Empowering National Cybersecurity: The CYRESRANGE Project

Andreea DINU, Carmen-Elena CÎRNU
National Institute for Research and Development in Informatics - ICI Bucharest
andreea.dinu@ici.ro, carmen.cirnu@ici.ro

Abstract: In an era characterized by rapid technological advancement, the field of cybersecurity emerges as a cornerstone for any nation aspiring to fortify its defenses against an array of potential cyber threats. Over the past decade, the proliferation of cyber attacks has highlighted the necessity that experts consolidate their knowledge and resources, by crafting robust tools and methodologies to safeguard national security within the cyber domain. Moreover, community engagement is of paramount significance in this context, with collaborative efforts serving as a linchpin for effective action in cyber defense. This paper aims to present a national initiative designed to bolster the arsenal of defense against external cyber threats, while concurrently raising awareness of these threats and expertise in this field through the utilization of national cyber range resources.
Keywords: cybersecurity, collaboration, national initiative, cyber range, awareness, training.

INTRODUCTION

In the advent of the digital era, the European Union (EU) has recognized the critical importance of cybersecurity in safeguarding the continent's digital infrastructure, citizenry, and vital sectors. As technologies are evolving and integrating deeply into key areas such as the military, commerce, and administration, the sophistication of cyber threats has also advanced, necessitating robust defensive mechanisms. The EU's digital strategy emphasizes a multi-faceted approach to cybersecurity, aiming not only to protect but also to foster resilience, cooperation, innovation, and leadership on a global scale. This strategy is encapsulated in initiatives and directives like the NIS Directive, the Cybersecurity Act, and the GDPR, which collectively aim to elevate cybersecurity standards across member states (European Commission, 2024).

Acknowledging the interconnected nature of digital threats, the EU has underscored the need

https://doi.org/10.54851/v6i1y202408

for collaboration among member states and between national actors as pivotal for fortifying the European cybersecurity landscape. Romania stands as a testament to these efforts, having embarked on a comprehensive strategy to enhance its national cybersecurity framework. Through strategic planning, educational initiatives, and the establishment of public-private partnerships, Romania aims to not only defend itself against cyber threats but also to build a resilient and skilled cybersecurity community.

INITIATIVES AT NATIONAL AND EUROPEAN LEVEL

At national level, Romania's Cybersecurity Strategy for 2022-2027 outlines a proactive stance against cyber threats, focusing on securing digital networks, fostering a high-performance digital ecosystem, and enhancing regulatory frameworks to match the pace of technological advancements. A cornerstone of this strategy is the emphasis on public awareness, education, and professional training, which are meant to cultivate a culture of cybersecurity awareness and expertise (Guvernul Romaniei, 2021). The pragmatic approach towards public-private partnerships in Romania reflects a strategic move to leverage collective expertise and resources in developing robust cybersecurity defenses. Educational programs, professional training, and innovation in the cybersecurity domain are envisioned to yield significant economic and social benefits, underscoring the critical role of collaborative efforts in enhancing national cybersecurity capabilities (Gorgan, 2023). The Bucharest Cybersecurity Conference of 2023 exemplifies Romania's commitment to advancing cybersecurity knowledge and fostering collaboration in this field. This platform gathered industry experts, policymakers, and professionals to tackle the nuances of cybersecurity policy, regulatory challenges, and sector-specific threats, facilitating a comprehensive exchange of knowledge and best practices (National Cyber Security Directorate - DNSC, 2023).

Another noteworthy national initiative is the CYSCOE - Cyber Security Cluster of Excellence, which aims to enhance national and international collaboration and to elevate cybersecurity education throughout Romania. In addition to contributing to Romania's operational and technical capacity, CYSCOE is actively developing educational initiatives and organizing cybersecurity events. These efforts position Romania as a hub of cybersecurity competitiveness on European and global scales.

