Romanian Association for Information Security Assurance

CYBERSECURITY: CHALLENGES AND PERSPECTIVES IN EDUCATION

A project with the support of

ROMANIAN NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM - CERT-RO

MINISTRY OF EDUCATION AND RESEARCH

ROMANIA
2020

Romanian Association
for Information Security Assurance

CYBERSECURITY - CHALLENGES AND PERSPECTIVES IN EDUCATION

EDITORS
Ioan-Cosmin MIHAI, Costel CIUCHI, Gabriel PETRICĂ

ROMANIA
2020

This book was achieved as part of a project launched by the Ministry of Education and Research through the National Authority for Scientific Research and Innovation.

The book expresses the opinion of the authors and does not necessary reflect the official opinions of their institutions. The correction belongs to the authors.

Acknowledgement

On behalf of the Romanian Association for Information Security Assurance (RAISA), we would like to express our gratitude to the Romanian National Computer Security Incident Response Team (CERT-RO) for the support offered in developing this book.

We are truly grateful to all the authors and we appreciate their dedication to write about the cybersecurity challenges and perspectives in education. Thank you all!

Academica Greifswald

Bluecherstr. 54A

18055 Rostock, Germany

ISBN: 978-3-940237-26-2

DOI: 10.19107/CYBERSEC-EDU.2020.EN

Table of Contents

Foreword

Dan CÎMPEAN
General Manager - Romanian National Computer Security
Incident Response Team (CERT-RO)

This is not the first time that renowned professionals from the cybersecurity field have joined forces to offer a compilation of works meant to readily support readers and field specialists alike, in their practical efforts, but also to inspire, reveal new perspectives and broaden horizons.

It is, however, correct for me to state that this is likely the first time one can notice such a confluence between deeply sophisticated topics as those richly presented by the volume "*Cybersecurity - Challenges and perspectives in education*", part of the works developed by RAISA (Romanian Association for Information Security Assurance).

The authors' individual efforts create, by simple juxtaposition of their papers, a unique overview of activities, models, aspects and approaches to our technological reality and the challenges imposed by the cybersecurity field.

Simultaneously, readers are the net beneficiaries of meticulously-crafted and detailed perspectives, analyses and complex concepts, presented nevertheless in a manner of unerring clarity and concision.

From a preliminary reading, I was pleasantly surprised by the pragmatism of ideas and recommendations within, particularly those addressed directly to the reader. In essence, each chapter urges us to apply ourselves, to implement, to validate our newly-gained knowledge in practice…

Education is, invariably, a key topic of all included works and is successfully and simultaneously approached from a Romanian, European and international perspective. Since cyberspace has no borders, it is clear that education within the field of cybersecurity must also find a way to transcend physical, cultural and geographical barriers. New skills must be developed, new knowledge must be acquired, a profound

cultural shift is desired from each of us, a new educational approach is needed. All this must be undertaken within a brief timeframe and under the increasing pressure of our swift, contemporary digital transformation.

I believe that "*Cybersecurity - Challenges and perspectives in education*" is a precious instrument, an effective and lavish aid in our quest. We would do well to start employing it today…

Foreword

Professor Ioan C. BACIVAROV, PhD

President of the Romanian Association for Information Security Assurance (RAISA)

The accelerated evolution of technology generates many opportunities, but also many challenges for the information society. The number of newly discovered vulnerabilities, data breaches and cyber-attacks is increasing, making cybersecurity a major concern among countries and businesses. The expansion of online activities, in the context of the COVID-19 pandemic, has highlighted the importance of cybersecurity issues and large-scale education and training in the field, practically for the entire population.

The volume "*Cybersecurity - Challenges and perspectives in education"* is part of the studies developed by RAISA (Romanian Association for Information Security Assurance), which emphasize the importance of cybersecurity in all its aspects (managerial, technical, educational), as well as the importance of international cooperation in this modern and sensitive field. This cycle of studies began with the work "*Considerations on challenges and future directions in cybersecurity*"[1], launched during the Romanian Presidency of the Council of the European Union, in 2019.

RAISA is a professional, non-governmental and public benefit association, founded in 2012 as an initiative dedicated to disseminating the concept of cybersecurity and fighting against cybercrime. The aim of this association is to promote and support information security activities in compliance with applicable laws and to create a community for knowledge exchange between specialists, academia, and the corporate environment. The vision of RAISA is to develop research and education in information security field, to contribute to the creation/dissemination of knowledge and technology in this domain and to create a strong "cybersecurity culture" at national level.

[1] This study was developed with the support of the Romanian National Computer Security Incident Response Team (CERT-RO) and the National Cyberint Center within the Romanian Intelligence Service. The study is available at https://www.raisa.org/documents/CybersecurityRO2019.pdf.

In the current context, it is important to underline that while organizations continue to purchase and deploy technical controls, not much has been done to focus on the human side of cybersecurity - so named *Layer 8*. The term *Layer 8* is often used by the IT professionals to refer to employees' lack of awareness and a weak overall cybersecurity culture. Consequently, is of crucial importance for all the countries, professional organizations, and companies to consolidate a powerful "cybersecurity culture". In this context, one of the main objectives of RAISA (*www.raisa.org*) is to support[2] research and education in the field of cybersecurity in Romania.

The study "*Cybersecurity - Challenges and perspectives in education*" is a collection of papers that emphasizes the importance of creating a culture of global cybersecurity, education, and training in this sensitive area. The views of some officials of the representative organizations in the field, such as CEPOL and ESDC, of some universities and other important organizations in the field, come to strengthen this idea.

The studies included in this volume address various aspects, from the creation of Cybersecurity Ecosystems to the development of university educational programs in the field, seen through the prism of a necessary education-research cooperation and an international approach in this field. Issues - from education for a digital world and the development of resilient education systems, capable of responding to cybersecurity challenges, to ethical and integrity issues - are the subject of interesting studies included in this volume.

This study contains papers from specialists with a vast expertise, from different domains, presenting a systematic and integrated approach of the essential aspects specific to the field of education and training in cybersecurity. The added value of the study is given by the analysis of future directions in the field from the perspective of the experts from the public, private and academic institutions.

RAISA is very grateful to all those who have contributed to this study and hopes this study will underline the importance of education in cyber-security field, as well as of the cooperation for all the countries, organizations, and companies, in order to consolidate a powerful cybersecurity culture.

[2] Among the notable activities developed by RAISA, we mention the "*International Journal of Information Security and Cybercrime*" (IJISC), a scientific journal indexed in international databases (*www.ijisc.com*), awareness websites (*www.securitatea-informatiilor.ro*, *www.criminalitatea-informatica.ro*, *www.securitatea-cibernetica.ro*), workshops, research projects and studies in the field of cybersecurity.

CEPOL - The European Union Agency for Law Enforcement Training Activities in the Field of Cybercrime

Dr.h.c. Detlef SCHRÖDER, Dr. Ioan-Cosmin MIHAI
European Union Agency for Law Enforcement Training (CEPOL)
info@cepol.europa.eu

1. About CEPOL

The European Union Agency for Law Enforcement Training (CEPOL) is dedicated to developing, implementing, and coordinating training for law enforcement officials. CEPOL brings together a network of training institutes for law enforcement officials in EU Member States and supports them in providing frontline training on security priorities, law enforcement cooperation and information exchange. It contributes to a safer Europe by facilitating cooperation and knowledge sharing among law enforcement officials from the EU Member States and, to some extent, from other countries, on issues stemming from EU priorities in the field of security; in particular, from the EU Policy Cycle on serious and organised crime.

CEPOL employs a multi-layered approach to learning, including:

- *Onsite activities*, which are typically comprised of courses, conferences, workshops, and seminars. With some exceptions, they normally last a week and are held in a training institute in one of the Member States or at the CEPOL HQ. Residential activities provide an opportunity to gain a deeper understanding of a subject.
- *Online learning* is a way of computer-based distance learning. Online learning takes place in form of webinars, online modules, online courses, cyberbites, e-Workshops, and e-Lessons.
- *The CEPOL Exchange Programme* allows law enforcement officers to spend one week with a counterpart in their own country, exchanging knowledge and

good practices, initiating cooperation projects, and fostering long-lasting learning and networking opportunities.

In particular, the onsite training activities and the Exchange Programme provide excellent opportunities for building up professional networks and trust among the officers engaged.

All activities are supported by CEPOL's Law Enforcement Education platform (LEEd). Through LEEd, users have access to tools and resources that support and deepen the learning experience. The LEEd platform also provides access to a large collection of e-Books and e-Journals, which provides registered users with access to international scientific publications related to police science and police practices.

2. CEPOL Cybercrime Academy

The different forms of cybercrime are a major threat for the internal security of Europe. In consequence, CEPOL has identified cybercrime as one of its key priorities for the upcoming years. In order to respond to the growing training demand in the cyber area, CEPOL has strengthened its cyber-training portfolio and has established the European Cybercrime Training Academy, which is properly equipped and configured to train one hundred participants simultaneously.

The CEPOL Cybercrime Academy Laboratory

The CEPOL Cybercrime Academy was officially inaugurated on the 13th of June 2019 in Budapest, by the European Union Agency for Law Enforcement Training (CEPOL), in the presence of a number of high-level guests and speakers, including the Deputy Prime Minister of Hungary, Dr Sandor Pinter, as well as the Director for Security at the European Commission, Mr Laurent Muschel.

The Academy is equipped with state-of-the-art hardware and software, fully configured to train up to one hundred participants at the same time. Cybercrime is one of the fastest growing forms of crime. The European Union is fully aware of the increasing consequences of cybercrime, and the need to protect cyberspace from incidents and malicious activities has become crucial for the functioning of our societies and economies. Developing the necessary knowledge and expertise in law enforcement authorities across Europe is key in addressing the evolving challenge of cybercrime.

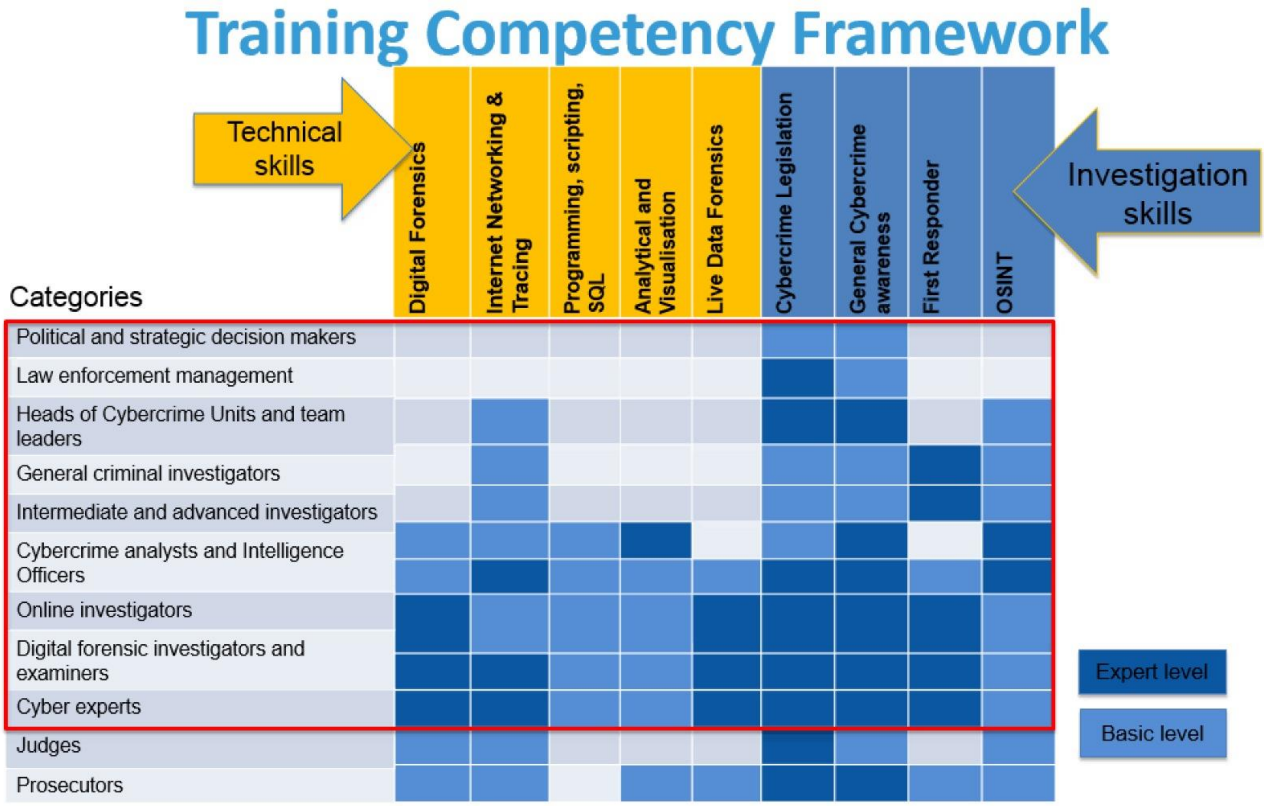
Speaking at the opening event, CEPOL's Executive Director, Dr. h.c. Detlef Schröder, underlined that: "*All electronic learning cannot replace the learning experience in a group of officers from different countries from the same profession in a classic training setting. This Academy will enable that we can offer to our Member States the required training on a by far higher scale*".

Opening Ceremony of CEPOL Cybercrime Academy

3. Training needs analysis on cybercrime

Training needs are analysed based on the Training Competency Framework (TCF) developed periodically by CEPOL in cooperation with The European Union Agency for Law Enforcement Cooperation (Europol), The European Union Agency for Criminal Justice Cooperation (Eurojust), The European Cybercrime Training and Education Group (ECTEG), The European Union Cybercrime Task Force (EUCTF), The European Judicial Training Network (EJTN). The TCF on Cybercrime identifies the required competencies and skills in combating cybercrime at the EU level for key actors ranging from law enforcement to the judiciary.

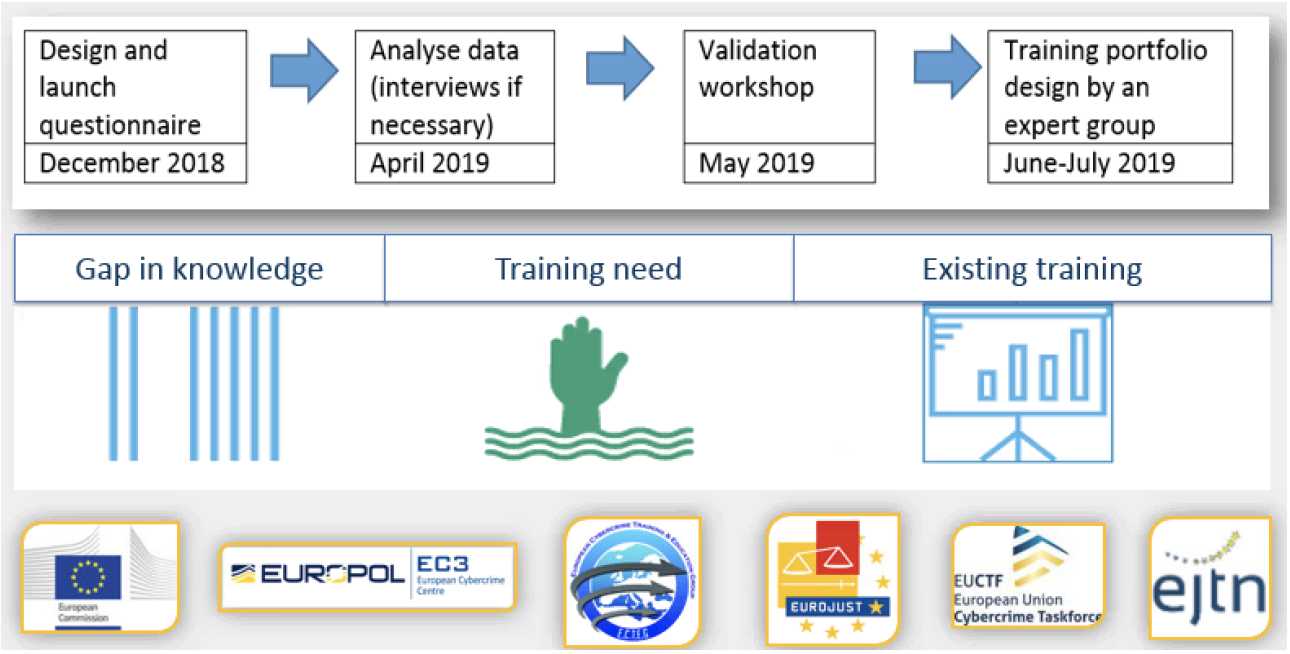
The TCF defines the level of knowledge LE officials taking part in cyber investigations should have in all roles and competencies. It distinguishes between basic and expert level of knowledge necessary to fulfil their daily tasks.



The Training Competency Framework

The analysis, its consequent prioritisation of training needs, and the design of the training portfolio is the outcome of a joint effort coordinated by CEPOL, Europol's EC3, ECTEG, EUCTF, Eurojust, European Commission, and EJTN – all

organisational members of the so-called Training Governance Model (TGM). The target groups for the Cyber Training Needs Analysis (TNA) are Heads of Cybercrime Units and Cyber-experts nominated by the Member States and Europol.

