of policy-making in addressing cyber threats.

Students taking this course will understand the strategic importance of cyber security in international relations, be able to analyze and apply international cyber laws and policies, develop communication and diplomatic negotiation skills related to cyber policy, and gain insight into the ethical challenges (Stanford University, 2024).

The course was instrumental in preparing students for roles in international organizations, government agencies and private sector firms where cybersecurity and policymaking intersect. By integrating cyber diplomacy concepts, the course provides students with a balanced skill set that includes technical competence and strategic insight.

4.2 Massachusetts Institute of Technology: Cyberpolitics in International Relations

The MIT course, "Cyber Policies in International Relations," examines the role of cyber capabilities in shaping international relations. It combines theoretical frameworks from international relations with practical insights into cyber policy and strategy.

Students taking this course will gain a deep understanding of the intersection of cyber capabilities and international relations, develop capabilities to develop and critique national and international cyber policies, understand the role of international law in governing state behaviour in cyberspace, and be able to develop strategies to address cyber conflicts and improve global cyber security (MIT, 2024).

The MIT course has successfully prepared students for careers in cybersecurity, policymaking, and international relations. Integrating cyber policy into the curriculum provides a comprehensive understanding of cyber security's strategic, legal and ethical dimensions, equipping graduates to identify solutions to global cyber threats.

4.3 Benchmarking and best practices

Both Stanford and MIT emphasize the importance of understanding international cyber law and policy. These courses cover key treaties and conventions, such as the Budapest Convention and the Tallinn Manual, giving students a solid grounding in international legal frameworks.

Both institutions address the strategic aspects of conflict and cyber warfare. By analyzing state-sponsored cyber attacks, students gain insight into the role of cyber capabilities in national security. This knowledge is crucial for developing effective defence strategies and engaging in international diplomacy.

Integrating ethical and human rights issues into the curriculum ensures that students know the broader implications of cyber security measures. Both Stanford and MIT include courses on the moral challenges of surveillance, data protection, and the balance between security and privacy.

The case studies reviewed demonstrate the effectiveness of integrating cyber diplomacy concepts into cyber security programs. Combining technical training with strategic, legal and ethical perspectives, these programs prepare students to address the multifaceted challenges of global cyber security. Romanian universities can build on these examples to improve their cyber security programs, ensuring that graduates are well-equipped to contribute to international cyber security and stability.

5. Curriculum proposal for Romanian universities

Given the escalating intricacy of cyber threats and the pressing need for a comprehensive grasp of cyber security, it is imperative that Romanian universities incorporate cyber diplomacy concepts into their cyber security programs. This subchapter introduces a meticulously crafted curriculum proposal that addresses this crucial need.

The proposed curriculum is structured into basic courses, optional courses, practical training and research components. The curriculum spans two years (four semesters) and is designed to provide a balanced mix of theoretical knowledge, practical skills and strategic insights. This proposition combines technical training with strategic, legal and ethical perspectives, ensuring a holistic preparation for future cybersecurity professionals.

Table 3. Curriculum proposal to integrate cyber diplomacy concepts

Year	Course	Description
Year 1 - Semester 1	Introduction to Cyber Security	Overview of the principles, threats and defence mechanisms in cyber security. Hands-on labs on basic cybersecurity tools and techniques.
Year 1 - Semester 1	Network Security	Fundamentals of network security, including protocols, firewalls and intrusion detection systems. Hands-on labs on securing network infrastructures.
Year 1 - Semester 1	Applied Cryptography	Principles of cryptography, encryption algorithms and cryptographic protocols. Practical exercises on the implementation of cryptographic solutions.
Year 1 - Semester 1	Ethics and Human Rights in Cyber Security	Exploration of ethical issues and human rights implications in cyber security. Case studies on the balance between security, privacy and civil liberties.
Year 1 - Semester 1	Scientific Research Methods	Introduction to research methodologies and academic writing. Preparation for research projects and dissertation work.
Year 1 - Semester 2	CyberSecurity Policies and Governance	Overview of national and international policies and governance frameworks in cyber security. Analysis of policy-making processes and regulatory environments.
Year 1 - Semester 2	Cyber Conflict and Warfare	Study of cyber warfare and state-sponsored cyber attacks. Case studies of significant cyber conflicts and their implications.
Year 1 - Semester 2	International Cyber Law	Examination of international treaties, conventions and legal frameworks governing cyberspace. Case studies on the application of international cyber law.
Year 1 - Semester 2	Digital Forensics and Incident Response	Digital forensics techniques and cyber security incident management. Practical laboratories.
Year 1 - Semester 2	Research Project I	The initial phase of a research project focused on a specific cyber security issue.
Year 2 - Semester 1	Cyber Diplomacy and International Relations	The role of cyber diplomacy in managing and mitigating cyber threats. Strategies for international cooperation and development of cyber norms.