The Cluj IT Cluster has launched an innovative and ambitious initiative to align and strengthen key players in the cybersecurity sector within the Northwest Region of Romania. This effort is part of the broader objectives of Digital Innovation Center for Society - eDIH4Society. Through this center, Cluj IT Cluster and its partners aim to accelerate digitalization and digital transformation across the region. This regional hub first aims to facilitate an open dialogue about future collaboration among present stakeholders and potentially other necessary actors, setting the stage for creating a specialized hub of excellence in the increasingly vital cybersecurity sector (Cluj IT Cluster, 2024).

The National Cyber Security Training Centre of Excellence (CSTCE) in Romania focuses on professional training in cybersecurity, aiming to guide participants toward careers in the industry. This center offers a variety of courses with levels ranging from introductory to advanced, covering topics such as ethical hacking, secure coding, and cyber intelligence. These courses aim to develop skills and provide recognized certifications that open new opportunities in the cybersecurity field. CSTCE's mission includes addressing the challenges faced by learners in state institutions and fostering a new generation of cybersecurity experts (National Cyber Security Training Centre of Excellence, 2023).

The Romanian Association for Information Security Assurance (ARASEC) is a non-profit, non-partisan organization focused on promoting information security. Established in 2012, ARASEC works to foster a community for sharing knowledge among specialists from institutional,

private, and academic environments. The association conducts conferences, seminars, and workshops, collaborates on national and international projects, and provides training to enhance information management skills. Additionally, ARASEC combats cybercrime and disseminates information on new vulnerabilities and threats, thereby significantly contributing to the national security landscape in Romania (ARASEC, n.d.).

CyberEDU is a dynamic platform designed to bridge the gap between theoretical knowledge and practical skills in cybersecurity. It offers a comprehensive range of hands-on training exercises inspired by real-world scenarios, tailored to individuals, companies, and universities. The platform focuses on boosting cybersecurity competencies globally through cyber-range-as-a-service technology, which includes immersive learning environments and competitions. CyberEDU aims to significantly enhance the practical cybersecurity skills of its users, promoting continual improvement and industry readiness (CyberEDU, n.d.).

The Romanian National Cyber Security Challenge is organized by the Romanian Intelligence Service, along with the National Cyberint Center, National Cyber Security Directorate (DNSC), and the National Association for Information Systems Security (ANSSI), with support from the private sector. The competition has an online stage and a final in-person stage, culminating in the selection of a broader group for Team Romania. The top ten participants and two alternates are chosen to represent Romania at the European Cybersecurity Championship. They prepare on the CyberEDU platform, which features exercises from previous national and international competitions (ROCSC, 2024).

The Romanian Intelligence Service operates the National Cyberint Center as its authority on cyber intelligence, designated by the Supreme Council of National Defence (CSAT). The center's main role is to address, prevent, and counter cyber threats, vulnerabilities, and risks to Romania's cybersecurity. It collaborates technically and informatively to safeguard critical IT and communication infrastructures and combats cyber threats from various hostile entities, including state and non-state actors, criminals, and terrorists. The center also plays a crucial role in raising public security awareness and has operated as the CERT for the Romanian Intelligence Service since July 2020 (Romanian Intelligence Service, n.d.).

These concerted efforts by Romania, aligned with the EU's broader cybersecurity objectives, underscore a proactive and collaborative approach to addressing the challenges posed by cyber threats. The development of a national cybersecurity community, geared towards readiness and responsiveness to cyber incidents, reflects the collective resolve to safeguard the digital frontier.

At the European level, cybersecurity initiatives are integral to safeguarding digital infrastructures and enhancing the resilience of information systems across member states. These efforts are coordinated through various frameworks and projects aimed at aligning cybersecurity strategies and practices.

The European Union's cybersecurity strategy revolves around strengthening cyber resilience, deterring cybercrime, and developing a cohesive cybersecurity policy framework across member states. This strategy focuses on protecting critical infrastructure, boosting the security of network and information systems, and enhancing the capabilities of cybersecurity professionals. It also emphasizes cross-border cooperation to tackle cyber threats effectively and ensure a safe digital market for all EU citizens (European Commission, n.d.).