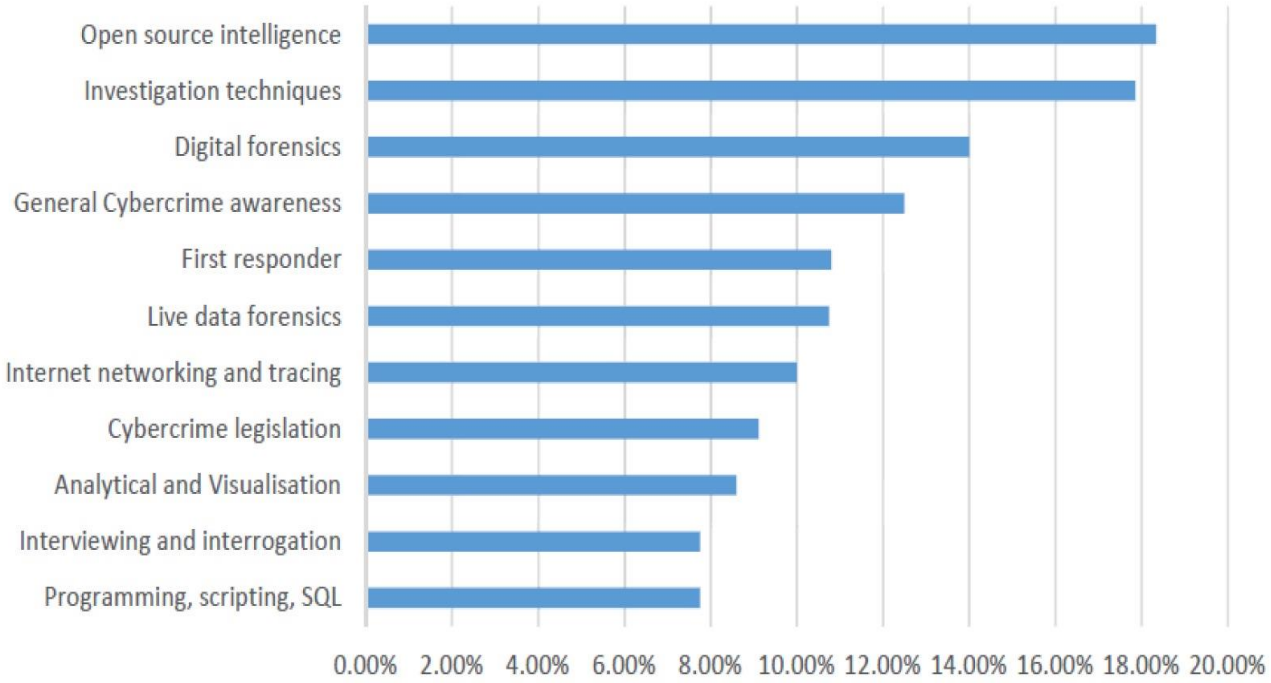


The Cyber Training Needs Analysis Methodology

The training is a matter of urgency, as it should be provided between six months and one year. The need is most pressing for cybercrime analysts, intelligence officers, digital forensic investigators, and examiners, whereas it can be delivered within a year to intermediate and advanced intelligence officers and to law enforcement management.

Training available on a national level by role

Existing training is scarce for all roles and competencies, meaning that only 10% of respondents indicated that national level training activities on this topic area are provided on a sufficient level. The profiles where most training is available is the one of digital forensic investigators and examiners.



Training available on a national level by competency

The competency most targeted by training on a national level is the use of Open Source Intelligence. Less than 10% of respondents indicated that national level training is available to enhance competencies in programming, scripting, SQL, analytical and visualisation, interviewing and interrogation, and cybercrime legislation.

In the profiles of intermediate and advanced intelligence officers, online investigators, cyber experts and first respondents, there are hardly any training opportunities available.

Based on the latest training needs assessment conducted by CEPOL, in close cooperation with the EU Member States, the demand towards qualifications offered by CEPOL on Cybercrime would require an annual training volume of approx. 3,800 officers to be trained.

4. Cybercrime training activities

CEPOL, in the last years, has invested in an enhanced portfolio of cybercrime related training opportunities. In 2019, CEPOL has trained 7,477 officials from EU Member States on such topics. For 2020, despite the massive challenges stemming from the COVID-19 pandemic, CEPOL estimates to reach out to 7,100 individuals from law enforcement services in EU Member States.

CEPOL covers all three EMPACT (European Union Policy Cycle) priorities on cybercrime: attacks against information systems, child sexual abuse and sexual exploitation, and non-cash payment fraud. CEPOL will implement in 2021 the following courses:

- *Child Sexual Exploitation on the Internet - Undercover Operations*

  The aim of this course is to enhance the fight against child sexual exploitation by creating and/or improving skills to operate undercover online and to bolster cooperation involving the identification of such crimes, and the production and dissemination of child abuse material on the internet by the organised crime groups.

- *Child Sexual Exploitation – Victim Identification*

  This course is designed to strengthen collaboration between law enforcement institutions from the EU MS, the Associate countries and the Candidate countries, in the identification of child victims of sexual exploitation, and to instil or develop skills of specialised law enforcement officers in the task of victim identification at the national and international levels.

- *Strategies in Managing Child Sex Offenders*

  The goal of this course is to facilitate the knowledge transfer between Member States on the application and coordination regarding the implementation of Directive 2011/93/EU of the European Parliament and of the Council, of 13 December 2011, on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework-Decision 2004/68/JHA.

- *Combating card fraud*

  The course provides a framework of cooperation and shared experiences on investigative methods involving crimes in the field of skimming devices and non-cash payment fraud, and aids in the development of skills dedicated to the collection of forensic evidence in matters of payment card fraud, such as skimming, as well as perspectives on the card-not-present fraud cases. Additionally, it helps to improve national and cross-border operational capacity on countering ATM attacks.

- *Open-Source Intelligence (OSINT) and IT Solutions – 2 courses*

  The aim of these courses is to enhance cyber-crime investigation by improving the collection, evaluation, collation, analysis and distribution of information for the purpose of tackling all forms of crime, in particular terrorism and organised crime, and by improving the quality and quantity of collected intelligence.

- *Darkweb and Cryptocurrencies – 2 courses*

  These courses focus on magnifying the cooperation on cross-border cases by employing the TOR-network and the Darkweb, and augmenting capabilities of finding virtual currencies (VC) in the course of criminal investigations, as well as identifying the existence of a VC wallet, notably in the context of searches.

- *Conducting Forensic Searches in Various IT Devices*

  The course seeks to enhance cyber forensics work by improving the skills of forensic experts in the matter of recovering digital evidence or data from electronic devices, particularly mobile and Internet of Things (IoT) devices, and by sharing experiences on computer data analysis, technical aspects of Internet investigations and examination of IT devices.

- *Cybercrime - advanced Windows file system forensics*

  This course is designed to provide cyber forensics experts with detailed knowledge on the recovery of evidence from file systems, and to allow them to explain forensic tools reports and conduct searches beyond commonly

reported traces in order to establish a trace history and potential use of anti-forensics.

- *Cross border exchange of e-evidence*

  The goal of this course is to improve prosecutors' and law enforcement officials' use and exchange of electronic evidence in investigation and prosecution of cybercrime, as well as the relevancy and admissibility of such evidence, ultimately enhancing cyber-investigations.

- *Digital forensic investigators training*

  The objective of this course is to ameliorate high-tech crime investigations by augmenting the officers' knowledge on Open-Source forensic software, file systems, data carving, evidential digital artefacts, networking and network security, cloud computing, email investigations, computer forensic strategies and live data forensics, based on the latest investigation techniques and methods.

- *First responders and cyber forensics*

  This course focuses on enriching cyber-forensics work by providing law enforcement officials with practical abilities in computer forensics, such as revealing and investigating traces of cybercrimes, by enhancing cooperation and harmonising investigative methods between law enforcement departments with regard to assessing a crime scene in case of a cyber-incident and to handling electronic evidence.

- *Cyber-Intelligence*

  The Cyber-Intelligence course provides necessary knowledge and skills to enable law enforcement officials to perform role tracking and analyses, and to counter digital security threats in order to produce actionable intelligence.

- *Malware Investigation*

  The scope of this course encompasses retrieval of information from the malware analysis process which will aid in locating criminals and their infrastructure during the course of the cyber-investigation.

- *Live Data Forensics*

  The purpose is to strengthen cyber-forensic work of law enforcement investigators by introducing them to powerful Live Forensics investigative techniques with an overview of Live Data Forensics and its uses.

- *Mac Forensics*

  The course offers general and practical knowledge of Mac OS X forensics at a basic level.

- *Linux Forensics*

  The course offers general and practical knowledge of Linux forensics at a basic level.

Due to the COVID-19 Pandemic situation, some of the aforementioned courses will be available online, on LEEd – CEPOL's online learning platform.

Additionally, different activities such as online modules, webinars, and cyberbites (micro-learning products delivered in the area of cybercrime – videos with interactive elements), alongside new CEPOL products like e-Workshops and e-Lessons, are already implemented or will be made available in due time.

The CEPOL e-Workshops are e-learning products that focus on interactive learning in small groups, which will be organised as a series of two to three online workshops over a period of 3-4 hours involving a maximum of ten participants and one or two trainers. The e-Workshops that will be implemented by CEPOL are:

- *CEO Fraud/Business Email Compromise.*

  The purpose is to improve performance of LE officers by sharing best practices, methods, and tools for fighting online fraud against companies.

- *Analysing Email-based Attacks.*

  The aim of this e-Workshop is to enhance the officers' investigation capacity in order to lower the number of email-based attacks.

The CEPOL e-Lessons are comprised of an estimated study time of up to sixty minutes, divided over a specific number of chapters or sub-topics. Overall, the e-Lessons are an interactive and explorative learning environment. The first e-Lesson to be implemented by CEPOL Cybercrime Academy is "*Cyber investigations in social*

networks", with the aim to enhance the LE officers' investigation capacity in order to discover and obtain electronic evidence from social networks.

5. Conclusions

The cybercrime phenomenon is, by its nature, rapidly developing, cross-national and without borders. Cybercrime encompasses traditional offences, content-related offences, and offences unique to computers and information systems. In recent years, the digital and cyber component in most types of crime has been constantly increasing.

As a learning organisation, the European Union Agency for Law Enforcement Training (CEPOL) approaches cybercrime training from a perspective of where the agency can best optimise its impact, partnering with relevant organisations and focusing on mainstreaming cybercrime into its overall learning and training strategy and the corresponding output.

CEPOL has strengthened its cyber-training portfolio and human resources, establishing the Cybercrime Training Academy in order to support the development and delivery of training, primarily for senior police and specialised officers with a range of activities in the cybercrime divisions of cyber-attacks, non-cash payment frauds, child sexual exploitation, cyber-forensics and electronic evidence.

References

[1] About CEPOL, https://www.cepol.europa.eu/who-we-are/european-union-agency-law-enforcement-training/about-us.

[2] CEPOL's Mission, Vision, and Values: https://www.cepol.europa.eu/who-we-are/european-union-agency-law-enforcement-training/mission-vision-values.

[3] CEPOL Cybercrime Academy, www.cepol.europa.eu/media/news/cepol-cybercrime-academy-inaugurated.

[4] Training Competency Framework on Cybercrime, 2019.

[5] CEPOL Operational Training Needs Analysis Cybercrime – Attacks against Information Systems, 2019.

[6] The impact of COVID-19 on law enforcement operations and training needs, 2020.

[7] CEPOL Training Catalogues 2020 and 2021.

CSDP Cyber Education, Training, Exercise and Evaluation (ETEE) Platform under the ESDC

Dirk DUBOIS, Dr. Marios THOMA, Dr. Gregor SCHAFFRATH
ESDC - European Security & Defence College
ESDC-CYBER-ETEE@eeas.europa.eu

Background

Following an update study undertaken by RAND Europe, the EU Military Committee (EUMC) agreed on a collegiate view to create a Cyber Defence Centre/Education, Training, Exercise and Evaluation (ETEE) Platform under the auspices of the ESDC. On 13 November 2017, the EDA Steering Board, bringing together the 27 participating Ministers of Defence, agreed with this collegiate view and decided to request the ESDC to establish such a Centre (hereinafter the 'Platform').

Constraints

Taking into account the 'modus operandi' of the ESDC, the idea was that the implementation of the Cyber ETEE Platform should not change the main characteristics of the ESDC as a Member States-driven network of training providers in the field of CSDP. The main aim would be to educate and train civilian and military personnel of the Member States and the EU institutions in different fields of cybersecurity and cyber defence, in particular staff deployed in or designated for CSDP missions and operations.

Proposal on the governance structure

The Platform was to be considered a project run under the auspices of the ESDC, similar to the European Initiative for the Exchange of Young Officers, the Doctoral School project and others.

At the pre-operational capability stage, it was decided that the Platform would be supported by the eLCIP configuration of the Board.

It (and its successor EAB.Cyber) would report back to the EAB (like other configurations) and provide advice to the Steering Committee. The Steering Committee would remain the sole decision-taking body of the ESDC.

Mission of the Cyber ETEE Platform

The mission of the Cyber ETEE Platform – as agreed to by the Steering Committee of the college - is to address cybersecurity and defence training among the civilian and military personnel, including for the CSDP requirements for all CSDP training levels as identified by the EU Military and Civilian Training Groups (EUMTG and EUCTG), and to upscale the training opportunities for the Member States.

At a later stage, and depending on the further development of such a concept, the Cyber ETEE Platform could advance ETEE opportunities for a wider cyber defence workforce (the so-called Cyber Reserve).

Decisions taken regarding the Cyber ETEE Platform

The Cyber ETEE Platform was established over multiple important milestones.

On 6 February 2018, the EU Member States, represented in the ESDC Steering Committee, decided that a Cyber Education, Training, Exercise and Evaluation (ETEE) Platform should be created within the ESDC. A questionnaire was sent out to identify the existing offers and demands for Cyber ETEE activities in the Member States, as well as the priorities and challenges for cooperation at EU level in this field.

On 14 May 2018, the Council adopted Decision (CFSP) 2018/712 amending Decision (CFSP) 2016/2382 establishing a European Security and Defence College, and broadening its activities in the cyber domain.

On 29 June 2018, the ESDC Steering Committee followed the advice of the EAB to refocus the mission of the eLCIP EAB configuration and to rename the configuration EAB.Cyber.

Three phases were identified for the implementation of the Platform: Pre-Initial Operational Capability (pre- IOC), Initial Operational Capability (IOC) and the Full Operational Capability (FOC).

EAB.CYBER

The role of EAB.CYBER in the creation of the Cyber ETEE Platform is crucial. The EAB.CYBER configuration has been mandated to deal with the practical aspects of implementing the Cyber ETEE Platform and specifically its mission is to facilitate the establishment and operation of the Cyber ETEE Platform, and to coordinate ESDC activities in the field of cybersecurity. EAB.CYBER may also be tasked with supporting EU projects.

The first EAB.Cyber meeting took place on 27 September 2018. During that meeting Professor Stavros Stavrou from the Open University of Cyprus, Dean of the Faculty of Pure and Applied Sciences, was nominated as the new (and current) Chair of EAB.CYBER.

EAB.CYBER meets regularly every three months during each academic year of the ESDC. Its discussion items comprise activities under the Cyber ETEE Platform (including curriculum development and activity evaluations), as well as developments in the overall cyber context. It is also the focal point to foster collaboration and to establish synergies between its network members in the academic and operational domains.

Situation Analysis in the Pre-Initial Operating Capability of Cyber ETEE

The European Security Defence College included cybersecurity as a horizontal topic in the context of many of its CSDP Orientation Courses and in the CSDP High Level Course (HLC). The ESDC provided one High Level Course and approximately 15 orientation courses per academic year.

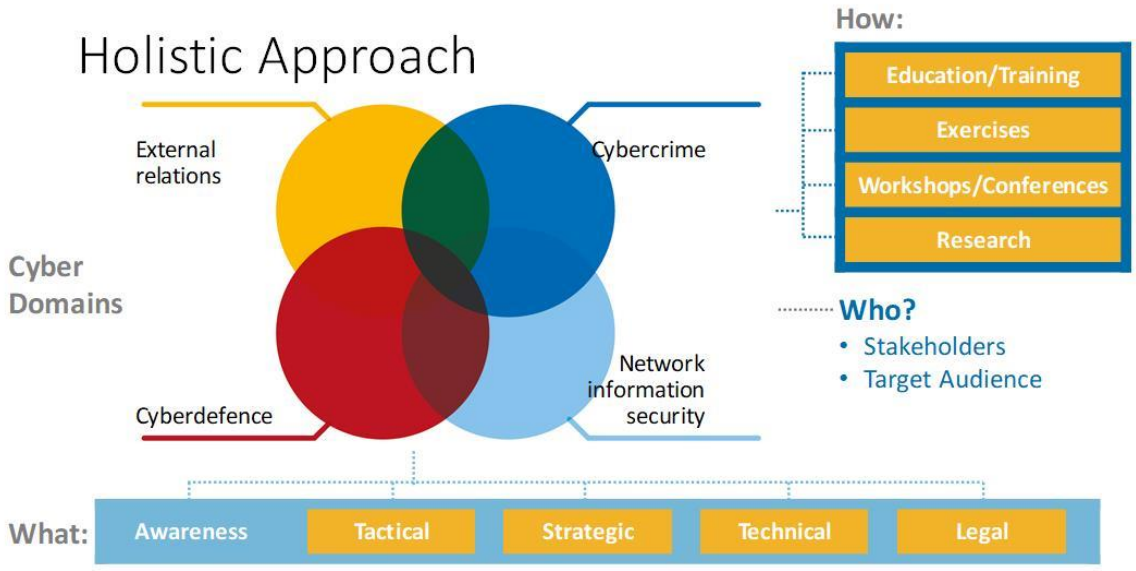
As dedicated courses, the ESDC offered two standard activities (‘Challenges of EU Cybersecurity’ and ‘Cyber Security, Cyber Defence’), as well as pilot activities such as the ‘Cyber-Security and Defence Course for Senior Decision-Makers’.

The target audience of the ESDC's dedicated Cyber Courses were mid-ranking to senior officials, dealing with strategic aspects in the field of cybersecurity and cyber defence from EU MS, EU institutions, and relevant agencies. For decision-makers, the courses were at awareness and strategic level.

The courses were provided and co-financed under the modus operandi of the ESDC and were cost-free for the participants.

Analysis of the EU Cyber Ecosystem

Based on the state of play regarding cyber within the EU and the decisions in place, the ESDC secretariat analysed the EU cyber ecosystem and the Member States' training requirements in the cyber field. During the first meeting of EAB.Cyber, on 27 September 2019, a new model to be followed regarding cyber training (implemented by the Cyber ETEE Platform) was proposed.



This model foresees the Cyber ETEE Platform to deal with all cybersecurity domains, such as Cyber Crime, Network Information Security, Cyber Defence and External Relations.

Implementation of the Platform

Furthermore, during the first meeting of EAB.Cyber, a concrete plan for the way ahead was proposed. Topics and fields of expertise (such as the 'tactical', 'strategic',

'technical' and 'legal' fields) were identified. This was done taking into consideration both best practices and Member States' replies to the questionnaire sent in 2018. Analysis is ongoing for each field of expertise. Awareness courses will build the basis for in-depth courses in the abovementioned fields.

It was proposed that the goals of the Platform should be achieved through:

- Education/training - curricula development for the different training courses organised under the ESDC Cyber ETEE Platform;
- Exercises - support for scenario development (covering the functional and operational level);
- Workshops/conferences - identification of topics, lecturers and institutions to be involved;
- Research - identification of relevant actors, best practices and new approaches.

Education and training-related activities (Courses, Exercises, Workshops, and Conferences) were identified as the ESDC's first priority.