Year 2 - Semester 1	Network Security	Network security, zero-trust architectures and secure network design. Hands-on labs on advanced configurations.
Year 2 - Semester 1	Cyber Threat Intelligence	Techniques for collecting, analyzing and using cyber threat intelligence. Practical exercises on intelligence tools and methodologies.
Year 2 - Semester 1	Practical Training and Internship	Practical experience through internships with industry partners, government agencies or international organizations. Application of theoretical knowledge in real situations.
Year 2 - Semester 1	Research Project II	The research project will continue, focusing on data collection, analysis, and preliminary conclusions.
Year 2 - Semester 2	Strategy and Risk Management	Development of cyber security strategies and risk management frameworks. Hands-on labs on cybersecurity risk assessment and mitigation.
Year 2 - Semester 2	Emerging Technologies	The study of emerging technologies (quantum, AI, blockchain, IoT) and their impact on cyber security. Challenges and solutions.
Year 2 - Semester 2	Multilateral Cyber Agreements	Examination of multilateral agreements and their role in global cyber security. Case studies of successful international collaborations in cyber security.
Year 2 - Semester 2	CyberSecurity Leadership and Management	Developing leadership and management skills for cyber security professionals. Hands-on exercises on leading cybersecurity teams and projects.
Year 2 - Semester 2	Dissertation	The final phase of the research project. Presentation of research conclusions.

By including courses such as "Cyber Diplomacy and International Relations," "International Cyber Law," and "Ethics and Human Rights in Cyber Security," students will gain an in-depth knowledge of the legal and ethical implications of cyber security. Thus, they will approach global challenges from an informed and balanced perspective.

Moreover, the Cyber Security Leadership and Management course will equip students with the essential management skills to coordinate cyber security teams and projects, effectively manage emerging crises and develop security strategies for cybernetics.

The inclusion of hands-on courses in "Digital Forensics and Incident Response" and "Cyber Threat Intelligence" provides the necessary skills to effectively detect, analyze and respond to cyber security incidents. Practical laboratories will ensure the application of theoretical knowledge in real scenarios.

The study of multilateral cyber agreements and international cooperation mechanisms in cyber security will exemplify how collaboration helps combat cyber threats and develop a stable and secure cyber environment.

The "Emerging Technologies" course prepares students to address the latest technologies, such as quantum computing, artificial intelligence, and blockchain, as well as challenges and opportunities. This knowledge is necessary to remain competitive in an ever-evolving field.

Introducing cyber diplomacy concepts into the curriculum of cyber security programs of Romanian universities can greatly impact the quality of the education offered. This interdisciplinary approach, coupled with practical training, will equip graduates to handle both technical and strategic aspects. As a result, they will be better prepared to contribute to national and global cyber security, fostering stability and safety in the digital environment.

5. Conclusions

As cyber threats become increasingly complex and globalized, cyber security education must evolve to include technical skills and strategic, legal and diplomatic perspectives. Integrating cyber diplomacy concepts into Romanian university curricula represents a significant step toward training a new generation of professionals capable of managing the multidimensional challenges of cyber security.

By including courses related to cyber diplomacy, students gain a deep understanding of cyber security's global and legal implications. This enables them to approach challenges from an informed and balanced perspective, preparing them for complex roles in central public administration, international organizations and the private sector.

There are several study programs that could use the integration of these concepts, such as international relations programs, computer science programs, cybersecurity and information security programs or law programs. Adding this layer to an international relations program would equip future diplomats to understand cyber threats and negotiate international treaties regarding cybersecurity. Understanding the geopolitical and societal aspects of their work for the technical programs would minimize the gap between technical expertise and strategic implications. Moreover, regarding law programs, cyber diplomacy concepts are important in terms of cybercrime or data governance, and understanding them better would benefit global regulations.