CyberSec4Europe is a research initiative aimed at developing a European Cybersecurity Competence Network by designing, testing, and validating governance structures based on best practices and extensive partner expertise. The project focuses on harmonizing cybersecurity measures across various sectors including digital infrastructure, finance, government, healthcare, and transportation, by developing software solutions, guidelines, and recommendations. It seeks to strengthen the EU's cybersecurity capacity to ensure a secure digital economy and maintain democratic values (CyberSec4Europe, n.d.).

The European Cyber Security Organisation (ECSO), established in 2016, serves as Europe's main cross-sectoral and independent membership organization in cybersecurity, partnering with the European Commission. It includes a diverse membership base from public and private sectors, such as large companies, SMEs, research centers, and universities across the EU and EFTA. ECSO focuses on strengthening Europe's digital sovereignty and cyber resilience through community empowerment, collaboration platforms, and public-private dialogues (ECSO - European Cyber Security Organisation, n.d.).

The CyberSecPro project aims to enhance the role of Higher Education Institutions (HEIs) in Europe by preparing a new generation workforce equipped with practical, marketable cybersecurity skills. The project involves 15 HEIs and 13 companies from 16 countries working together to create a collaborative and multi-modal training program. This program is designed to bridge the gap between academic degrees and working life, focusing on hands-on skills necessary for driving a secure and trustworthy digital transformation in critical economic sectors (CyberSecPro, n.d.).

The EU is actively enhancing cybersecurity through various funding programs, notably through Horizon Europe, Digital Europe, and the Connected Europe Facility. These programs support research, technological development, and the deployment of cybersecurity measures. Additionally, the establishment of the European Cybersecurity Competence Centre and a network of national coordination centers focuses on pooling resources and expertise across the EU. ENISA (European Union Agency for Cybersecurity) plays a critical role in advising and setting strategic priorities for these efforts, aiming to achieve a high level of cybersecurity across the Union (ENISA, n.d.).

The EU's strategic efforts in cybersecurity highlight a unified and proactive approach to combat cyber threats, mirroring the commitment seen in Romania's initiatives. By fostering cooperation among member states, establishing robust networks of expertise, and funding targeted research and development projects, the EU is building a resilient cybersecurity ecosystem. These measures are crucial for enhancing the collective ability to predict, respond to, and mitigate cyber incidents, thus protecting the digital integrity of Europe's interconnected societies. Each cybersecurity initiative across Europe contributes to strengthening the continent's defenses against cyber threats. From educational programs that train the next generation of cybersecurity professionals, to research projects that develop cutting-edge security technologies, and collaborative networks that enhance information sharing and best practices, each effort plays a crucial role. Together, these initiatives strengthen the collective cybersecurity posture, making Europe more resilient against increasingly sophisticated cyber attacks, thereby securing digital infrastructures and safeguarding the digital economy.

THE CYRESRANGE PROJECT

The enhancement of cybersecurity capabilities within the European Union (EU) member states can be significantly advanced through the strategic interconnection of robust cybersecurity infrastructure and the development of immersive, hands-on security exercises. These exercises are designed to closely mimic real-world scenarios, thereby providing cybersecurity professionals with the practical experience necessary to effectively respond to and mitigate cyber threats. By simulating realistic cyber-attack scenarios, these exercises facilitate a comprehensive learning environment that supports the development of critical response strategies and preventive measures. The incorporation of such practical exercises necessitates a collaborative approach, encompassing both technical and operational cooperation among participants. This collaborative framework is instrumental in fostering an environment conducive to the exchange of expertise and to a constructive discussion of varying perspectives on cybersecurity challenges. Furthermore,

the concept of cyber ranges plays a pivotal role in this strategy. Cyber ranges are specially configured infrastructures that enable the execution of a wide array of cybersecurity exercises, encompassing various scenarios across different domains. These ranges are tailored to simulate an array of real-life cyber situations, thereby providing an ideal setting for reinforcing the cybersecurity capabilities of participants. Through the provision of customized cybersecurity exercises, cyber ranges offer a unique opportunity to enhance the practical skills of cybersecurity professionals, equipping them with the knowledge and competencies required to navigate the complexities of the cyber landscape effectively (Sharkov et al., 2022).