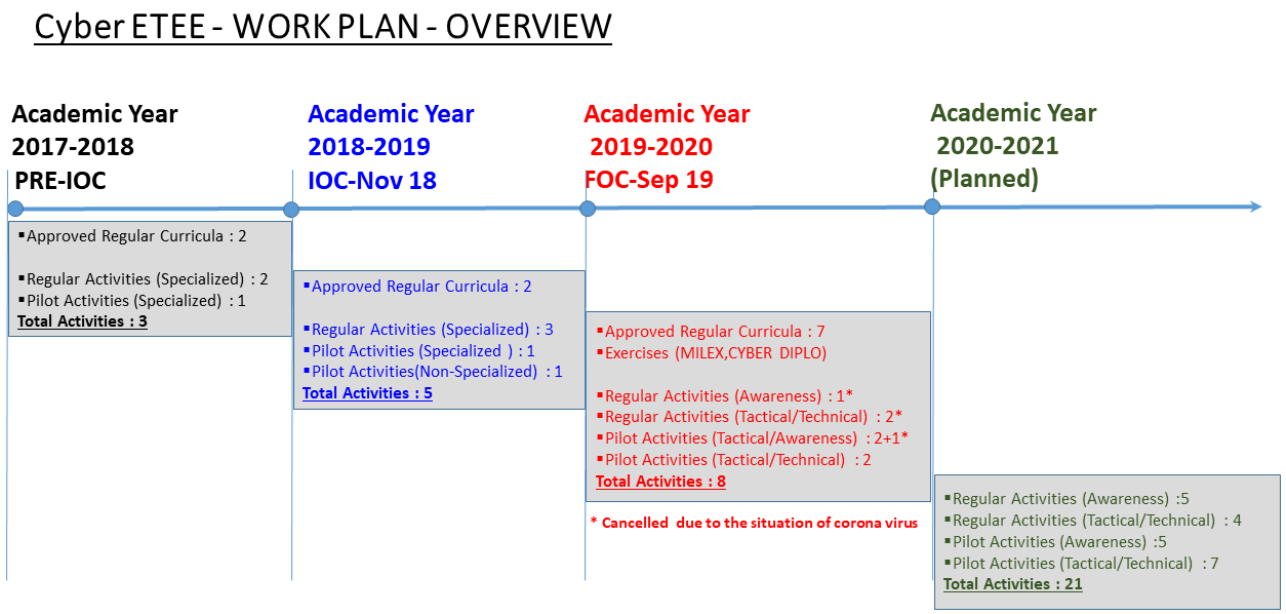
Initial Operational Capability (IOC)

After its kick-off meeting on 20-21 November 2018, the Cyber ETEE Platform was running at the Initial Operational Capability. During this academic year, four SNEs were recruited from the Member States: Cyprus (July 2018), Germany (November 2018), Romania (January 2019) and Greece (June 2019).

At the time, EAB.Cyber was constituted of 61 organisations. The accession of four new network members and one associated network member was initiated. Three regular training courses were provided during this academic year.

Furthermore, during the IOC, the Cyber ETEE was involved in several activities such as offering keynote speakers at EU conferences, seminars and workgroups, speaking in NATO conferences, and engaging with EU Commission-funded projects.

The College attributed great importance to collaboration with EU agencies, such as ENISA and EDA. Several specific projects were launched with in collaboration with both.



Full Operational Capability (FOC)

FOC was reached on September 2019 and was declared during the 5th EAB.CYBER.

While the Platform is still in its early stages, it is already becoming an active, visible and a successful actor in the EU cyber ecosystem. Additional cyber activities have been planned in all cyber domains and at all levels during the academic year 2020–2021, including tactical/technical activities with high expertise.

The Cyber ETEE Platform was involved in supporting both the European External Action Service during the Cyber DIPLO 2019 exercise and the EUMS during the MILEX 2019 exercise. A collaboration, which will be repeated for this academic year.

Current developments

Additional courses and curricula are established every year and co-funding for technical courses has been expanded. Among the newest are:

- Tactical level activities (Cybersecurity organizational and defensive capabilities, Training in critical infrastructure protection with emphasis on cyberspace);
- Strategic – Tactical level activities (Cyber diplomacy modular course, Cyber defence policy at national and international level);

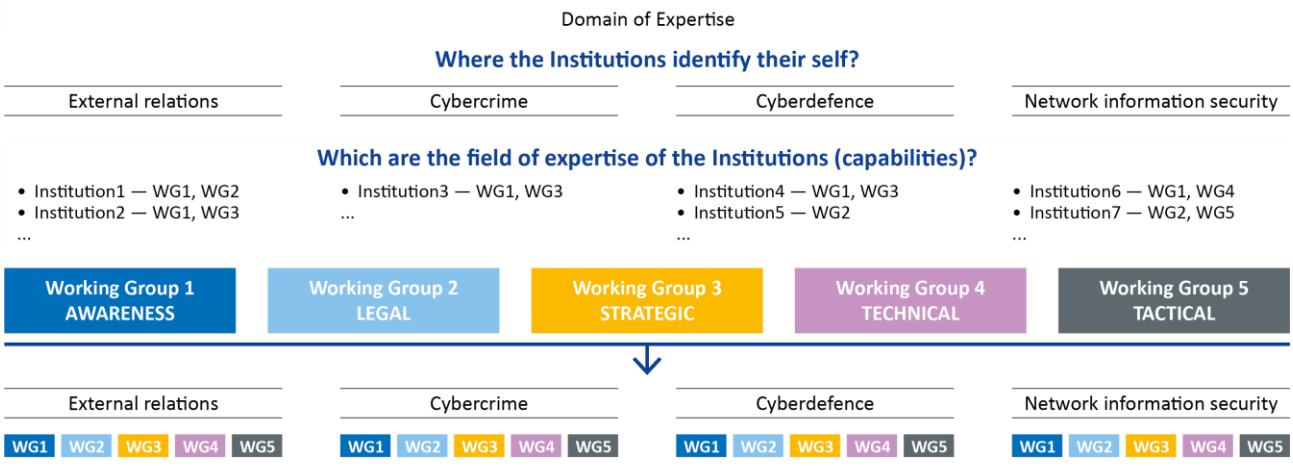
- Technical level activities (Information security management and ICT security);
- Awareness level activities (EU cyber security challenges, The role of the EU's cyber ecosystem in global cyber security stability).

You can find more information regarding the courses at the ESDC website[1] or through the Goalkeeper[2] application.

Moreover, the ESDC continues its engagement in the EU-NATO collaboration process by establishing working relations with the NATO Maritime Interdiction Operational Training Center, welcoming it among its Associated Network Partners, and by participating as keynote speaker and moderator in NATO Cyber conferences.

Network Members have been clustered in working groups. To this end, they were asked to position themselves according to their domain of expertise (External Relations, Cybercrime, Cyber defence and Network Information Security - NIS), and accordingly identify their field of expertise (in-house capabilities) as follows:

- WG1 - Awareness Working Group 1;
- WG2 - Legal Aspects Working Group 2 (Legal framework);
- WG3 - Strategic Working Group 3 (Decision-making procedure);
- WG4 - Technical Working Group 4 (ICT expertise and hands-on);
- WG5 - Tactical Working Group 5 (Planning/Acting).



[1] https://esdc.europa.eu
[2] https://goalkeeper.eeas.europa.eu/

In an effort to increase cohesion within the cyber domain and to improve the exchange between academic research and the operational world, ESDC is currently exploring the establishment of a research cooperation program under the Cyber ETEE Platform. The idea is to leverage the knowledge and innovative power of academia for the problems existing in the operational field.

Vision – way forward

Given that the ESDC is a network college (capabilities and resources are within the network of the College), its Cyber ETEE Platform aims to facilitate training coordination within the EU cyber ecosystem in order to:

- transfer cyber knowledge between domains,
- focus and to deepen/strengthen cyber expertise,
- thereby improve the quality of education/training/exercises,
- develop cooperation and synergies (saving resources and time), and
- reduce overlaps and achieve the necessary complementarity between actors.

The goal is to deliver directed, sophisticated, and target-oriented activities by harmonising and standardising Cyber ETEE, thereby establishing a common European cybersecurity culture at EU level and at the same time contributing to global cyber stability.

Cybersecurity from a University Perspective

Prof. Dr. Udo HELMBRECHT
Technical Director Research Institute CODE, Department of Computer Science,
Universität der Bundeswehr München, Germany
udo.helmbrecht@unibw.de

1. Our today's digital world

Every part of your daily life is digitally permeated. E-banking, e-health, e-commerce, e-education, e-everything are all now totally dependent on an open, safe and secure cyberspace. We are witnessing the development and deployment of smart manufacturing, the Internet of Things (IoT) and computer controlled critical infrastructures. Digital is challenging the delivery of old business models, while at the same time providing opportunities for the new world. We see new challenges to old business models, where for example mobile phone manufacturers and internet search engine companies are moving into smart transport. Europe has to embrace this challenge and take the lead in the digital revolution by delivering disruptive business models, using innovative technologies and services, in a safe and secure manner. Europe has to ensure the trust of its citizens and industry to have the necessary confidence to work with digital. Thus, research is fundamental to achieve European prosperity and European technical sovereignty in a competitive globalized world.

The delivery of Digital can be broken into three components, the generation of digital data, the transmission of digital data from the generator of the data to the processor, and the storage of digital data. The transmission of data between the source and processor of the data is another critical part of the digital chain. Encryption, digital signatures and trusted secure communications of digital data are key enabler of the internal market.

The volume of data being generated in our digital world is growing at exponential levels. The average computer for sale in the high street and online now

holds terabytes of information. What this term means is that for every terabyte of storage there is 1000 million pieces of digital information to be stored. It is against this background that the term Big Data has been invented. One of the relatively new business models that has developed in the last few years to cope with the volume of Big Data is the Cloud Computing business model. In this model citizens and industry can have their data stored in a central location where the expertise, capacity and security should be available to store the data in a secure manner.

2. The tole of the digital industry

The importance of industry in the digital world cannot be underestimated. We see initiatives of the European Commission such as Innovation for Manufacturing SME (IM4S)[1], Horizon Europe[2] and Connected Europe Facility (CEF)[3], promoting the next generation of technologies. Data breaches, theft of intellectual property, sabotage of industrial processes is not new. What is difficult is the quantifying of the losses that are occurring due to breaches in digital network and information security. The healthcare sector was the most targeted by hackers in 2020 and the data breaches cost were estimated to $2.5 billion[4]. The growth in the cybersecurity insurance market is testament to the increasing realisation of the importance of this subject and the concern that CEOs are increasingly attaching to cyber security. What is clear, is that cyberattacks are increasing, the attacks are becoming more sophisticated, and the losses are escalating.

3. Emerging technologies

Universities play an important role in the research of emerging technologies. This chapter gives an overview of current emerging technologies:

The below links were accessed on 15th October 2020:
[1] https://ec.europa.eu/digital-single-market/en/innovation-ict-manufacturing-smes
[2] https://ec.europa.eu/info/sites/info/files/research_and_innovation/knowledge_publications_tools_and_data/documents/ec_rtd_factsheet-horizon-europe_2019.pdf
[3] https://ec.europa.eu/digital-single-market/en/connecting-europe-facility
[4] https://healthitsecurity.com/news/health-sector-most-targeted-by-hackers-breach-costs-rise-to-17.76b

3.1. Chip technologies

Moore´s law is well known but the challenge is that transistors reach atomic scale and fabrication costs continue to rise. The classical technological driver that has underpinned Moore's Law for 50 years could fail and it is anticipated to flatten by 2025[5]. So, what comes beyond Moore?

Today's desktops, laptops, smart phones or cloud services are based on the traditional von Neumann architecture. The same goes for technologies like edge-computing or high-performance-Computing (HPC). In the future the innovation might not take place in classical computer hardware. Quantum computers might be an alternative. Also, in the field of robotics or artificial intelligence we will see progress. Running algorithms on dedicated hardware like graphics processing units (GPU) can be an alternative. Thus, for example research on advanced materials, new computer architectures are needed.

3.2. Cloud Services

Cloud services are todays backbone of out digital society. Without the available of cloud services, we could not buy online, book flights online, use navigation systems, chat with our business partners or private friends in social networks or search for information. Different categories of cloud-Services used today are Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service or in the end everything-as-a-Service.

There are Benefits and cyber security risks of cloud-services. On one hand we have the cost-effectiveness regarding administration, maintenance and investment costs. On the other hand, the challenges are centralized local versus decentralized (cloud) control, "my own server room" versus virtual systems and system components (e.g. virtual machine, virtual memory) in the cloud and the different national legal regulations where the cloud provider physically hosts their systems.

[5] https://royalsocietypublishing.org/doi/10.1098/rsta.2019.0061

In the lockdown phase of the Covid 19 pandemic[6] our business and private life would not have worked anymore without cloud services like video conferences or online shopping to name a few examples. But we could also see that privacy is key and Cybersecurity is essential to protect these cloud services against malware, espionage and other attack vectors. Research on these topics is needed.

3.3. Internet-of-things (IoT)/ Internet-of-everything (IoT/IoE) and Smart systems

The miniaturization of computer chips allows ubiquitous computing. Already today smart watches, fitness trackers, surveillance cameras in households are commodity. Smart Homes and Smart Cities are the next technological step. But from a cybersecurity perspective IoT can become a nightmare. Well knows examples are the Mirai Botnet[7] or Wanna Cry[8] incident.

3.4. Usable security

Humans are fallible. Machines at least much less often. In Cybersecurity, humans are therefore considered to be the weakest link in the security chain. Insecure passwords that are passed on or written down, ignored security notices or security solutions bypassed on purpose are commonplace. Thus, in the design phase of secure systems usable security takes into account the way in which humans interact with computing devices. The objective is to design devices and systems for the need of human users.

3.5. 5G Technology

From a technical perspective 5G is part of the technical evolution in the telecom sector. The new technological feature is, that with the 5G technology we get a very low latency, greater speed in transmissions (15 or 20 Gbps) and greater bandwidth[9]. On the

[6] https://en.wikipedia.org/wiki/COVID-19_pandemic
[7] https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers
[8] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst
[9] https://www.iotsworldcongress.com/advantatges-of-5g-and-how-will-benefit-iot/

other hand, 5G has become a political issue, because from a European or American technical sovereignty perspective Europe respectively the USA would depend in the sectors of critical infrastructures on Chines companies' technology and products. The European Commission endorses a toolbox of mitigating measures agreed by EU Member States to address security risks related to the rollout of 5G[10]. There are initiatives in Europe via university and industry research to develop and produce 5G components "made in Europe"[11].

3.6. Software trends

With new technologies also new software trends are coming up. The so-called App-world, i.e. applications for smart devices like smart phones, required new software development environments. Platforms like github[12] or nmp[13] and others provide building blocks which can even be loaded at runtime. This is a nightmare for security experts because the question is: how to avoid the injection of malware in app stores or how to ensure the integrity of software downloaded from platforms. In addition the software complexity is increasing and the correctness problem comes on top.

Other examples are automatic programming, natural language processing, or using the blockchain technology.

3.7. Data Science

Big Data is currently a buzz word. The availability of, from a user perspective, unlimited computer power and data storage by cloud services allows applications which were not possible a decade ago. The research in the area of data mining and data analytics is becoming mainstream.

[10] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123
[11] https://ec.europa.eu/digital-single-market/en/towards-5g
[12] https://github.com
[13] https://www.npmjs.com

3.8. Artificial Intelligence (AI)

AI is the simulation of human intelligence processes by machines, especially computer systems. These processes include learning, reasoning and self-correction. AI was a hype in the 1970s. But the "valley of tears" followed a decade later, because promises could not be fulfilled. Today AI is becoming part of our daily life in today smart home systems or bots replacing humans in call centers. We are still at the beginning. Self-driving cars have been a buzzword in the AI industry. But the development of autonomous vehicles will definitely revolutionaries our transport systems.

As usual when new technologies are put into consumer products, companies focus on fancy functionality. Privacy and security are primarily seen as a cost factor. Thus, we need Cybersecurity research e.g. in the area of privacy enhanced technologies. Other research topics are validity, traceability, integrity/correctness of results.

3.9. Biometrics

Around 2005 there was a big discussion about putting digital fingerprints, which were usually taken only from criminals, and digital pictures of our faces into electronic Identity cards or passports[14]. 10 years later fingerprint sensors and face recognition are commodity in smart phones. But with new algorithm facial recognition can be spoofed and hacked[15]. The Biometrics Laboratory[16] evaluates the reliability of biometric technologies in real operational conditions with real biometric datasets, and to identify best practices in their deployments.

3.10. Robotics

Modern manufacturing plants can only be run economically when automation is brought to the maximum possible level. Thus, robotics is the core element of todays industry 4.0[17]. New technologies like 5G allow the dislocation of manufacturing

[14] https://www.tagesspiegel.de/politik/sicherheitsplus-oder-gefahr-fuer-den-buerger/655386.html
[15] https://securitytoday.com/articles/2019/03/01/the-flaws-and-dangers-of-facial-recognition.aspx
[16] https://ec.europa.eu/jrc/en/research-facility/biometrics-laboratory
[17] https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution

machines, because of the low latency 5G communication possibility. But when machines are not secured in a plant with fences, availability and integrity, the core Cybersecurity elements, become essential. Industry 4.0 cybersecurity is therefore a hot research topic.

3.11. Summary of emerging technologies

Our today's private and business life depends in an essential way on the confidentiality, integrity and availability of digital products and services.

The above examples show the rapid technological evolution where university and industry research are the foundation of new digital products and services. We could list here much more examples. The intention of this paper is to give the reader an idea about today's emerging technologies and their implication for the Cybersecurity in our daily digital life.

4. Cybersecurity Challenges and Research

As mentioned above the three Cybersecurity elements confidentiality, integrity and availability are essential in our digital society. The security of our information is fundamental and as the digital transformation takes place, our lives become more exposed to cybersecurity threats.

New challenges to Information Security and Cybersecurity are evolving responses from new technologies and new business models. We see risks like:

- Key risks result from increasing systems complexity! Mastering complexity is he challenge.
- Technical risks to guarantee system resilience and interoperability.
- Social risks of technological developments like the above mentioned.
- Ethical risks for advanced ICT design, development and deployment.
- And not to forget normative aspects and regulatory frameworks in the global Cyberspace.

The European Union agency for Cybersecurity ENISA published a report on European research and development priorities in Cybersecurity based on desktop research and interviews with Cybersecurity experts [18] . This report looks into cybersecurity threats to our European society in order to identify priorities in cybersecurity research. The objective is to find mitigation measures before those cybersecurity threats materialise.

I will pick up one example of emerging technologies which will also change today's Cybersecurity paradigm: quantum technologies.

In the 1920s physicists had developed the laws of quantum mechanics[19] which are the basis of modern technologies like electronics, digital technologies, lasers (CD-player), mobile phones, satellites, televisions, nuclear technologies, modern chemistry, medical diagnostics, just to name a few. Today we are talking about the second quantum revolution.