Incorporating cyber diplomacy concepts into cyber security education in Romanian universities can profoundly impact the quality of education and professional training. Graduates of these programs will be well prepared, combining technical skills with strategic and diplomatic understanding. Romanian universities can significantly contribute to national and international cyber stability and security through this improved curriculum, training tomorrow's leaders who will protect and support a safe and resilient digital environment.

REFERENCES

Asghar, M. R. & Luxton-Reilly, A. (2020) A case study of a cybersecurity programme: curriculum design, resource management, and reflections. In: *Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*. New York, NY: Association for Computing Machinery. pp. 16–22. https://doi.org/10.1145/3328778.3366918.

Bucharest University of Economic Studies. (2022) *Cybersecurity curricula 2022-2024*. https://ism.ase.ro/curricula/cybersecurity-curricula-2022-2024/ [Accessed 30 Sept. 2024].

Kosseff, J. (2018) Developing collaborative and cohesive cybersecurity legal principles. In: *2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia*. pp. 283-298. https://doi.org/10.23919/CYCON.2018.8405022.

MIT. (2011) *Cyberpolitics in international relations: theory, methods, policy*. https://ocw.mit.edu/courses/17-447-cyberpolitics-in-international-relations-theory-methods-policy-fall-2011/pages/syllabus/ [Accessed 30 Sept. 2024].

Pierini, G. (2016) *Cyber security meets diplomacy: the EU-NATO cooperation and the Italian case*. https://tesi.luiss.it/20167/1/627242_PIERINI_GABRIELE.pdf [Accessed 30 Sept. 2024].

Stanford University (2024) *Fundamentals of cyber policy and security*. https://explorecourses.stanford.edu/search?view=catalog&filter-coursestatus-Active=on&page=0&catalog=&q=INTLPOL+321%3A+Fundamentals+of+cyber+policy+and+security&collapse= [Accessed 30 Sept. 2024].

University of Bucharest (2020) *SLA English presentation*. https://sal.cs.unibuc.ro/wp-content/uploads/2020/04/SLA-Engleza-Prezentare.pdf [Accessed 30 Sept. 2024].

„Dunărea de Jos” University of Galați (2022) *Combaterea criminalității informatice: study plan*. https://www.fdsa.ugal.ro/images/2022/plan_invatamant/Pl_Inv_12_FDSA_2021_M_Combaterea_criminalitatii_informatice.pdf [Accessed 30 Sept. 2024].

„Ovidius” University of Constanța (2023) *Master's curriculum*. https://fmi.univ-ovidius.ro/wp-content/uploads/2023/09/planuri-invatamant/csml1.pdf [Accessed 30 Sept. 2024].

Politehnica University of Bucharest (2024) *Advanced cybersecurity: curriculum*. https://doubledegree.ro/assets/curriculum/master/Advanced_Cybersecurity_en.pdf [Accessed 30 Sept. 2024].

Politehnica University of Timișoara (2024) *Cyber systems and information security: curriculum.* https://ac.upt.ro/specializari/securitatea-informatiilor-si-a-sistemelor-cibernetice-planul-de-invatamant/ [Accessed 30 Sept. 2024].

Technical University of Cluj-Napoca (2021) *Cyber systems security: master's curriculum.* https://cs.utcluj.ro/files/educatie/masterat/2020-2021/M_SISC_20-21.pdf [Accessed 30 Sept. 2024].

Transilvania University of Brașov (2024) *Cyber security master's programme in English.* https://www.unitbv.ro/267-programe-de-studii/programe-de-studii-masterat/2719-cyber-security-in-limba-engleza.html [Accessed 30 Sept. 2024].

University of East London (2024) *MSc Cyber Diplomacy*. https://uel.ac.uk/postgraduate/courses/msc-cyber-diplomacy [Accessed 30 Sept. 2024].

Vasiloiu, I. C. (2022) Cybersecurity education in Romania - competitive advantage in the EU market. In: *International Conference on Virtual Learning, vol. 17.* pp. 297-307.

Vasiloiu, I. C. (2023) Cyber diplomacy: a new frontier for global cooperation in the digital age. *Informatica Economica*. 27(1), 41-50.