In September 2023, the Cyber Ranges Resiliency Networks – CYRESRANGE was launched, with the aim of strengthening the national cybersecurity capabilities. The project is funded through the EU Digital Europe Program, under the call DIGITAL-ECCC-2022-CYBER-03, action type: DIGITAL JU SME Support Actions and it is coordinated by Constanta Maritime University with the assistance of partners including the National Institute for Research and Development in Informatics – ICI Bucharest, Bit Sentinel SRL, Orange Romania SA, Cyber Dacians SRL, Cyber Security Excellence Cluster Association, CYSCOE.

Figure 1. *Logo of CYRESRANGE initiative [own source]*

CYRESRANGE aims to enhance the capabilities of current cyber ranges, with the goal of establishing a network of Cyber Security Centers of Excellence both nationally and regionally. This network will rely on interconnected cyber ranges, emphasizing the enhancement of scenario developers' experiences and incorporating an extensive gamified experience for learners. The project strives to lay the foundation for a community of content creators, fostering the emergence of new cybersecurity job roles. Additionally, the goal is to empower professionals to expand their cybersecurity competencies and proficiency in essential technologies while introducing a cost-efficient technology solution for integrating new cyber ranges. The CYRESRANGE main objectives at national level are the creation of various cybersecurity tools and of a collaboration framework:

- A sophisticated cyber range platform designed to swiftly onboard organizations into a dedicated space for practice, facilitating rapid engagement in cyber security exercises.
- A comprehensive wizard tool that empowers professionals to effortlessly design and customize training modules, exams, competitions, recruitment processes, or Tabletop Exercises (TTXs), without the need for technical expertise.
- A personality assessment tool aimed at assisting students and professionals in identifying suitable cyber security career paths based on their personality traits.
- The development of a universal language for large-scale exercises enhances the learning experience through gamification and simulations, offering a variety of training scenarios like TTX, Adversarial, Traffic or User Simulation, and team-based exercises (Red vs Blue, Blue Team, Purple Team, King of the Hill, Capture the Flag). This approach aims to provide an immersive and realistic training environment.
- A shared repository accessible to CYRESRANGE members for exchanging Tactics, Techniques, and Procedures (TTP), threat intelligence, and profiles of adversaries and users.
- The establishment of a Regional Resilience Network that integrates diverse infrastructures and technologies across various regions, supported by a consortium of cyber security professionals trained in uniform methodologies and processes for incident response.

- The creation of a unified API to facilitate the seamless integration with existing cyber ranges or the broader network of federated cyber ranges.
- The introduction of an innovative technology that allows for the sharing of resources among cyber ranges to support extensive network simulations. This technology is geared towards enabling a broad spectrum of adversarial tactics and realistic traffic conditions.
- The formation of strategic partnerships with industry leaders and subject matter experts to ensure access to the latest cyber security tools, technologies, and best practices. These collaborations aim to bolster the resources of the Cyber Security Centers of Excellence and offer advanced training and education opportunities.
- The launch of a marketplace dedicated to training, career development, and scenario crafting, which:
  - Encourages content creators through incentives to develop structured training programs and cyber security exercises.
  - Enables students and professionals to choose from a variety of training options on the marketplace, preparing them to bolster the cyber defenses of both public and private sector organizations.
  - Offers a structured training and certification framework that adheres to national, European, and international standards, such as MITRE, NICE, OWASP etc. This framework aims to elevate the credibility of the national training centers and ensure participants acquire the necessary skills for professional success.
  - Supports the execution of pre-designed exercises and scenarios within individual organizations and through collaboration with other entities.