The phenomenon of entanglement, which physicists have only really been able to understand in recent years is the basis of quantum computing and quantum communication. The well-known physicist Richard Feynman already in 1981 proposed in a keynote address at the California Institute of Technology the idea of a computer that could act as a quantum mechanical simulator[20]. In 1984 Charles Bennett and Gilles Brassard defined the first quantum cryptography protocol for quantum key distribution[21]. But it needed a couple of decades until quantum computers became available or quantum communication protocols were implemented in large scale experiments.

The impact of scalable quantum computers on security can be divided into two classes:

- Techniques to provide resistance to attacks using quantum computing like *post quantum cryptography (PQC)* or *Quantum Safe Cryptography (QSC)*;

[18] https://www.enisa.europa.eu/news/enisa-news/european-research-and-development-priorities-in-cybersecurity
[19] https://www.britannica.com/science/atom/The-laws-of-quantum-mechanics
[20] The keynote was published in 1982 in the International Journal of Physics, https://link.springer.com/article/10.1007/BF02650179
[21] https://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf

- Techniques taking advantage of quantum effects like superposition, entanglement and uncertainty like *Quantum Key Distribution (QKD)*.

A scalable quantum computer would break the currently used asymmetric cryptosystems based on RSA and elliptic curves. Polynomial time quantum algorithms for factoring RSA modules and calculating the discrete logarithm on elliptic curves have existed since the publication of Shors Algorithm (1994)[22]. Other quantum algorithms such as the Grover search and the Simon problem also have implications for symmetric cryptography, especially for key lengths and operating modes. A detailed report on the status of quantum computer development was published in 2020 by the German federal office for information security BSI[23]. The US National Institute of Standards and Technology NIST has initiated a process to promote, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms[24].

Secure communication over the Internet is an essential prerequisite for trustworthy cooperation in all areas of our society. Applications, data, messages, telephone calls or e-mails must be protected from unauthorized third parties on the Internet. We must invest today in order to be prepared in terms of an appropriate risk management. Research and development are the foundation to be prepared for the "post-quantum era" where powerful, universal quantum computers can practically break all public key encryption and key exchange methods used today. This would affect confidentiality services with a long-term protection requirement, such as the exchange of personal messages, video conferences or online banking, as well as signature certificates with long terms. Quantum Key Distribution QKD (distribution of quantum keys) is a process that uses the physical properties of quantum mechanics to provide two or more parties with a common, secure key for communication. The advantage of the quantum key exchange compared to classic key distribution methods is that the security achieved is based on known physical laws and not on assumptions about the performance of computers and algorithms or the reliability of trusted persons. The security of the various quantum key exchange procedures arises from the fact that

[22] https://ieeexplore.ieee.org/document/365700/authors#authors
[23] https://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer.html
[24] https://csrc.nist.gov/projects/post-quantum-cryptography

an attacker who is eavesdropping on the key transmission is noticed, and even the amount of information he has tapped can be measured[25].

The European Commission and European member states picked up the quantum challenges and launched quantum flagship programs. For example, the European Commission will fund over 10 year at least one billion Euros[26] and the German Ministry for Research invests 650 million Euros for research on quantum technologies[27]. And the universities in Europe will play an essential role in the research of quantum technologies.

[25] https://qt.eu/discover-quantum/underlying-principles/quantum-key-distribution-qkd/
[26] https://qt.eu/about-quantum-flagship/introduction-to-the-quantum-flagship/
[27] https://www.bmbf.de/de/quantentechnologien-7012.html

Cyber Higher Education in Israel - From Cybersecurity to Cyberspace

Tal PAVEL, PhD[1]
Head of Cyber Studies, the Academic College of Tel Aviv-Yaffo, Israel
Talpv@mta.ac.il

1. Introduction

Cyberspace poses many challenges that affect the individual and society as a whole in a wide variety of aspects in every sector or country. Part of the characteristics of cyberspace is that it is innovative and involves modern technology. Besides, it deals with issues related to working procedures and policies as well as the human factor and appropriate training.

Due to cyberspace innovation and crucial impact on a variety of areas of life, the need arises to know this field and its implications on various sectors, and to impart diverse knowledge: general knowledge of cyberspace to the general public, as well as training professionals in various fields. This includes teaching cyber and digital space in a variety of faculties in various academic institutions in order to train qualified personnel in this field, but also an educated public with digital skills, aware of the capabilities that exist in cyberspace and the dangers inherent in it.

This work analyzes the domain of teaching cyber in academic institutions in Israel, by examining the existence of dedicated study tracks in these institutions. This is to answer two research questions: (1) How many and which academic institutions offer dedicated cyber studies programs? (2) What academic cyber studies programs exist and how can they be characterized?

[1] The author wishes to thank Mr Eynan Lichterman, Research & Emerging Technologies, Israel National Cyber Directorate, for his contribution to this study.

2. Methodology

The study examines the extent and type of cyber teaching in designated study tracks in academic institutions in Israel. To this end, double filtering was implemented: (1) The study analyzes only academic cyber studies and avoids cyber studies given by non-academic and private colleges and various business companies. (2) The study analyzes only designated cyber studies programs and avoids individual courses. Besides, the study did not include academic conversion programs, part-time studies, diploma studies, preparatory courses, courses for the general public, academic and non-academic events, cyber competitions, as well as research institutes or cyber laboratories in these institutions. Moreover, this study does not analyze the level of awareness of cybersecurity defence in those academic institutions.

To analyze the cyber education programs in academic institutions in Israel, a process consisting of several stages was implemented: (1) Mapping academic institutions in Israel recognized by the Council for Higher Education and listed on the council's website (https://che.org.il); (2) Creating a unified list of 60 recognized academic institutions; (3) Analyzing their websites to examine the extent of cyber studies programs in each of the academic institutions. Thus, this study relies solely on the information that appears on the websites of these institutions. The findings were verified with the Israel National Cyber Directorate, for validation.

3. Literature review

Various studies have examined the relationship between cybersecurity and academic institutions, alongside various initiatives which worked to create a unified framework for cyber academic studies.

For example, the “Cybersecurity Curricula 2017” initiative of the Association for Computing Machinery (ACM) and the IEEE Computer Society (IEEE-CS) (among others) to form the “Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity” (CYBERSECURITY CURRICULA 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, 2017). This document outlines in detail, alongside the vision of the task force in this area, the “Content of the

Cybersecurity Curricular Framework." This framework consists of several knowledge areas that individually define the areas of knowledge and topics required in the framework of teaching cybersecurity in academic institutions. This is from a variety of non-technological aspects: data security, software security, component security, connection security, system security, human security, organizational security, societal security. This may echo McCumber's model (McCumber, 1991), which sees the ways to maintain information security (confidentiality, integrity, availability) as a complex of three aspects: technology; policy and practice; education, training and awareness. Other government initiatives are those of the National Cyber Security Centre in the UK (National Cyber Security Centre, 2017) and the US Cyber Career Pathways Tool (National Initiative for Cybersecurity Careers and Studies, no date), while academically examining such government initiatives (Wang Ping et al., 2019). However, it should be noted that all these references to cyberspace relate to the aspects of cybersecurity and not to the broad sense of imparting comprehensive and diverse knowledge to the general public about this domain, its characteristics, opportunities and challenges.

Various studies have addressed the level of cybersecurity among academic institutions (Chapman, 2019); the level of senior college leaders' involvement in cybersecurity and their main concerns (Gearhart G. David et al., 2019); the need for cybersecurity awareness in academic institutions and the ways for improvement (Hunt, 2016; Muniandy et al., 2017; Zwilling et al., 2019). This is done, among other things, by training qualified personnel in the cyber field and practical recommendations in this domain, such as the need to integrate cyber teaching in all age groups, including primary and secondary schools (Kay David J. et al., 2012). In addition, various studies examined different issues of cyber teaching and different teaching materials in higher education institutions (Kapitzke, 2000; Said Samuel Essa, 2018; Tims et al., 2009) and different topics that need to be included in such academic studies (Cohen Brian et al., 2018). Another study analyzed the Thailand Cyber University (TCU) as a test case for the application of relevant knowledge (Sombuntham & Theeraroungchaisri, 2006).

4. Findings

The Council for Higher Education in Israel accredited 60 academic institutions: universities – 9; other higher education institutions - funded institutions – 20; other higher education institutions – non-funded institutions – 10; academic colleges of education - 21.

Table 1 lists all 13 academic institutions in Israel that provide dedicated cyber studies programs, indicating the degree (B.A., M.A.) and the name of the program and the department:

Tab. 1. *Cyber Studies in Higher Education Institutions in Israel*

Name of institution	**Undergraduates**		**Graduates**	
	Department	**Program**	**Department**	**Program**
Ariel University	Computer Science	Cyber Program		
Ben-Gurion University of the Negev	Electrical and Computer Engineering	Communication, Information and Cyber		
	Software and Information Systems Engineering	Data Security and Information Warfare	M.Sc. in Information Systems Engineering	Specialization in Cyberspace Security
Bar-Ilan University			M.A in Political Studies	Military and Security studies with specialization in cyber and strategy
			Computer Science	Cryptography and security
	Computer Engineering	Cybersecurity		
University of Haifa	Department of Computer Science	Single major in Information and Data Security		
Tel Aviv Universiy - The Scientific-Engineering Channel	Faculty of Social Sciences	Cyber, Politics and Government Studies	The School of Political Science	M.A. in Cyber Politics and Government
	Electricity-Computer Engineering	Information Security and Cyber track (from the fourth year)		
	Computer science	Focus on Information		

Name of institution	**Undergraduates**		**Graduates**	
	Department	**Program**	**Department**	**Program**
		Security and Cyber		
	Industrial Engineering and Management	A collection of specializations in Information Technologies and Cyber		
Tel Aviv Universiy - The General Channel	Social Sciences (the programs in Economics, Political Science, Sociology and Anthropology and Psychology)	Cyber, Culture and Society Division		
	Humanities (the multidisciplinary program)	Cyber and Information Technologies		
	Law	Cyber Study Program (from the second year)		
The Hebrew University of Jerusalem	Electrical and Computer Engineering	Cluster of computer and cyber systems		
The Open University of Israel	B.Sc. in Computer Science	Specialization in Online Space Security (Cyber Security)		
The Technion – Israel Institute of Technology	B.Sc. in Computer Science	Cyber and Computer System Security Program		
The Afeka Academic College of Engineering	B.Sc. in Software Engineering	Specialization in Information Security and Cyber		
The Academic College of Tel Aviv-Yaffo	B.Sc. in Information Systems	Cyber Studies		
Lev Academic Center	B.A in Software Engineering	Cyber specialization	M.Sc Data Mining	Specialty methods for identifying cyber attacks
Netanya Academic College	B.Sc in Computer Science and Mathematics	Cyber division		
Interdisciplinary Center Herzliya	B.Sc in Computer Science	Network-Era Security Systems		

The following findings emerge from the data:

Academic institutions

- Universities - 8 out of 9 universities in Israel offer a dedicated cyber studies program (marked green in the table).
- Other higher education institutions - funded institutions - 3 out of 20 of such institutions offer a dedicated cyber studies program (marked in light blue in the table).
- Other higher education institutions – non-funded institutions - 2 out of 10 of such institutions offer a dedicated cyber studies program (marked in orange in the table).
- Academic Colleges of Education - None of the 21 colleges of education offer a dedicated cyber study program.

Education programs

Degrees - 8 academic institutions offer cyber studies program as part of B.A. studies. Only 4 institutions offer such program as part of M.A. studies.

Departments - Apart from Tel Aviv University's "General Channel," which consists of cyber courses in social sciences and humanities, all undergraduate cyber courses in academic institutions in Israel are taught in departments of Computer Science, Information Systems, Software Engineering or Industrial Engineering and Management.

However, out of four cyber studies programs in the master's degree, two are studied in the departments of Political Science, related to the fields of military, security, government and politics, while the two other programs are part of the departments of Information Systems Engineering and Data Mining.

5. Conclusions

The analysis of the findings enables us to draw the image of cyber education in academic institutions in Israel regarding dedicated cyber studies programs in these institutions. Thus, it is possible to draw several conclusions as well as answer the two research questions underlying this study.

The findings indicate that cyber studies programs are offered by 8 out of 9 universities and 5 out of 30 academic institutions designated by the Council for Higher Education in Israel as "other higher education institutions."

But the cyber domain is not included in any of the academic colleges that train the future generation of teachers and educators in Israel (0 out of 21 academic colleges of education) (Research Question 1 - How many and which academic institutions offer dedicated cyber studies programs?).

The findings also indicate that the academic point of view of the cyber domain is mostly security, whether as part of technological studies, in most cases as part of undergraduate studies, or in security-military aspects as part of a master's degree.

It is worth mentioning the Tel Aviv University activities in cyber studies programs, where two different cyber tracks are available: the science-engineering track, and the general track, where cyber programs are available in various social sciences and humanities departments. Therefore, Tel Aviv University is an exception that should be adopted by other academic institutions as a model (Research Question 2 - What academic cyber studies programs exist and how can they be characterized?)

The cyber domain is related to every area of our modern lives and affects them in a real, immediate and far-reaching way, besides being a space based on technology. Thus, the expectation is that cyber study programs will be taught in a greater number of academic institutions, with an emphasis on academic colleges. It is also necessary to develop dedicated courses for cyber studies in departments that do not only deal with technology. In this regard, dedicated programs must be established for cyber-related teaching as part of multidisciplinary studies and in the faculties of Humanities and Social Sciences, where the emphasis will be placed on relevant aspects in the cyber domain.

In addition, it is mandatory to teach cyber-related topics in a professional and dedicated manner in education-related academic institutions while training teachers and educators not only to teach cyber as a technological profession but also to impart knowledge to various audiences in the general public about cyberspace, its characteristics, opportunities and dangers.

This study was intended to describe the state of cyber studies as appearing in dedicated programs in academic institutions in Israel. Further research will be able to delve deeper and analyze the cyber courses taught in these institutions and the syllabi. However, such a study would require a preliminary definition of what is cyber and which topics are part of cyberspace. This should be done by analyzing cyber-related topics taught in academic institutions around the world. Facing these difficulties in classifying cyber-related topics, such further research will be able to define more precisely academic institutions of cyber studies in Israel, at the level of academic institutions and the topics studied in these institutions as well.

It is necessary to act towards imparting knowledge on various aspects of cyberspace and not only the technical aspects related to the security of cyber, information and operating systems against various attacks, or military-security affiliation to cyberspace. Teaching cybersecurity areas is indeed necessary for training experts and professionals, mostly technological, who will be able to cope with cyberattacks and incidents whose frequency and intensity is increasing daily. However, this narrow view ignores many aspects related to cyberspace that affect our lives daily and are not necessarily related to information security and systems. Therefore, we must work to ensure that cyber studies in academic institutions in Israel will deal with cyberspace and not just cybersecurity.

References

[1] Chapman, J. (2019). *How safe is your data? Cyber-security in higher education*. https://www.hepi.ac.uk/wp-content/uploads/2019/03/Policy-Note-12-Paper-April-2019-How-safe-is-your-data.pdf.

[2] Cohen Brian, Albert Michelle G, & McDaniel Elizabeth A. (2018). The Need for Higher Education in Cyber Supply Chain Security and Hardware Assurance. *International Journal of Systems and Software Security and Protection (IJSSSP*, *9*(2), 14–27.

[3] *CYBERSECURITY CURRICULA 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. (2017). 1–123. https://doi.org/10.1145/3184594.

[4] Gearhart G. David, Abbiatti Michael D, & Miller Michael T. (2019). Higher Education's Cyber Security: Leadership Issues, Challenges and the Future. *International Journal on New Trends in Education and Their*, *10*(2), 11–17. http://pkim.pps.uny.ac.id/sites/pkim.pps.uny.ac.id/files/7%20ijonte_2019.2.complete.pdf#page=18.

[5] Hunt, T. (2016). *Cyber Security Awareness in Higher Education*.

[6] Kapitzke, C. (2000). Cyber pedagogy as critical social practice in a teacher education program. *Teaching Education*, *11*(2), 211–229. https://doi.org/10.1080/713698968.

[7] Kay David J., Pudas Terry J., & Young Brett. (2012). Preparing the Pipeline: The U.S. Cyber Workforce for the Future. *Defense Horizons*, *72*, 1–16. https://apps.dtic.mil/sti/pdfs/ADA577318.pdf.

[8] McCumber, J. R. (1991). Information Systems Security: A Comprehensive Model. *14th National Computer Security Conference*, 328–337. https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1991/10/01/proceedings-14th-national-computer-security-conference-1991/documents/1991-14th-NCSC-proceedings-vol-1.pdf.

[9] Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. *Journal of Information Assurance &*, *2017*, 1–13. https://doi.org/10.5171/2017.800299.

[10] National Cyber Security Centre. (2017, August 9). *NCSC-certified degrees*. https://www.ncsc.gov.uk/information/ncsc-certified-degrees.

[11] National Initiative for Cybersecurity Careers and Studies. (n.d.). *Cyber Career Pathways Tool*. Retrieved October 17, 2020, from https://niccs.us-cert.gov/workforce-development/cyber-career-pathways.

[12] Said Samuel Essa. (2018). *Pedagogical Best Practices in Higher Education National Centers of Academic Excellence / Cyber Defense*

Centers of Academic Excellence in Cyber Defense. https://search.proquest.com/openview/cf4fc1b4c2c77a6c0b2cf927ca3ce77f/1?pq-origsite=gscholar&cbl=18750&diss=y.

[13] Sombuntham, S., & Theeraroungchaisri, A. (2006). *Thailand Cyber University: The Strategic Move to Higher Education Reform*. https://www.researchgate.net/profile/Supannee_Sombuntham/publication/265668124_Thailand_Cyber_University_The_Strategic_Move_to_Higher_Education_Reform/links/54c9a3a20cf2807dcc277120/Thailand-Cyber-University-The-Strategic-Move-to-Higher-Education-Reform.pdf.

[14] Tims, H., Turner, G., Duncan, C., & Etheridge, B. (2009). Work in progress - Cyber discovery camp integrated approach to cyber studies. *Proceedings - Frontiers in Education Conference, FIE*. https://doi.org/10.1109/FIE.2009.5350510.

[15] Wang Ping, Dawson Maurice, & Williams Kenneth L. (2019). Improving Cyber Defense Education Through National Standard Alignment: Case Studies. *National Security: Breakthroughs in Research and Practice*, 78–91.

[16] Zwilling, M., Lesjak, D., Natek, S., & Anussornnitisarn, P. (2019). How to Deal with the Awareness of Cyber Hazards and Security in (Higher) Education? *Management, Knowledge and Learning International Conference 2019*, 1–7. http://www.toknowpress.net/ISBN/978-961-6914-25-3/papers/ML19-130.pdf.

Cyber Law.
How to Upgrade Knowledge at the University Level: Building the New Generation of Cyber Professionals

Dr. Nathalie RÉBÉ
Université de Bourgogne Franche-Comté, France
nathalie_rebe@etu.u-bourgogne.fr

1. Introduction

Cyber law shares an important place in the cybersecurity and privacy landscape. Often undertrained on this key topic, information technology (IT) and computer sciences (CS) students lack the right tools to protect themselves, their inventions, and others in a work-related setting. The European Union has enacted legislations to safeguard information technology and computer systems, as well as data and business transactions. However, several regulatory issues remain due to the cross-border aspect of cyber matters. As technology has evolved exponentially since the 80s, so have cybercrimes. As the demand for cyber experts in the workplace grows, cyber professionals will need to acquire more focused legal tools within their university curricula to compete with skilled cyber criminals so as to be able to protect companies, organisations and individuals' systems as well as their information from cyberattacks.

2. Cybercrimes

Cyber law pertains to the legal practices relating to the internet, networks, as well as computer hardware and software. While these cybercrimes are perpetrated online, their impact is on the physical world. Cybercrimes covers a wide range of illegal activities, from intellectual property theft, unlawful data access or usage, cyber-attacks, fraud, cyber-terrorism, money-laundering, bullying, forgery, defamation, piracy, scams, child pornography, to human trafficking, among others.

Some cybercrimes are driven by financial motivation, whereas others are aimed at creating panic and disruption to their target's data and/or systems. The cyberworld is, then, a platform which enables physical crimes to take place. The dark web, being the most infamous example of a criminal networking platform, is where people can purchase illegal items, such as weapons or pursue illegal other activities. By studying cyber law, students can acquire the necessary knowledge to understand online criminal activities' investigations and prosecution mechanisms.

3. EU Cyber Security

Cyber security refers to the protection and recovery of networks, programs, electronics, computers and mobile devices from malicious cyberattacks targeting individuals, networks and businesses designed to access, change or delete data, extort money, steal intellectual property, or confidential information, or simply interfere with business activities.

Cyber security is aimed at recognising, preventing, fighting and/or limiting vulnerabilities, identifying potential security breaches and cyber-attacks as well as developing strategies for avoiding future violations. Unauthorised usage of computers and accounts, wireless intrusions, and insider threats, are current pressing cybersecurity menaces, which can take the form of: viruses, worms, Trojan horses, malware, ransomware, social engineering, advanced persistent threats (APTs) and control system attacks, such as denial of service (DoS).

There are numerous cybersecurity measures available to prevent cyberattacks. However, cyber-professionals are continuing to be very frequently challenged regarding the protection of infrastructure, network security, application' security and design, cloud security, user account identification and management, end-user education, data loss prevention as well as fraud, process and policy creation.

To date, 72% of counties worldwide have developed their own laws to pursue cyber-crime according to UNCTAD[1]; however, regrettably, cyber legislations differs

[1] UNCTAD. 'Data and privacy unprotected in one third of countries, despite progress'. April 29, 2020. Available at https://unctad.org/news/data-and-privacy-unprotected-one-third-countries-despite-progress (accessed October 16, 2020).

between countries. The European Union has created its own cybersecurity regulations to be incorporated into its members national laws. There are three main regulations within the EU which are part of the Digital Single Market strategy[2].

- The Network and Information Systems (NIS) Directive[3], which came into effect in August 2016 and involves digital service providers (DSPs) and operators of essential services (OESs) in the EU engaged in critical societal or economic activities.
- The Regulation 2016/679[4] of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, also called the General Data Protection Regulation (GDPR). This came into force on May 25, 2018, thus repealing Directive 95/46/EC[5]. The GDPR regulates data protection rights and obligations.
- The EU Cybersecurity Act[6], which came into effect on 27th June 2019, establishes an EU-wide cybersecurity certification framework for digital products, services and processes. This has reinforced the previous mandate of the EU governing agency, namely the European Union Agency for Cybersecurity (ENISA). Until now, ENISA initiatives have included an EU Cyber Security Strategy, the EU Cloud Strategy, and Open Standards in Information Communications Technology.

[2] European Commission. 'Building strong cybersecurity in the European Union: resilience, deterence, defence'. June 5, 2019. Available at https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence (accessed October 16, 2020).

[3] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (2016). Available at https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed October 16, 2020).

[4] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (2016). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC#_blank (accessed October 16, 2020).

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (1995). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A31995L0046&from=FR#_blank (accessed October 16, 2020).

[6] Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), (2019). Available at https://eur-lex.europa.eu/eli/reg/2019/881/oj (accessed October 16, 2020).

4. EU Data Privacy

The Internet is subject to conventional laws with regards to intellectual property and transactions, yet great concerns arise with the increasing use of algorithms, IOT and AI into our daily lives that can intrude in our homes. That is, our privacy is under threat in terms of our conversations being listened to, our location being uncovered and our everyday actions being tracked. In the age of new technologies, privacy is a luxury.

The European Union (EU) and the United Kingdom (UK) enacted data protection regulations concerning restrictions on the collection, storage and use of personal data for businesses, public bodies and other organisations in 2018, which are provided under the EU General Data Protection Regulation[7] (GDPR), and the UK Data Protection Act.[8] EU Data Protection regulations cover new data protection rights and obligations, the processing of personal data and offer increased security measures for intellectual property[9] as well as encompassing unfair competition concerns. The protection of the GDPR applies to individuals and businesses located in the EU that offer goods or services to persons in the community. The GDPR has an extra-territorial effect, as it also places obligations on organisations that operate outside the EU that offer goods or services to individuals in the EU and/or monitor the behavior of data subjects living in the EU.

In business, unauthorised access, use, change, disclosure and deletion of data is currently very common. The GDPR offers individuals more extensive control over the disclosure of their personal data (names, email addresses, social media, IP addresses, financial information, and more). Six key fundamental data protection principles that businesses and organisations must comply with when they collect, process and store individuals' personal data are provided by Article 5 of the GDPR. Specifically, personal data must be lawful, fair and transparent, purpose limitation, data

[7] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (2016). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC#_blank (accessed October 16, 2020).

[8] UK Data Protection Act (2018). Available at https://www.legislation.gov.uk/ukpga/2018/12 (accessed October 16, 2020).

[9] Intellectual property rights include copyright protection, patents, trademarks, protection of databases, as well as data protected as trade secrets.

minimisation, accurate, storage limitation, have integrity and be confidential, according to Article 5.1 of the GDPR.[10] Controllers are also responsible for ensuring compliance with the GDPR's principles under Article 5.2 of the legislation.[11] New data protection concerns raised by social media and digital platforms, cloud computing, and automated decisions have also been incorporated in the GDPR. The legal principles offered by the regulation consist of the right to access information (art.15), the right to data portability (art.20), right to consent (art.7), the conditions applicable to a child's consent in relation to information society services (art.8), right to rectification (art.16), right to erasure (art.17), and automated decision-making (art.22).

The United Kingdom 2018 Act of the Parliament national law on Data Protection[12] incorporated the GDPR directly into domestic law after the UK exited the EU. The Act implements the processing of personal data and incorporates new offences, such as selling, or offering to sell, personal data knowingly or recklessly obtained or disclosed, knowingly or recklessly obtaining or disclosing personal data without the consent of the data controller, and the retaining of data obtained without consent.[13]

Additionally, the ePrivacy Regulation, or so-called Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)[14], was planned to be repealed by the Proposed regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications [15] starting 25 May 2018. While still under discussion, this new legislation is meant to apply any business that processes data in relation to any form of online communication service that utilizes online tracking technologies, or engages in

[10] GDPR, Article 5.1.
[11] GDPR, Article 5.2.
[12] UK Data Protection Act (2018). Available at https://www.legislation.gov.uk/ukpga/2018/12 (accessed March 16, 2020).
[13] UK Data Protection Act (2018), Part 6- Offences relating to personal data, 170-173. Available at http://www.legislation.gov.uk/ukpga/2018/12/part/6/crossheading/offences-relating-to-personal-data/enacted, (accessed October 16, 2020).
[14] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), (2002). Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 (accessed October 16, 2020).
[15] EU Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), (2017). (2002). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=SL (accessed October 16, 2020).

electronic direct marketing, and focuses on cookies, as well as on the confidentiality of communications, electronic consent, and privacy.

5. Regulatory issues

Whilst there have been many collaborative efforts between countries and the private sector to improve cybersecurity and privacy laws, the underregulated vast cyberspace does not provide a sufficiently strong common legislative framework for safeguarding infrastructures and individuals at the international level. This opens the door to criminals as enforcement and punishments has become more complex following the *nulla crimen nulla poena* legal principle. Cybercrimes involve cyberspace, which leads to jurisdictional issues as the cyber world allows cross-border transactions and activities. As it is impossible to sue someone in cyberspace, a physical court needs to held cases. However, the plurality of jurisdictions and regulations regarding online activities makes the determination of subject matter jurisdiction and punishment complicated. The anonymity offered by the internet makes it hard to collect all the necessary evidence and connect it to individuals. The establishment of a permanent Cyber Tribunal similar to existing special international crimes tribunals at the Hague has been pushed for by many lawyers and scholars. This would require the mandating of states parties to an annexed convention regulating cyber-matters as an effective means of judgement of cybercrime.

6. Career Opportunities

Information technologies and computer sciences are a growing field of interest for students as new categories of work emerge in this field, which offer competitive salaries. Education in cyber law will be in high demand as more businesses become engaged in lawsuits or subject to legal difficulties, with the attendant necessary paperwork. Mitigating cybersecurity risks requires a good knowledge of the law of different countries. Regulatory change impacts on organisations as security policies and internal controls are driven by international guidelines, which constantly need updating. As there is a lack of competent jurists in this field, since there are too few

educational cyber law programmes, cyber-professionals will need to know cyber law well in order avoid experiencing trouble in the area of policy creation, intellectual property, and safeguard on the behalf of their organisation. Graduates in cybersecurity and cyber law could seek careers in police and military environments, internet providers and telecom companies, as well as business and consulting. Compliance, information security, risk, and cyber-engineering have so far been the preferred vocations for cyber experts.

7. Coursework Recommendations

Cyber security programmes should incorporate international best practices, policies and regulatory knowledge, business and management strategies and governance structures, thus a robust understanding of the future work environment. IT law requirements for university students will need to include modules such as the following: 'Introduction to crypto law"; "The evolution of international cyber regulatory practices by country", "Cybercrimes" and "Cyber laundering regulations and practices". Given project management and analytics are requirements for cyber-professionals, legal and incident risk management measures relating to cyber breaches are important tools that need to be added to the university curriculum. The importance of "Cyber Incident Risk Management" must also be promoted in classrooms as decisions must often be taken rapidly to ensure safety. Risk management involves administrative and legal knowledge, as well as practical. Security tools are essential for organisations as they help prevent, identify, and fight cybercrimes. Given intellectual property and privacy are key elements in data protection and transfers, "Privacy law", and "Data protection" courses should be offered to students as part of their cyber educational programmes. "Cyber business and contracts law" could be interesting electives with many cyber professionals orientating their career to business, as well as consulting is the future.

The potential dangers of "New technologies" and the inherent new legal threats that derive from them must be understood by future cyber-professionals. These technologies include matters such as the Big Data, Deep Learning, blockchain, AI, IOT,

biometry, and face recognition. "Automated decision-making legislations and cases" should be a particular concern as Artificial Intelligence (AI) is already able to establish e-contracts and advertising, which should spur greater responsibility on the behalf of humans, in particular, given AI's ever-increasing progress. The "Cloud regulatory framework" must also be a topic fully understood by future experts. Soon enough, Virtual Reality (VR) will require international regulation and will also need to be studied by professionals.

8. Conclusion

The lack of strong regulatory measures and skilled professionals in the cyber domain will have a negative impact on privacy and international security. The field of cybersecurity requires constant re-regulation and overwatch, which is expensive and procedure-wise, very time consuming. Building new experts in cyber law is therefore crucial to assist in creating and updating regulations. Current university level courses lack content that requires investigating worldwide cyber laws. The lack of professors with dual expertise can explain why knowledge is often compartmentalised when delivered in classrooms/lecture theatres. Most IT experts learn more at work than they did in formal education; however, the addition of basic legal competencies within school/university curricula would enhance their capacity to strengthen international security. In addition to mastering technology being important, so too is providing students with understanding of the means of regulating intangible crimes, where cooperation is needed between jurists and cyber experts. Only those with expertise in law and technology can constantly keep track of new crimes and technological issues encountered at the practical level, for such people cannot only understand the field, but also, recognize the illegal threats encountered.

A Model of International Cooperation: CyberEDU 202X

Daria CATALUI
University of Lancaster, United Kingdom
daria.catalui@protonmail.com

1. Introduction

This article speaks to practitioners interested in applying effective models of international cooperation. The test aims to promote cyber education by developing programs in a public-private partnership.

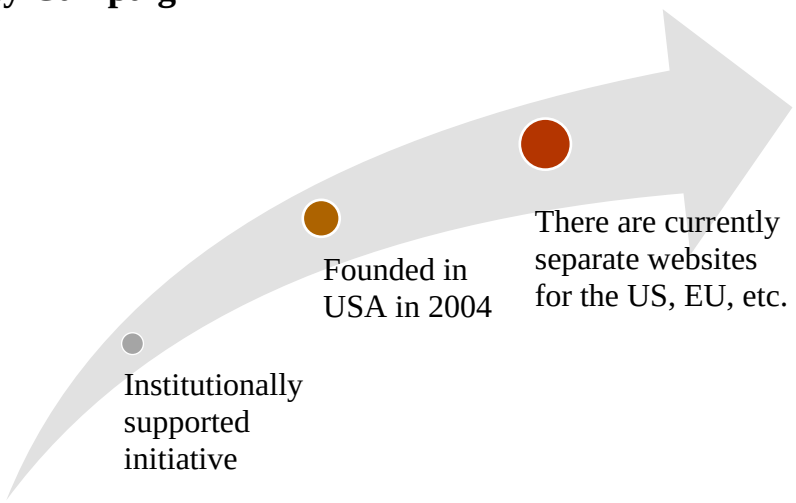
2. Context

Do you think there is a solution that can meet all needs? Probably not, but I believe that there are models that work properly and that can inspire any professional in the field of cyber education. I will try to present these models from the practitioner's angle of analysis. These are:

- The model of global cooperation underlying the *Cyber Security Awareness Month* advocacy campaign.
- The model of European cooperation underlying the *European Cyber Security Challenge*.
- The model of global cooperation underlying the *Safer Internet Day*.
- The model of global cooperation underlying the *Girls in ICT Day*.
- The model of European cooperation underlying the *Code Week*.
- The model of global cooperation underlying the *Data Protection Day*.

In conclusion, I will present a common cooperation format, named in the context of this article: *CyberEDU 202X Cooperation Model*.

The Model of Global Cooperation Underlying *the Cyber Security Awareness Month* Advocacy Campaign



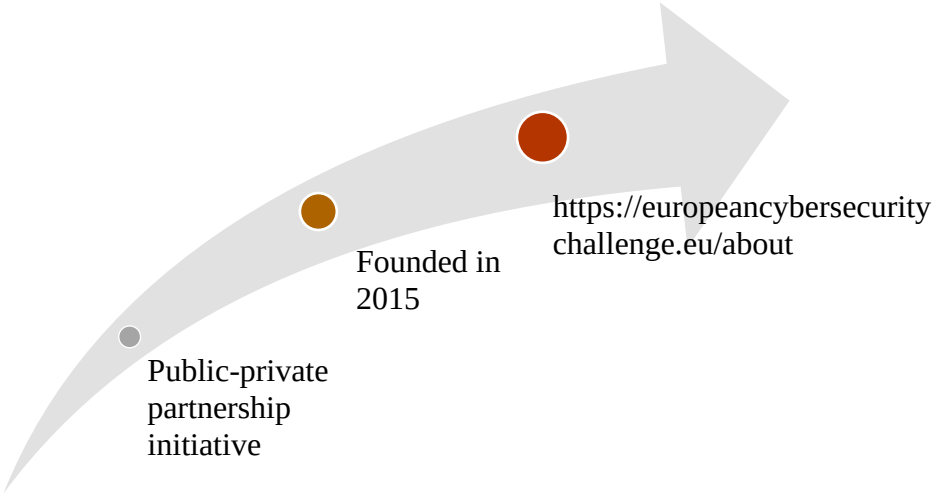
This initiative was created following a public-private partnership between the US Government and a Washington-based Association, to be developed progressively in the US by involving representatives of Silicon Valley technology companies, then internationally through government partnerships and events as the Internet Governance Forum.

In the European Union, the transatlantic partnership was only established in 2010, when the strategy mentioned cooperation for advocacy month and the organization of cyber exercises. In Europe the campaign grew step by step, in 2011 a feasibility report was published, in 2012 a pilot was organized, then in 2013 more than 20 countries were involved.

After several editions, the campaign is already growing exponentially, following the well-established steps from the first edition in 2013, namely: country coordinator, activities in a public-private partnership, frequent online meetings between the main actors. It is important to add that partners are supported by advocacy and lobbying, intangible means.

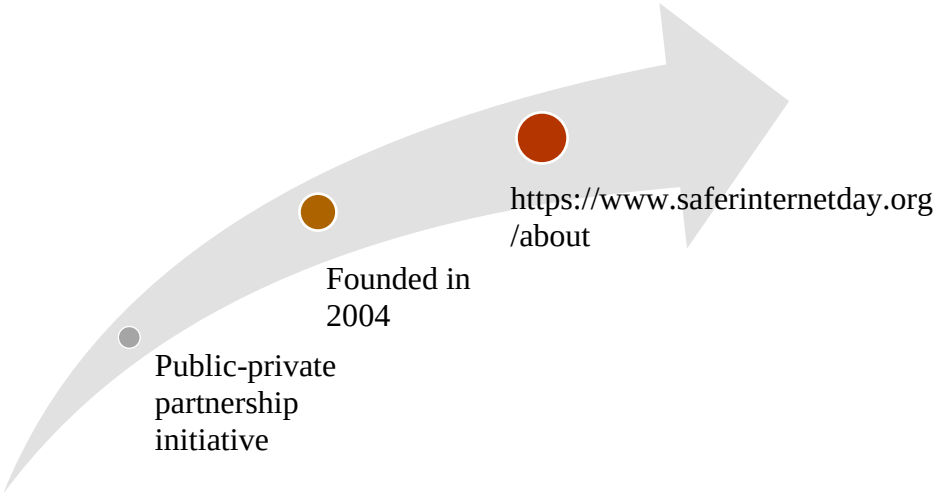
In this case, the main advantage is the mention of this initiative in the European cybersecurity strategy of February 2013, being a defining element for implementation at the European level.