ICI Bucharest will play a pivotal role in this project, offering multifaceted contributions to its success. Primarily, ICI Bucharest will serve as one of the initial three cyber ranges to be interconnected, facilitating the integration of newly developed applications. This critical infrastructure will not only support the project's technical backbone but also provide a testing ground for its outputs.

In the realm of content development, ICI Bucharest will make a significant contribution by designing scenarios and tests tailored to the implemented applications. These scenarios and tests are essential for validating the applications' efficacy and ensuring they meet the intended cybersecurity objectives.

Furthermore, ICI Bucharest will engage in the dissemination of the project's results, playing a crucial role in sharing insights and advancements with the broader community. This will include active participation in the organization and execution of cybersecurity events and exercises, which are vital for demonstrating the project's outcomes and facilitating hands-on experience with the developed solutions.

The project offers ICI Bucharest an unparalleled opportunity to collaborate closely with national experts, fostering an exchange of best practices. Such interaction is anticipated to significantly enhance the institutional capabilities of ICI Bucharest's cyber range, positioning it as a leader in cybersecurity innovation and collaboration within the national context. Through these diverse contributions, ICI Bucharest aims to bolster the project's objectives and reinforce its standing as a central figure in advancing cybersecurity measures and infrastructure.

ALIGNMENT WITH OTHER IMPORTANT INITIATIVES IN THE FIELD

The CYRESRANGE project is being developed in line with the existing cybersecurity objectives, policies, and strategies at both national and European levels. The project's outcomes, including an enhanced infrastructure readiness, increased interconnectivity, and better-trained cybersecurity staff, will support the objectives outlined in Article 3 of the Digital Europe Programme (European Commission, 2024). These objectives focus on reinforcing the security of digital products and services. Furthermore, the project's achievements are in harmony with the

aims of the European Cybersecurity Competence Centre (ECCC), particularly in terms of bolstering cybersecurity capacities, knowledge, and infrastructure to protect EU economy against cyber threats.

This initiative will establish a central hub for conducting a wide array of complex cybersecurity drills. This aligns with the goal stated in preamble (42) of the Network and Information Security (NIS) Directive (NIS 2 Directive, 2024), which emphasizes the importance of simulating real-time incident scenarios for the preparedness and collaborative security efforts of Member States. The platform will enhance sector-wide readiness and foster information sharing through customized exercises, thereby increasing resilience against Advanced Persistent Threats (APT) in alignment with the EU Cybersecurity Strategy.

Consistent with the NIS 2 Directive and the EU CyCLONe network (ENISA, 2024), the framework designed through this project is suited for executing strategic, operational, and technical cross-sectoral crisis management exercises at both national and European levels. These exercises will test the system and team readiness, contributing to ENISA's mandate of organizing large-scale exercises as mentioned in preamble (47) of the Cybersecurity Act (ENISA, 2019).

Addressing the cybersecurity job shortage identified in the ENISA Report on Cybersecurity Skills Development in the EU in 2019 (ENISA, 2020), which highlighted a deficit of 291,000 positions, the CYRESRANGE project aims to mitigate this gap. By enhancing training and development in line with the evolving demands of cybersecurity, the project will attract and train users, fostering the development of scenarios by cybersecurity enthusiasts. This approach will expedite the training and retention of cybersecurity professionals, aiding the EU's long-term ambition of achieving technological sovereignty. The project introduces the new role of cybersecurity content creator, thereby increasing the platform's appeal to independent cybersecurity enthusiasts interested in scenario development, ultimately supporting the growth and retention of cybersecurity talents over the long term.