The Model of European Cooperation Underlying the *European Cyber Security Challenge*



This initiative also implemented in public-private partnerships has been difficult to initiate considering factors such as a rich market of cybersecurity companies. These companies were/are very active and interested exclusively in attracting new talent. After difficult coordination at the beginning, at this moment the initiative has become a great success, supported by an increasing budget. I will highlight two aspects: the public partnership has brought coherence in the coordination of the actors present and the coordination with the public policies in the field. Then private organizations were motivated to create the advanced digital skills that the market/companies need.

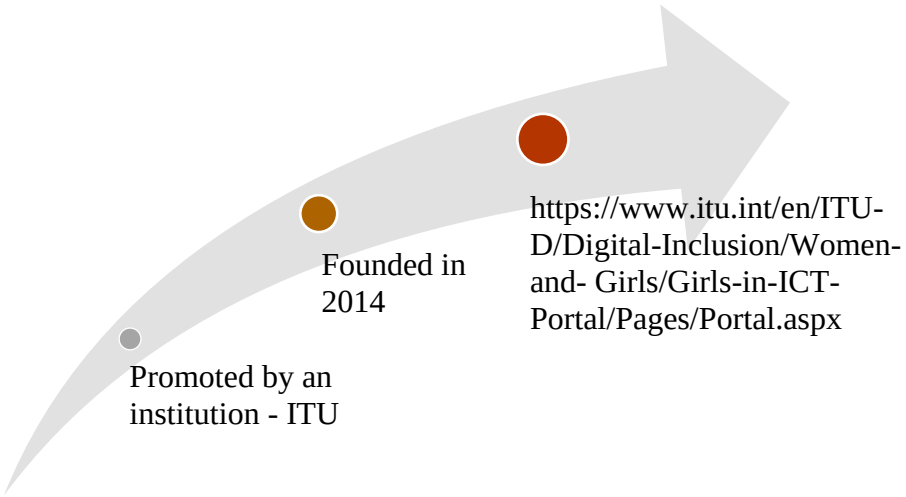
The Model of Global Cooperation Underlying the *Safer Internet Day*



This initiative has developed at an impressive pace being initiated by an academic project funded by the European Union. It has now surpassed any pre-established success indicator and is a global initiative for specific online education

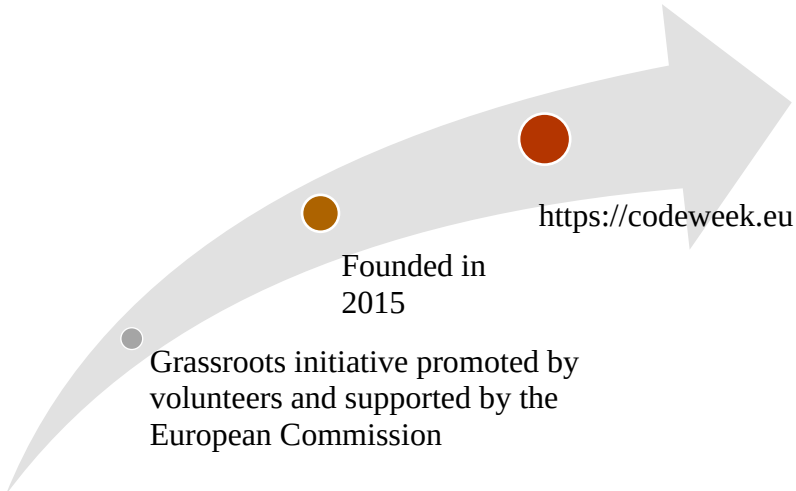
activities. I think it is important to mention the support received by an academic network of teachers, the central coordination by a single team.

The Model of Global Cooperation Underlying the *Girls in ICT Day*



For the present model, two aspects are of interest for this article. First of all, the institutional effort to promote the initiative. Secondly, the involvement focused on ITU member countries. Statistics show that the initiative is growing in support, but my observation is that the goal or mission stated from the beginning changes along the way. At present, the promotion of ICT among girls is a global mission, without geographical or economic correlation for the target audience.

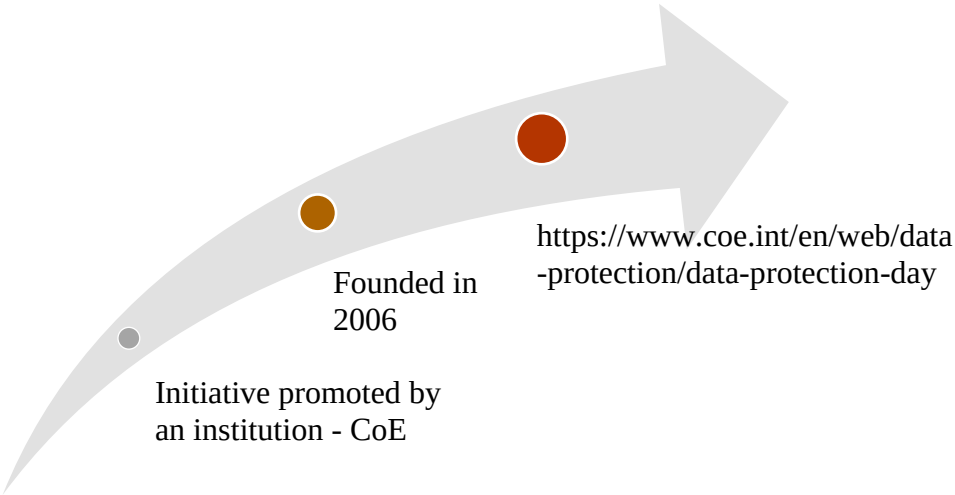
The Model of European Cooperation Underlying the *Code Week*



This initiative launched at the European level and turned international movement started in 2013 in a working meeting on institutional dialogue. The Young Advisors

network convened by the European Commissioner for Digital Agenda Europe was the perfect laboratory. The European Commission has supported this idea through multi-annual planning and freedom of implementation for all volunteers involved. Also, since the first editions, the initiative has benefited from ambassadors for each country involved, which contributes to increasing motivation and involvement. Another strength of the initiative I believe is the decentralization of coordination. This element significantly increases involvement but loses the common structure of activities.

The Model of Global Cooperation Underlying the *Data Protection Day*



In the context of this initiative, it is worth noting the correlation of the project with the existing public policy strategy. Celebrated every year in January, the initiative has grown in importance with the adoption of the GDPR in the EU and beyond. But the campaign is not backed by central coordination or relevant educational resources.

3. Conclusion

By presenting these examples offered by the international cybersecurity landscape, I want to highlight the differences and similarities between them.

The basic model that works efficiently is not necessarily promoted by the abundant financial resources of a single actor, but rather by a content strategy and a coordination model for the actors involved. The steps to follow in developing good international cooperation in the field of cybersecurity education or CyberEDU 202X are:

1. Plan a strategy with measurable objectives and communicate the same message to all actors involved. One coordinated voice!
2. From one edition to another, it improves the educational content and the participation of the interested actors. Encourages partnerships of any kind!
3. Improves interaction through flexible coordination. Give the right to action to every actor involved!

References

[1] Cyber security month USA [Online]. Available at https://web.archive.org/web/20140731143707/http://www.staysafeonline.org/ncsam/about, [Accessed on 5/11/2020].

[2] Cyber security month UE [Online]. Available at https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month, [Accessed on 5/11/2020].

[3] Cyber security challenge UE [Online]. Available at https://europeancybersecuritychallenge.eu/about, [Accessed on 5/11/2020].

[4] Safer Internet Day [Online]. Available at https://www.saferinternetday.org/about, [Accessed on 5/11/2020].

[5] Girls in ICT Day [Online]. Available at https://www.itu.int/en/ITU-D/Digital-Inclusion/Women-and-Girls/Girls-in-ICT-Portal/Pages/Portal.aspx, [Accessed on 5/11/2020].

[6] EU Code Week [Online]. Available at https://codeweek.eu/, [Accessed on 5/11/2020].

[7] Data Protection Day [Online]. Available at https://www.coe.int/en/web/data- protection/data-protection-day, [Accessed on 5/11/2020].

Perspectives Regarding the Application of the Principles of Ethics and Integrity in Cyberspace

Lisa Maria ACHIMESCU, PhD
National Defence College, "Carol I" National Defense University
lisa.achimescu@gmail.com

Angela IONIȚĂ, PhD
„Mihai Drăgănescu" Research Institute for Artificial Intelligence
aionita@racai.ro

1. Introduction

Our behavior when accessing the digital universe undergoes constant metamorphosis, as those who access the Internet are ceaselessly changing and the role that the Internet plays in our lives increases exponentially. In 1995, only 1% of the world's population had access to the Internet. Nowadays there are over 4 billion Internet users worldwide and this number is growing.[1]

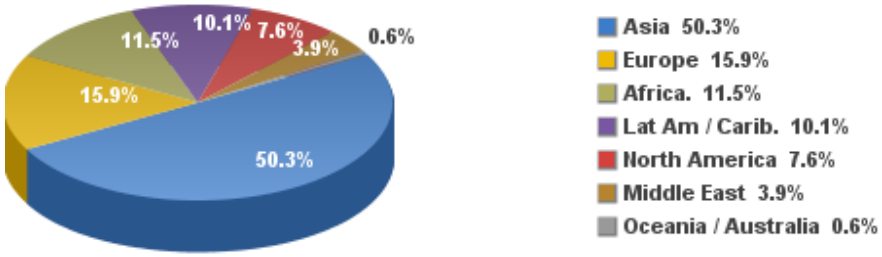


Fig. 1. *Distribution of Internet users worldwide in 2020*[2]

World Regions	Population (2020 Est.)	Population % of World	Internet Users 30 June 2020	Penetration Rate (% Pop.)	Growth 2000-2020	Internet World %
Africa	1,340,598,447	17.2 %	566,138,772	42.2 %	12,441 %	11.7 %
Asia	4,294,516,659	55.1 %	2,525,033,874	58.8 %	2,109 %	52.2 %
Europe	834,995,197	10.7 %	727,848,547	87.2 %	592 %	15.1 %
Latin America / Caribbean	654,287,232	8.4 %	467,817,332	71.5 %	2,489 %	9.7 %
Middle East	260,991,690	3.3 %	184,856,813	70.8 %	5,527 %	3.8 %
North America	368,869,647	4.7 %	332,908,868	90.3 %	208 %	6.9 %
Oceania / Australia	42,690,838	0.5 %	28,917,600	67.7 %	279 %	0.6 %
WORLD TOTAL	7,796,949,710	100.0 %	4,833,521,806	62.0 %	1,239 %	100.0 %

Fig. 2. *World statistics on internet use on the population of 2020*[3]

[1] https://vpngeeks.com/internet-privacy-statistics/
[2] Source: Internet Users Stats, www.internetworldstats.com/stats.htm, Basis: 4,574,150,134 Internet Users in March 3, 2020, Miniwatts Marketing Group
[3] Source: www.internetworldstats.com/stats.htm, Miniwatts Marketing Group

Obs. (1) World statistics on the use of the Internet and on the population shall be made on 20 July 2020;

(2) The population number is based on data provided by the United Nations Population Division (https://www.un.org/development/desa/pd/events/CPD53);

(3) Information on Internet use was taken from Nielsen Online[4], International Telecommunications Union[5], GfK[6], local ICT regulators, etc.

The 2020 new Digital reports - published in partnership with We Are Social and Hootsuite - reveal that digital, mobile and social networks have become an indispensable part of everyday life for people around the world (Kemp, 2020).

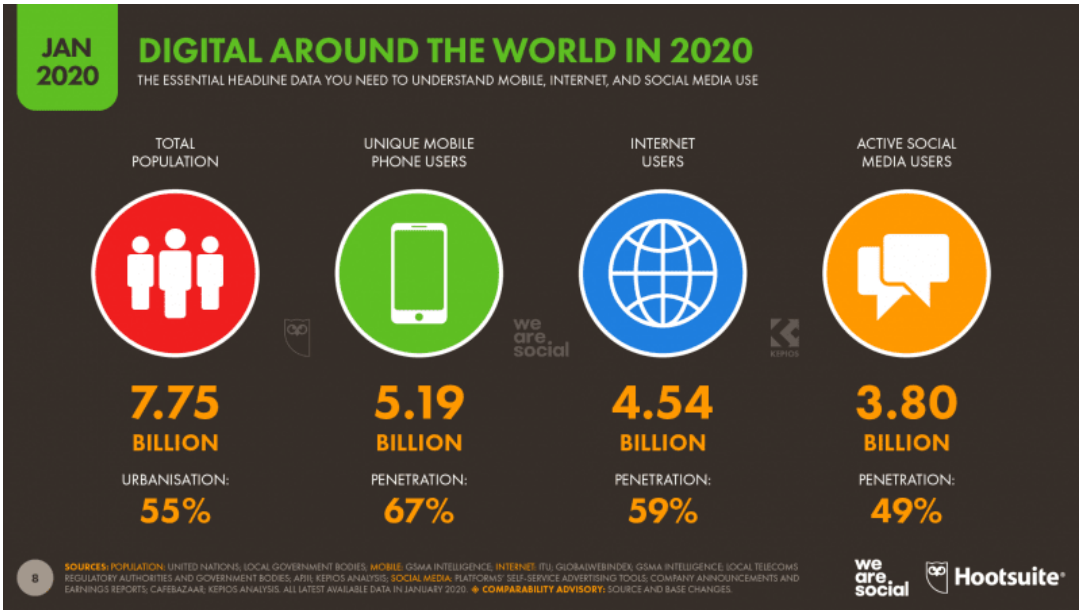


Fig. 3. *The digital universe*[7]

More than 4.5 billion people are now using the Internet, while almost 60 percent of the world's population is already online. Regardless, some important challenges continue to exist as to how everyone has access to and the degree of security of the life-changing digital connectivity.

The crucial role that *cybersecurity* holds in protecting privacy, rights, freedoms, including our physical security, appears to assume an increasingly leading position.

[4] https://www.nielsen.com/us/en/
[5] https://www.itu.int/en/Pages/default.aspx
[6] https://www.gfk.com/home
[7] Source: Kemp, 2020, https://thenextweb.com/growth-quarters/2020/01/30/digital-trends-2020-every-single-stat-you-need-to-know-about-the-internet/

Progressively, as the vital infrastructure remains online and vulnerable to *cyberattacks*, data is being affected by infringements, involving the leakage or breaches of personal information that are becoming alarmingly frequent and by a growing awareness in respect of cyberattacks sanctioned by the state. The substantive relevance of cybersecurity has undoubtedly become a matter of public interest.

2. The characteristics & the technical and legal valences of the cyberspace

The term *cyberspace*[8] has become an everyday platitude, a modern truism. The number of digital platforms users worldwide, known in the English language as *the global digital population*, covers 4.57 billion people, at the time of our present scientific inquiry, representing roughly 60% of the world's population[9]. Assessing trend evolution in this domain since the 2000s up until the present moment emphasized an exponential increase in the number of digital platforms users, with around 950,000 new users per day. It is not an unfathomable perspective that we may witness a completely digitalized world in the horizon of the next 25-30 years and, under no circumstances, this scenario can be attributed to the far-fetched purview of a science fiction narrative.

Universality can be deemed as one of the main characteristics of cyberspace, given that the entirety of the globe has become "*cyber*"[10]: today, all aspects of our lives are dominated by *cyber*. The phenomenon can also be observed in societies previously known as "developing countries", which are embarking the *cyber bubble* due to the remarkably expeditious development of wireless telephone networks. But this accelerated progression is even more manifest in developed societies, where cyber coverage continues to be much more significant and accelerated. Indeed, we cannot equate cyberspace only to the Internet, because all interconnected networks, public or private, regardless of their means of interconnection (wires, fibers, proximity waves, satellite waves, etc.) constitute *the cyberspace*. Computers are, indubitably, an

[8] Cybernetics derives from the Greek *kubernētēs* which refers to a pilot or helmsman. Also related we have the Greek word *kubernēsis*, which means "gift of government" and applies to the notion of leadership. The study of cybernetics involves the fields of computer science, engineering and biology, as well as their advances.
[9] https://datareportal.com/, https://www.statista.com/
[10] Everything related to the internet, viewed from a collective perspective.

important component, but one has to take into consideration other devices such as *smartphones* or private networks of any kind. These different networks coexist, hybridize or isolate themselves, weaving together the all-encompassing complex web of "*cyberspace*" that now organizes and monopolizes our entire existence. As in the case of electricity or cars, there is no turning back.

One needs to reiterate that this *new space* cannot be reduced to computers alone. Cyberspace can be described according to a three folded layered model: a hardware layer (because, despite the emergence of "*virtuality*" (*virtual reality*), cyberspace is based on an extremely dense and often unnoticed physical infrastructure); a logical layer (the computer itself); and a semantic layer, often disregarded, but extremely important (Kempf, 2012). "*Data or information transported*" in cyberspace cannot be considered neutral in its nature: data is "*qualified*", represents information and the manner in which is rendered, as well as the bypath of delivering it, represents an integral part of cyberspace.

Cyberspace constitutes a novel and innovative domain. This truism emphasizes its *anthropic*, terrene and artificial structure, being therefore deeply human, thusly, warranting the inclusion of the social dimension in its analysis.

The social dimension can be furthermore characterized by the inclusion of an increasing number of actors. From a strategic point of view, it cannot be reduced to the traditional actors or to the concept of state power. On the contrary, cyberspace includes, perhaps for the first time in recent history, the individual as a strategic actor. The individual represents an extremely mobile and versatile actor; they can be temporarily or permanently associated, to form circumstantial coalitions or to join structured and clearly defined projects, thus obtaining "*real*" effects, in or due to cyberspace.

Last but not least, given the strategic objectives of actors in cyberspace, two more essential characteristics can be distinguished, which will determine all calculations and evaluations.

Firstly, one has to bear in mind *the principle of non-attribution* (Kempf, 2012). According to the generally accepted opinion, cyberspace is considered to be characterized by absolute transparency, providing immediate access to all data and

information. However, those skilled in this "art" can easily perform *covert, hidden or non-transparent actions* (Kempf, 2012). Cyberspace, despite appearances, constitutes in fact an opaque space in which the connection between such an action (hidden/covert/non-transparent) and its author cannot be inferred. Otherwise stated, a certain actor cannot be easily "*blamed*" (*held liable*) for a cyberattack on another actor. Not being able to identify the *opponent* can be both a huge advantage and a huge hindrance. This anonymity of one's belligerence represents a novelty from a strategic point of view. (Kempf, 2012).

The second essential characteristic of cyberspace constitutes its non-lethality: conflicting actions in cyberspace are not lethal (at least for the time being). Notwithstanding, one of the well-known criteria related to traditional warfare represents the fact that it often results in the death of combatants. The non-lethality of cyberspace means that the actions that take place there "create less noise" (Kempf, 2012) and, especially, do not effortlessly prompt emotional reactions in the media (Kempf, 2012). This illustrates, in fact, another facet of the opacity of cyberspace, stemming from the lack of transparency of the actions that unfold within it.

The first consequence of cyberspace opacity is enhanced leeway in maneuvering of various actors. Mankind underwent a stage in which strategy was mainly defined by means of defense, for several reasons: moral (especially after the catastrophes of the two world wars), legal (according to the United Nations Charter, the only legitimate cause of war represents self-defense), and especially technical, due to the dominance on the international scene of nuclear weapons (Kempf, 2012). This led to a "strategic uprising" which curbed and contained the use of extreme actions. In fact, as Carl von Clausewitz postulated, each and every war is intended to escalate violence (von Clausewitz, 2018). With the development of nuclear energy, this escalation became far too dangerous: taking nuclear action to the extreme meant, in fact, "game over" for all actors involved, so no one gambled the risk of causing a nuclear catastrophe. Thus, contrary to popular opinion, nuclear strategy is not an offensive strategy, but a fundamentally defensive one.

The emergence of cyberspace was a technological event that also changed the "*grammar of war"*, causing a new strategic fracture. Cyberspace is opaque, non-lethal, because the facts occurring there cannot be easily attributed to the actors who generated them, irrespective of whom "had the initiative". The whole world, the actor-state, the group or the individual thus regains freedom of maneuver. *In nuce*, the offensive becomes possible again. However, the return to offensive must be subject to opacity constraints. Basically, cyberspace represents the technological response to the evolutions of asymmetric warfare, in regard to solutions to recent conflicts: cybernetics makes possible the impossible (Kempf, 2012). Basically, *cyber space* allows a kind *conflict re-symmetrization*, because all actors will be able to act in cyberspace (Kempf, 2012).

Cybernetics uses key concepts such as "information and communication technologies" (ICT), "information systems" (IS) or "information technologies and systems" (ITS). Therefore, it is imperative to clearly demarcate these concepts, and, subsequently to specify how the concept of ethics can be understood by applying it to these specific instruments.

First, information and communication technology (ICT) or information technology (IT) generally refers to: "All technological instruments and resources that make it possible to transmit, record, create, share or exchange information, including computers, Internet web sites, blogs and e-mail), technologies and devices for live transmission (radio, television and internet) and time-lapse (podcast, audio and video recordings, recording support) and telephony (fixed or mobile, satellite, video conferencing, *etc.*). "(UNESCO, 2015)[11]

At an organizational level, information systems (IS) are used to designate "all human, organizational, methodological and technical resources of a company, allocated to the acquisition, processing, preservation and dissemination of information necessary for the company's business activities" (Reix, 2002). This definition creates

[11] The UNESCO Science Report: Towards 2030. This report analyzes the main development trends in world science for the last 5 years. It was launched in Paris on November 10, 2015, on the International Day of Science for Peace and Development. The UNESCO Science Report is one of the most important instruments that countries can use to monitor progress towards the 2030 Agenda for Sustainable Development goals.

the possibility of identifying three dimensions of the information systems: the information dimension, the technological dimension and the organizational dimension. As such, the information system includes technological instruments such as IT/ICT, as previously defined. As a consequence, one can refer to information systems based on technological instruments.

Since human interactions began to take place in cyberspace, the issues of regulating the domain from a legal point of view and of creating general legal norms that would regulate domains such as the Internet presented themselves.

The query of what becomes the social connection in a networked society constitutes, in part, the answer to the question of what is law in an environment such as cyberspace, a virtual place resulting from the interconnections between computers. The characteristics of the cyberspace influence the way we interpret law as well as its normative valences, because the development of information technologies favors the discussion of categories based on which we can define the legal framework of various activities that take place in cyberspace. Indeed, cyberspace endorses the transition of sovereignty from state actors to network owners, as well as individuals and other users acting in cyberspace. The reasons underlying and justifying the creation of legal norms are subject to change due to the general-universal nature of the activities carried out in cyberspace. Additionally, the means by which specific legal norms are expressed reflect the contexts brought into focus by cyber communication.

The demonstrative use of notions in a continuous development and transformation or of variable content reflects a change in role distribution between normativity sources. Regulation resulting from the technical architecture synergy, social norms, self-regulation, the contractual market and law are not unique to cyberspace, but the phenomenon indicates the imperative to explore new ways of understanding and acting on Internet normativity.

Cyberspace constitutes a virtual space where data is generated, stored, modified and exchanged using digital information and communication technologies, through networked systems. The Internet is a component of cyber infrastructure. The continuous development of global interconnection and our growing dependence on

complex technologies creates an unprecedented vulnerability, which affects all the activities of state actors, both economic and social. Possible threats on the Internet range from the so-called "traditional" crime to terrorist activities, including systematic private *data espionage* and *cyber espionage* (in the latter two cases the practice may or may not be abusive), to the point of sabotaging critical infrastructure, the consequences of which can be catastrophic for the security of state actors. To these are added propaganda activities, such as "*fake news*". Risks are also exacerbated by the fact that an increasing number of states are developing their capabilities in *cyber wars* and are therefore equipping themselves with means by which they can impose their strategic or geostrategic interests.

Public international law constitutes the international legal framework that mainly governs the behavior of states. In this context, the question may arise as to whether international humanitarian law can also regulate the behavior of states in the cyber environment. The Center of Excellence for Cyber Defense Cooperation produced version 2.0 of the Tallinn Manual in 2017, with the aim of preventing the occurrence of cyber events in a legal vacuum (Tallinn Manual 2.0)[12].

In international law, there is no legal vacuum in terms of cyberspace. It is generally acknowledged that the most comprehensive framework is currently provided by international law, defined in particular in the UN Charter (United Nations, 1945), the fundamental treaties on human rights, as well as general international law, which also applies to cyberspace. As a result, a *cyberattack* by a state actor, comparable in its consequences to that of an armed aggression, can justify the use of self-defense in compliance with the provisions of the UN Charter. When *cyber operations* are conducted in the context of armed conflict, the provisions of international humanitarian law must be observed. In cases where operations have the sole purpose of obtaining information, the principles of human rights are applicable. However, the specificity of

[12] Created by nineteen experts in international law, the "Tallinn 2.0 Manual of International Law on Applicable to Cyber Operations" published in 2017, is the second updated and considerably expanded edition of the second version, of 2013, of the "Tallinn Manual on International Cyber Warfare". The Tallinn 2.0 Manual is the most comprehensive analysis of how existing international law applies to cyberspace. The Tallinn Manual is available in both material and electronic copies at Cambridge University Press (© Cambridge University Press 2017). The drafting of the Tallinn 2.0 Handbook was facilitated and led by NATO's Center of Excellence for Cyber Defense; https://ccdcoe.org/research/tallinn-manual/

cyberspace represents a challenge for the practical application of the international law norms. In general, state actors are committed to recognizing, complying and enforcing international *cybersecurity* law and actively contributing to the clear norm specification in applying public international law in *cyber space*.

One of the groups of experts who studied the international law applicable to "electronic warfare" and "electronic operations" that do not meet the threshold of war stated that the Tallinn Manual is not legally binding on states. However, it provides an overview of the application of international law in cyberspace and represents a starting point for ongoing discussions between specialists in international law studying the norms applicable to cyberspace. When international relations are governed by legal norms and not by political or military power, thus corresponding to the declared objectives of foreign policy, they ensure the independence and prosperity of states and cooperation in order to generate a peaceful international order. For this particular reason state actors are actively involved in defining the international law applicable to cyberspace. Neutrality, as an instrument of foreign and security policy, would, in principle, also apply during IT operations equivalent to armed conflicts between states. The practical application of the international law of treaties in cyberspace should, however, be clarified in international proceedings, in order to ultimately contribute to increased legal certainty for both state actors and legal entities on the territory of state actors, as well as for the population.

State actors are trying to establish their jurisdiction over licit (*lawful*) and illicit (*unlawful*) activities that take place in the field of cyberspace. In this regard, they outline, based on legal norms, the borders of their national territory within the physical and informational domain of cyberspace. While most private operators are located in the United States and therefore fall under US territorial jurisdiction comprising several states with different jurisdictions, more and more countries want to repatriate Internet infrastructure on their territory in order to fall under their own jurisdiction.

For example, on September 1, 2015, the Russian Federal Law N242-FZ of July 21, 2014 (Federal Law No. 242-FZ, 2014)[13] came into force, forcing foreign bodies to store personal data of Russian nationals on Russian territory. This legal provision allows Russia to exercise its normative and jurisdictional jurisdiction over foreign servers due to *jus loci*. The tendency to territorialize cyberspace also concerns its information field. State actors want to present in their national legislation the content of websites that can be consulted on their national territory, even if they are managed from a foreign territory. Thusly, the issue of the dual jurisdiction of state actors emerges.

First, national courts have to justify their jurisdiction in relation to the illegal (*unlawful*) activities carried out on the internet by private operators on a territory other than their own. French judges, for example, have stated that they have jurisdiction to adjudicate cases related to the outcome of the effects of a particular website on French territory. French jurisprudence has gradually improved the criteria assessment on the basis of the degree of connection between goods and persons that can be evaluated in the context of illegal (*unlawful*) activities carried out on certain sites, taking into account site accessibility, target audience, language used, etc.

It is worth mentioning that the sanctions adopted against these sites, in accordance to national law, also had extraterritorial effects. Following the case of *Google v. Spain* before the Court of Justice of the European Union (CJEU)[14], anyone can demand that a search engine delete websites that directly concern them. In *Google v. Spain*, the European Court of Justice has ruled that European citizens have the right to ask search engine companies, such as Google, which collects personal information for profit, to remove links to private information when the information in question is

[13] Federal Law no. 242, of July 21, 2014, regarding the amendment of some legislative acts of the federation regarding the procedures of personal data processing within the telecommunications and informatics networks, available in English at: https://pd.rkn.gov.ru/authority/p146/p191/ [accessed 23 August 2020]

[14] The case concerns a Spanish citizen who wants an article published in the Spanish newspaper *La Vanguardia Ediciones* to be deleted, or, if this is not possible, then requests that the article no longer appear on the Google search results list. He claims that the information he wants deleted is related to an old debt, which he has long been paid. His requests were also rejected by the publication and Google Spain, which argued that the request should be submitted to Google's headquarters in the United States. As a result, the citizen lodged a complaint with the Spanish personal data supervisor, which rejected the publication's request for deletion of information, but instead issued an order to Google Spain "to take all necessary steps in order to withdraw the targeted data from its indexations and make it impossible to access these data in the future." (Audiencia Nacional, Recurso 725/2010, Sala de lo Contencioso-Administrativo. Sección 1ª, 2 February 2012). Google has challenged the decision in court.

no longer relevant. The Court did not state that the newspaper should remove the article. The Court however found that the fundamental right to confidentiality (*privacy*) is more important than the economic interest of the company and, in certain circumstances, the public interest, represented in this case by the access to information. The European Court upheld the ruling of the Spanish Data Protection Agency, which affirmed the right to freedom of the press and ruled against the request to remove the article on personal bankruptcy from the press organization's website.

In France, the National Commission for Informatics and Freedoms (*Commission nationale de l'informatique et des libertés* - CNIL) notified Google to list all the geographical extensions of its search engine, not limited to European extensions, which had the consequence of applying French law worldwide. By regulating illegal (*unlawful*) activities, in compliance with national law, on accessible websites on French territory - and therefore potentially on all websites - the French State can exercise an extraterritorial legal effect concerning its normative and jurisdictional competence.

Considering the ethical use of information technology, cybernetics, as an act "both legally and morally acceptable to a large majority of the community" (Jones, 1991), knowledge of legal and regulatory mechanisms becomes essential, especially since according to one of the general principles of law "*nemo legem ignorare censetur*"[15].

However, the ITS legislation's status is marked by many shortcomings, due to several factors, including the lack of a specific branch of IT law, the dematerialization of trade and the rapid development of ITSs, and is far behind the development of legal norms, renowned for their inertness. At the present moment, for the most part, there are only disparate (*heterogeneous*) legal provisions regulating specific situations, which have generated them. One can find oneself in the unlikely situation where companies dealing with ITSs are at a standstill not knowing whether or not they comply with legal norms or fit into a legal framework.

[15] Latin adage that translates as follows: "No one can be considered ignorant of the law"; expresses the principle of law that everyone is presumed to know the law and no one can invoke ignorance of the law; the error of law does not exonerate from liability.

This constitutes the reason why some authors recommend that organizations define their own internal ITS and regulatory code:

"*In the absence of specific policies and a code of ethics, electronic information and the prevention of actions that do not fall within the coordinates of ethics are difficult to manage. (...) It is mandatory for organizations to define specific procedures, policies and codes of ethics in order to ethically manage their IT and electronic information." (*Dessai et al., 2008)

The purpose of creating and developing a legal system is to tackle attacks on computer systems and cybercrime. It aims to protect both IS and their contents against any intrusion, sabotage or unauthorized modification. Thus, the law sanctions acts committed by a natural or a legal person.

a. Copyright protection:

Copyright protects the software by its mere development without the completion of any particular formalities. As in the case of literary or artistic works, the creator of the software has, on the one hand, moral rights which are copyright and copyright compliance which prohibits its modification without the author's permission; on the other hand, it has patrimonial rights, respectively, the reproduction and the exploitation right of the software.

b. Patent protection:

In principle, software is not patentable; however, software is likely to be protected by a patent that produces a "*technical effect*", fulfilling the three classic patentability criteria: *i.e.* is something new[16], involves an inventive step and is susceptible of industrial application[17].

Databases are intellectual creations, mainly due to the choice of presentation and organization made by the authors. Therefore, like any intellectual creation, databases can be subject to copyright protection. Their legal regime results from the European

[16] Invention/Innovation: if not included in the state of the art (i.e., to all knowledge made available to the public).
[17] An invention is susceptible of industrial application if its object can be used in at least one field of activity in industry, agriculture or any other activity and can be reproduced with the same characteristics whenever necessary.

Directive of 11 March 1996.[18] With regard to databases, the scope of copyright protection is limited to the structure of the database, excluding data *per se*.

The copyright holder is the author of the database. For databases created at the initiative of a company by its employees or a person specifically employed for this purpose, there is no automatic devolution (transfer of a right from one person to another) of the rights over the employer. However, companies may provide for this on the basis of a copyright contract. As this copyright protection has a formal nature, it was necessary to provide additional protection to the informational content of the database in compliance with *sui generis* rights[19].

Thus, in addition to copyright protection, the informational content of the database can be protected by a *sui generis* right. This protection ensues from the notion of "*substantial investment*"[20] and benefits the database manufacturer. The latter is deemed to be the holder of the rights over the informational content of the database; the manufacturer of the database is the natural or legal person who takes the initiative and the appropriate investment risk.[21] This legal framework protects the manufacturer of the database for a period of 15 years against any repeated extraction or any substantial qualitative or quantitative extraction[22] of the information content of the database.[23]

[18] Directive 96/9 / EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
[19] The *sui generis* rights of database manufacturers - Law 8/1996 on copyright and related rights.
[20] Law 8/1996 art. 140 (4): "For the purposes of this law, the manufacturer of a database is the natural or legal person who has made a substantial quantitative and qualitative investment in obtaining, verifying or presenting the contents of a database."
[21] Law 8/1996 art. 141 (1): "The manufacturer of a database has the exclusive patrimonial right to authorize and prohibit the extraction and/or reuse of all or a substantial part of it, assessed qualitatively or quantitatively."; (4) "The right provided in par. 1. shall apply irrespective of the possibility of protecting the database or its contents by copyright or other rights. The protection of databases by the right provided in par. 1. shall not prejudice existing rights with regard to their content."
[22] Law 8/1996 art. 141 (2): "For the purposes of this law, it is understood by: a) extraction: the permanent or temporary transfer of all or part, assessed qualitatively or quantitatively, substantial of the contents of the database on another medium, by any means or under any form; b) reuse: any form of making available to the public all or a substantial part of the contents of the database, assessed qualitatively or quantitatively, by distributing copies, renting or otherwise, including making available to the public the contents of the database , so that everyone can have access to it at the place and time chosen individually. The first sale on the domestic market of a copy of the database by the holder of the *sui generis* right or by consent exhausts the right to control the resale of this copy; (3) Public loan of a database is not an act of extraction or reuse."
[23] Law 8/1996 art. 143 (1): "The rights of the database manufacturer shall arise once the database has been finalized. The term of protection shall be 15 years, starting on 1 January of the year immediately following the completion of the database."

In the joint communication of the High Representative of the European Union for Foreign Affairs and Security Policy held in Brussels on 13 September 2017, entitled "*Resilience, deterrence and defense: building strong cybersecurity for the EU*", was emphasized that:

"*Cybersecurity is critical to both our prosperity and our security. As our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed. Cybersecurity incidents are diversifying both in terms of who is responsible and what they seek to achieve. Malicious cyber activities not only threaten our economies and the implementation of the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. Our future security depends on transforming our ability to protect the EU against cyber threats: both civilian infrastructure and military capacity rely on secure digital systems. This has been recognized by the June 2017 European Council*[24]*, as well as in the Global Strategy on Foreign and Security Policy for the European Union.*"[25]

3. Approachable/accessible solutions in cyberspace

The digital universe has become more dangerous than ever, as attackers extend their tentacles beyond phishing, attacks that target everything from stolen credentials, to improper configurations in the cloud, to remote access instruments.

Parallel development of offensive and defensive capabilities will become an increasingly important topic as AI systems become more complex, available and easier to implement. Everything from spam emails trying to deceit you into revealing credit card details to denial-of-service attacks designed to disable critical infrastructure will increase in frequency and sophistication.

The technology available to help avoid casualties, such as deep learning security algorithms, automation of systems vulnerable to human error and biometric identity protection, is becoming increasingly effective.

[24] http://www.consilium.europa.eu/ro/press/press-releases/2017/06/23-euco-conclusions/.
[25] http://europa.eu/globalstrategy/.

Artificial Intelligence (AI) is already present in many areas of defense, including cybersecurity. Security information and event management software (security information and event management/real-time cybersecurity analysis platforms) are among the first examples of AI in this field. In the domain of code analysis and behavioral analysis of computer systems, AI mainly develops new and effective methods in the fight against cybercrime and cyberattacks. Increased use of AI, capable of processing significant amounts of information in record time, makes it possible to identify malicious codes more efficiently by comparing them with coded databases classified according to their nature. Regarding the analysis of computer systems operations, the AI contribution could improve identification of abnormal behaviors that are symptomatic of security attacks or breaches. However, several difficulties counterbalance the opportunities that AI offers to cyber defenders. First of all, the difficulty in analyzing codes that suffered changes in their evolution represents a hindrance.