In accordance with Article 4 of the Law no. 58 on Romania's cyber security and defense (Romanian Parliament, 2023) passed by the Romanian Parliament, the project's applicability across various industries and scenarios will aid in safeguarding IT networks and systems which are crucial to cyber defense, national security, public order, and governance. It also aims to cultivate a national cybersecurity culture by raising awareness of the related vulnerabilities, risks, and threats, and the promotion of proactive and preventive actions. By aiding technical users and critical infrastructure providers in identifying and responding to cybersecurity vulnerabilities, the project aligns with essential direction of the Romanian Cybersecurity Strategy and of other EU strategies. This strategy aims to ensure security through the understanding, prevention, and elimination of cybersecurity threats. The project has embodied a collaborative effort among the private sector, public sector, and academia from its inception, supporting resilience-building activities.

CONCLUSIONS

Cybersecurity stands as a critical cornerstone for national and European security, underpinning the very essence of modern societal, economic, and governmental functions. As our reliance on digital technologies escalates, so does our vulnerability to cyber threats that seek to exploit the interconnected fabric of our digital existence. The importance of cybersecurity at both the national and European levels cannot be underrated; it is fundamental to safeguarding our digital infrastructures, protecting the privacy of citizens, and ensuring the seamless operation of essential services.

At the national level, cybersecurity is paramount for protecting critical infrastructure, including energy grids, transportation systems, healthcare services, and financial networks. A breach in any of these areas can have far-reaching consequences, from economic damage and disruption of services to threats to national security and public safety. Nations, therefore, prioritize the development of

robust cybersecurity frameworks, policies, and strategies to defend themselves against cyber threats, enhance their digital resilience, and ensure the continuity of critical services.

European Union (EU) initiatives underscore the collective understanding of the fact that cybersecurity is not confined by national borders; cyber threats are inherently transnational. By recognizing this, the EU has adopted a comprehensive approach to cybersecurity, aiming to foster collaboration among member states and enhance the collective cyber defense capabilities.

Moreover, the EU's digital strategy emphasizes the significance of innovation, education, and public-private partnerships in the realm of cybersecurity. By funding cybersecurity projects and supporting the establishment of a network of Cyber Security Centers of Excellence, the EU facilitates the sharing of knowledge, resources, and best practices. This approach is instrumental in addressing the cybersecurity skills gap, enhancing the cybersecurity preparedness of public and private sector entities, and fostering an environment of continuous learning and adaptation to the evolving cyber threat landscape. The CYRESRANGE project represents a significant step forward in the quest for enhanced cybersecurity. By leveraging the power of collaboration, practical training, and innovative technology, the project not only contributes to the immediate strengthening of national and regional cybersecurity capabilities but also lays the groundwork for a sustainable, resilient digital future. As cyber threats continue to evolve in complexity and scale, initiatives like CYRESRANGE are essential for ensuring that Romanian digital defenses remain robust and agile, capable of protecting the critical digital infrastructures that underpin the Romanian society and economy.

ACKNOWLEDGEMENT

The article is supported by the project Cyber Ranges Resiliency Networks – CYRESRANGE, funded through the EU Digital Europe Program, under the call DIGITAL-ECCC-2022-CYBER-03, action type: DIGITAL JU SME Support Actions, grant agreement no. 101128088.

REFERENCE LIST

ARASEC. (n.d.) *Asociația Română Pentru Asigurarea Securității Informației.* https://www.arasec.ro/ [Accessed 7th May 2024].

Bit Sentinel. (n.d.) *Servicii de securitate cibernetică și penetration testing*. https://bit-sentinel.com/ro/ [Accessed 29th April 2024].

CYSCOE - Cyber Security Cluster of Excelence. (n.d.) https://cyscoe.ro/ [Accessed 29th April 2024].

CyberEDU - Next-gen hands-on training for students and cyber security professionals. (n.d.) Cyber-Edu.co. https://cyber-edu.co/, [Accessed 7th May 2024]

CyberSec4Europe. (n.d.) Cyber Security for Europe. https://cybersec4europe.eu [Accessed 7th May 2024].

CyberSecPro. https://www.cybersecpro-project.eu [Accessed 7th May 2024].

Cyber Dacians|Professional Offensive Security and Compliance Services. (n.d.) Cyberdacians.com. https://cyberdacians.com/ [Accessed 29th April 2024].

Cluj IT Cluster. (2024) Cluj IT Cluster a pus bazele primului HUB regional de securitate cibernetică din România., https://www.clujit.ro/cluj-it-cluster-a-pus-bazele-primului-hub-regional-de-securitate-cibernetica-din-romania/ [Accessed 7th May 2024].

ECSO - European Cyber Security Organisation. (n.d.) ECSO - European Cyber Security Organisation. https://ecs-org.eu/ [Accessed 7th May 2024].

European Commission. (2024) *Cybersecurity Policies.* https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies [Accessed 7th May 2024].

European Commission. (2024) *Shaping Europe's Digital Future - The Digital Europe Programme*. https://digital-strategy.ec.europa.eu/en/activities/digital-programme [Accessed 22nd March 2024].

European Commission. (n.d.) Cybersecurity Strategy. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy [Accessed 7th May 2024].

ENISA. (2020) *Cybersecurity Skills Development in the EU*. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union [Accessed 7th May 2024].

ENISA. (2024) *EU CyCLONe*. https://www.enisa.europa.eu/topics/incident-response/cyclone [Accessed 7th May 2024].

ENISA. (n.d.) *EU funding in cybersecurity*. https://www.enisa.europa.eu/topics/research-and-innovation/eu-funding-in-cybersecurity [Accessed 7th May 2024].

ENISA. (2019) REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881,[Accessed 7th May 2024]

Gorgan, O. (2023) *Romania`s cybersecurity strategy - a short introduction.* https://privacyoutloud.ro/2022/07/19/romanias-cybersecurity-strategy-a-short-introduction/ [Accessed 7th May 2024].

Government of Romania. (2021) *Strategie din 30 decembrie 2021 de securitate cibernetică a României, pentru perioada 2022-2027* (Romania's Cybersecurity Strategy of 30th December 2021 for 2022-2027). https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235 [Accessed 7th May 2024].

ICI București. (n.d.) Ici.ro. from https://ici.ro/ro/ [Accessed 29th April 2024].

National Cyber Security Directorate, DNSC. (2023) *Bucharest Cybersecurity Conference* https://www.dnsc.ro/bucharest-cybersecurity-conference-2023/about/ [Accessed 7th May 2024].

National Cyber Security Training Centre of Excellence. (2023) Centrul National de Formare in Securitate Cibernetica. https://cstce.ro/ [Accessed 7th May 2024].

NIS 2 Directive. (2024) *Preamble 41-50, Final Text*. https://www.nis-2-directive.com/NIS_2_Directive_Preamble_41_to_50.html

Orange. (n.d.) www.orange.ro. https://www.orange.ro/ [Accessed 29th April 2024].

ROCSC. (2024) ROCSC24 - Campionatul Național de Securitate Cibernetică, https://www.rocsc.ro/ [Accessed 7th May 2024].

Romanian Intelligence Service. (n.d.) *Cyber intelligence.* https://www.sri.ro/cyberint [Accessed 7th May 2024].

Romanian Parliament. (2023) *LAW No 58, dated March 14th, 2023 on Romania's cyber security and defense, and for amending and completing some normative acts*, https://www.sri.ro/assets/files/legislatie/2024-eng/the_Law_No_58.pdf [Accessed 24nd April 2024].

Sharkov, G., Todorova, C., Koykov, G. & Nikolov, I. (2022) Towards a Robust and Scalable Cyber Range Federation for Sectoral Cyber/Hybrid Exercising: The Red Ranger and ECHO Collaborative Experience. *Information & Security.* 53(2), 287-302. doi: 10.11610/isij.5319.

Universitatea Maritimă din Constanța. (2024, April 24) https://cmu-edu.eu/ [Accessed 29th April 2024].