In behavioral analysis, there is a risk associated with the ability of AI to detect certain attacks. The amount of data to be processed is immense and, despite the increased AI capabilities, weak signals cannot be identified. Hervé Debar (Debar, 2018) defines these difficulties as the issue of the rule (norm) that governs the political dimension of information systems use and that of excessive investment in data. A major difficulty in the development of AI in cybersecurity relates to the advantage that the attacker has in this area. Due to the eternal theory of the sword and the shield, the imagination of the attacker should not, under any circumstance, be underestimated.

AI efficiency can be limited by information saturation or by multiplying false alarms and anomalies. It will be more difficult for AI to conceal its vulnerabilities than for the attacker to imagine new attacks, new malicious codes. Evermore, it would be impossible for AI to prevent unforeseen attacks in its startup code. Therefore, defensive AI can always lag behind attackers' innovations. Despite the possible improvements that AI development could bring in the field of cybersecurity, there are still significant limitations in this area that imply a real need to continue to support people in decision-making and implementation for efficiency and adaptability issues.

Both the regulatory landscape and that of suppliers have undergone dramatic changes, with the European Union beginning to enforce strong data privacy regulations from May 2018, and California following suit in January 2020.

Artificial intelligence (AI) will play an increasing role in both cyberattack and defense. On the other hand, we must not forget that AI represents the new arms race, but unlike previous arms races, anyone can get involved - there is no need for resources that previously were available only to governments.

This means that while AI is undoubtedly researched and developed as a means of paralyzing the civilian and defense infrastructure of an enemy state during war, it also can be easily deployed anywhere by criminal gangs and terrorist organizations.

So, rather than between nations, today's race runs between hackers, crackers, phishers and data thieves and cybersecurity experts, whose job is to address these threats before they cause any harm. Just as AI can "learn" to identify patterns of behavior or coincidences that may signal an attempted attack, it can learn to adapt to mask the same behavior and fool our defenses.

In 2020, research suggests that the number of vacant cybersecurity jobs will increase from just 1 million in 2014 to 3.5 million. This skills deficit is most likely to become a growing public interest issue in the first part of this new decade (Perhach, 2018). The threats our generation faces today in cyberspace, from thieves trying to clone identities (*identity thief*) to commit fraud, to political disinformation campaigns aimed at changing the course of democracies, will only become more intense if there are not enough people with the necessary skills to counter them.

The next generation of AI-based attacks will be ingenious enough to mimic the behaviors of certain users in order to outfox even qualified security personnel. This could include the ability to create complex and personalized phishing campaigns that will successfully deceive even the most threat-conscious of us. Without investing in training existing staff on how to prevent or mitigate cyberattacks in their field, as well as without hiring experts with the capacity to detect new threats, the industry is in peril to lose big time.

No doubt, the implementation of these mature defenses requires access to an expert and experienced workforce in cybersecurity - which will become a proliferating challenge in coming years.

4. The relevance of cybersecurity from a human rights perspective

In his opening remarks to the United Nations General Assembly in 2017, Secretary-General Antonio Guterres stressed that the growing number of threats to cybersecurity has become one of the major threats to international security. In addition to the threat of cyber warfare, cyberattacks have led to the closure of hospitals, the disconnection of high-powered transformers, paralyzed cities and even compromised the integrity of the democratic process.

As cyber threats become more commonplace, more sophisticated and with increasingly serious consequences, no wonder that governments, industry and cyber industry experts emphasize the need to strengthen cybersecurity. But more often than not, these efforts overlook the dimension of human rights, or, worse, perceive it as an obstacle to cybersecurity. This constitutes a wrong assumption and the time has come for it to be regarded as such.

No universally recognized definition of cybersecurity has been formulated. But the definition provided by the "*An Internet Free and Secure*" working group of the FOC (Freedom Online Coalition) is undoubtedly interesting.[26] This group of technicians, human rights experts and government officials *defines cybersecurity as maintaining - through policy, technology and education - the availability, confidentiality and integrity of information and basic infrastructure to increase the safety of people online and offline.*

Using the FOC's definition of cybersecurity, one can easily understand that threats to cybersecurity - or cybernetic security - can also be regarded as human rights

[26] The Coalition for Online Freedom is a group of governments committed to working together to support the freedom of the Internet and to protect fundamental human rights - free expression, association, assembly and online privacy - worldwide. The coalition was established in 2011 at the inaugural Conference on Online Freedom in The Hague, the Netherlands, at the initiative of the Dutch Foreign Ministry. Today, the Coalition has 30 members from Africa to Asia, Europe, the Americas and the Middle East. All Member States signed the founding document FOC (Freedom Online: Joint Action on Free Speech on the Internet) and pledged to respect the principle that offline human rights are the same as online.

infringements. Denying the provision of information and its basic infrastructure, in the form of network closure, for example, infringes a wide range of rights, in particular by restricting access to information and allowing people to express themselves, gather peacefully and associate, but also to enjoy a number of economic, social and cultural rights. In 2018, there were 196 internet networks interruptions/cuts in 68 countries.

There are countless examples of situations where information security is compromised or breached, whether through data leaks for financial gain, mass surveillance by governments or targeted attacks on human rights defenders or journalists, in violation of the right to privacy, among many other rights. Confidentiality of communications infringements led to serious human rights violations, including detention, torture and extrajudicial killings. A case that sparked outrage can be cited[27]: the surveillance of Saudi dissident Omar Abdulaziz[28] which contributed to the extrajudicial execution of Saudi journalist Kamal Kashoggi.

According to a complaint, Abdulaziz's phone was hacked compromising the confidentiality of his communications with Kashoggi about opposition plans in the months leading up to his murder.

Although most people will experience some form of cyber insecurity in their lives, even those for whom access to the Internet represents a significant challenge, not everyone experiences this insecurity equally. Human rights defenders, journalists and anyone in a situation of marginalization or vulnerability, due to religion, ethnicity, sexual orientation or gender identity, for example, fall into specific risk-sensitive groups. They are more likely to be targeted by government or other surveillance agencies, and the consequences of rather general threats, such as data leaks or shutting down the Internet, are often much more serious in their case due to their special position in society.

The more people and objects connected, the greater the risks associated with cyber insecurity. Unfortunately, governments do not put human rights at the center of

[27] *See also* the European Parliament resolution on the killing of journalist Jamal Khashoggi at the Saudi consulate in Istanbul (2018/2885 (RSP)).

[28] Abdulaziz has almost half a million "followers" on Twitter. He wrote that Saudi Arabia seems to place him among the top three "influencers" in Saudi Arabia.

discussions or, worse, use the excuse of cybersecurity to strengthen their control over the Internet. The development of legal rules, policies and standards on cybersecurity tends to be found in "*opaque*" or "*safe*" places and therefore does not benefit from the input of civil society or human rights experts. This runs counter to a multi-stakeholder approach to internet governance, based on the full commitment of governments, the private sector and international organizations.

This approach excludes, in particular, the skills and monitoring needed to protect human rights. Cybersecurity discussions often take place within the confines of intelligence services or other military or government agencies that are not subject to public and civil society control and vigilance. Cybersecurity is sometimes equated with national security, a sacred sphere in which governments can do anything out of sight and, even more importantly, out of public control. As a result, laws, customs and policies are not defined in a human rights framework and enable power abuse.

Thus, it becomes increasingly clear that international human rights provisions also apply to digital technologies.[29] Be that as it may, when it comes to cybersecurity, human rights are never at the crux of the discussion, and, unfortunately, sometimes not even part of it. This is due, to a certain extent, to the fact that international cybersecurity debates mainly address the issue of attacks between state actors and therefore fall under international security and disarmament. Nevertheless, the content of these debates and the resulting standards have implications for the manner in which state actors approach cybersecurity at a national level.

Of particular concern are the efforts of the Shanghai Cooperation Organization[30], as the group has been campaigning for years to expand national sovereignty and control over cyber information. Since 2013, UN has ruled that international law, which includes international humanitarian law and international human rights law, also applies to cyberspace. In 2015, a group of government experts dealing with

[29] *See* Resolutions of the Human Rights Council on "Promotion, protection and observance of human rights on the Internet", 20/8 (2012), 26/13 (2014), 32/13 (2016) and 38/7 (2018).

[30] In April 1996, China, Russia, Kazakhstan, Kyrgyzstan and Tajikistan signed an agreement in Shanghai to deepen military confidence at the border, and a year later, in Moscow this time, the five countries signed another agreement to reduce military forces at the border. These agreements laid the groundwork for what was called the Shanghai 5 (*Shanghai Five*). The main role of this organization was to demilitarize borders and strengthen neighborly relations between Member States.

developments in the field of information and telecommunications in the context of international security clarified that respect for human rights and fundamental freedoms is "crucial" and recommended that states comply with United Nations resolutions on human rights on internet as well as respect for privacy in the digital age.

International human rights mechanisms provide specific guiding criteria, which are fully applicable to cybersecurity and which should refer to the development of standards of responsible conduct of states in the field of cyberspace. For example, the United Nations Special Procedures[31] justify the need for a strong coding process to ensure the confidentiality of information and how the closure of networks (*n.n.* Internet) violates human rights provisions and unjustifiably impedes free access to information. A set of standards in international human rights law, in this case "UN Guiding Principles on Business and Human Rights" (part of the *United Nation Development Programme* - UNDP) adopted by the Human Rights Council[32], which clearly explains the responsibility of the private sector to respect human rights, to reduce negative effects of its actions and to remedy the damage. This constitutes a fundamental problem, given that the private sector owns and/or operates most of the infrastructure, *hardware and software*, on which the Internet depends.

In order to promote and respect human rights in the digital age, the time has come for cybersecurity to be addressed as a human rights concern.

First of all, the idea that human rights are an obstacle to security must be rejected. Perhaps the most frequently cited example in illustrating that human rights thwarts security constitutes the thesis that codification, which represents an essential factor for the application of the right to privacy, impedes the pursuit of justice. Governments

[31] *See* European Parliament resolution of 14 January 2009 on the development of the UN Human Rights Council, including the role of the EU (2008/2201 (INI)); Special procedures UN art.10 .: "(…) considers that Special Procedures are the basic element of the UN mechanisms for the protection of human rights and emphasizes that the effectiveness and credibility of UNHCR in the protection of human rights is based on cooperation with special procedures and their implementation as well as on the adoption of reforms leading to the strengthening of their capacity to deal with human rights violations."

[32] Resolution no. 26/9 of 26 June 2014 of the UN Human Rights Council in which it was decided to "*establish an unlimited intergovernmental working group on human rights and transnational corporations and other enterprises, whose mandate is to develop an international instrument legally binding to regulate, in international human rights law, the activities of transnational corporations and other enterprises.*"

regularly advocate for the introduction of a *backdoor*[33] in the coding process to allow law enforcement access to encrypted communications. Experts agree that coded data cannot be given to a state actor without being offered to all governments, as well as to malicious non-state actors. In other words, cybersecurity for law enforcement cannot be undermined without undermining the security of all and endangering human rights. And that's because cybersecurity is inexorably associated with the security of individuals, which is one of the foundations of human rights.

Cybersecurity and human rights are complementary, interdependent and mutually reinforcing.

Thereby, a human rights-based approach to the development of legal norms, policies and practices on cybersecurity becomes imperative. Cybersecurity risks should never be used as a pretext for human rights infringements. On the contrary, recognizing that individual and collective security remains at the heart of cybersecurity implies that the protection of human rights should be at the heart of cybersecurity policies development. At an international level, it should be imperative to anchor debates on cybersecurity in international human rights law. The Freedom Online Coalition (FOC) working group developed a set of recommendations focused on cybersecurity and human rights to ensure that cybersecurity policies and practices are based on human rights and fully compatible with said rights. In fact, cybersecurity policies and practices should comply with human rights from the very beginning of their conception. These recommendations, which have been endorsed by 30 FOC member governments and more than 24 NGOs, are a useful starting point for rooting cybersecurity policies and practices in the field of human rights.

Companies should comply with human rights and governments should hold them accountable for their infringements. Although the "UN Guiding Principles on Business and Human Rights" (part of the *United Nation Development Programme* -

[33] *A backdoor* is a way to gain access to a program, an online service, or an entire computer system. *A backdoor* will bypass normal authentication mechanisms.

UNDP) adopted by the Human Rights Council provides the necessary framework, the need for a more rigorous monitoring and control of information technology companies still remains, taking into account that the afore mentioned companies are, customarily, the ones providing the hardware and software used to launch cyber attacks, but also providing the first line of defense in the case of cyberattacks. In addition to conducting human rights impact assessments to identify, understand, analyze and address the negative effects of their policies and practices on ensuring human rights compliance, they should examine the governance, processes and control instruments used to secure information on human rights. Certain companies have taken initiative to implement advanced self-regulatory procedures. In this regard, one can cite Microsoft's "*Cyber Security Technical Agreement*", which aims to respond to all cyberattacks that pose a risk to individuals. However, the agreement does not present a specific human rights perspective.

Cybersecurity processes must be multi-stakeholder and inclusive, but also multidisciplinary, both in the field of human rights and in terms of technological expertise.

This can be translated in positioning cybersecurity outside the confines of national security and intelligence agencies and challenging the idea that cybersecurity represents primarily a matter of national security. Given that citizens are so often required to make sacrifices in the name of national security, it is essential that these sacrifices be taken into account with particular care in order to maintain a balance between necessity and proportionality. There should be independent monitoring of responses to international security threats to verify that they are justified, more transparency and public debate to ensure national security, which should not be confused with the security of the ruling regime.

Digital technologies represent a new and unforeseen challenge for human rights and security that will require much more study, research and analysis. As long as

cybersecurity and human rights are not seen and treated as complementary, two sides of the same coin, both cybersecurity and human rights will suffer.

5. Issues regarding the application of the principles of ethics and integrity in cyberspace

Information technology ethics represents a discipline that has its roots in the ethical theories of moral philosophy. From its origins, starting with Wiener's work on cybernetics in the 1940s (Wiener, 1948; Wiener, 1954; Wiener, 1964) to the present day, is generally accepted that ethical theories of moral philosophy should be galvanized to understand and analyze the problems generated by cyberspace (Manner, 1996).

A plethora of ethical theories could be found within moral philosophy. It can even be affirmed that there are as many conceptions of ethics as there are recognized philosophers in the field of ethics. Thus, we have: the Aristotelian ethics of virtue, Kantian deontology, Bentham's hedonic utilitarianism, Levinas' ethics of responsibility or so-called *alterity*, Jonas' technological responsibility, Morin's trust ethics, etc. Equally, one can encounter as many ethical theories as there are disciplines, in terms of applied ethics: for example, medical ethics, business ethics, e-commerce ethics, IT ethics, etc.

On the other hand, traditionally, four major currents of ethical thinking in Western moral philosophy can be distinguished: deontological ethics, utilitarian ethics, virtue ethics, and pragmatic ethics. To these currents there can be added other non-Western ethical traditions, for example those of African and Asian origin, which may constitute a fifth major ethical trend.

Deontological ethics is founded on the observance of moral duties that function as absolute restrictions on all behaviors. According to deontological theories, any act must comply with the standards, regardless of the consequences. Duty (responsibility, obligation) is, thusly, analyzed as an "unconditional practical necessity of action" (Kant, 1971). In other words, an action is moral only if it is in accordance with the moral norms, *i.e.* action should be subject to the observance of rules (norms), regardless

of its consequences. The ethics of information technologies and systems, as a branch of professional ethics (Gotterbarn, 1991) is deeply rooted in the deontological perspective. As such, it promotes good practice and establishes a set of mandatory rules, by drafting codes of conduct for IT professionals and, as a result, for all information technology and systems users within the company. The "*10 Commandments of Computer Ethics*" published by the Institute of Computer Ethics and the Code of Good Practice for the use of information technologies and systems of an organization represent a concrete illustration of this fact. Kantian deontology is founded on the concept that man has three fundamental characteristics - reason, freedom, dignity, that is, human beings are endowed with reason, are free and possess dignity. Indeed, due to the fact that any human being is endowed with reason, is "*auto nomos*"[34] (*self sufficient*), consequently one can discover for oneself, without the help of any authority, the moral laws that govern one's actions. In this respect Kantian deontology can be interpreted as a belief ethic.

For the belief ethic, an action is morally correct if it is consistent on the one hand with a moral rule and on the other hand with the goodwill (intention) of the individual. "Goodwill" constitutes a primordial concept that makes the morality of an action not its result, but its intention, without which it can be objectively good without being moral (Courdarcher, 2008). On the other hand, an action is considered to be moral if it can be "*universalized*", *i.e.* can be applied by all human beings.

Human beings are fully responsible for their actions and take responsibility for them both in the present and the future. The ethics of responsibility stems from the statement that "we must be held accountable for the foreseeable consequences of our actions" (Weber, 1963). The ethics of responsibility is expressed in a "technological" or "ecological" responsibility in Jonas (Jonas, 1979) and in an ethic of alterity in Levinas (Levinas, 1995).

Specifically, the ethics of responsibility in Jonas reflects in a renewal of the categorical Kantian imperative of the obligation to maintain the permanence of an authentic life on earth in a context of technological change. Levinas' ethics of alterity,

[34] From the Greek *autonomos* which means "having its own laws/rules".

which claims that there is a responsibility to the other when one discovers the *Other's* true face (human essence). This ethic, nascent from "religious transcendence", which means that meeting *Others* generates responsibility towards them and requires prohibition of violence; for example, the observance of the commandment "*thou shalt not kill*" (Levinas, 1995).

Discussion ethics represents a theory developed within the Frankfurt School of Habermas (Habermas, 1992) and Apel (Apel, 1994). Its bedrock rests on the idea of consensus for ethical and moral research and aims to establish a basic principle for moral deliberation and evaluation of the validity of norms. Consensus is understood as the agreement of all participants in a discussion.

This theory emanates from the postulate that neither truth, nor *cogito*, nor divinity is accessible. Therefore, we are dealing with a transparent communication that refers to the informed choice of a certain set of individuals. At the same time, the ethics of discussion lay down the rules for authentic, free and successful communication, *i.e.* transparent communication that promotes mutual understanding in order to reach an agreement; it represents the communicative process organized around the values of transparency, impartiality, sincerity, truth and relevance. The course of the discussion revolves around the overriding requirement of freedom and equality for all participants.

Utilitarianism is a moral theory founded on the principle of utility and emphasis on the consequence of actions. It represents a form of *consequentialism* in the sense that, for *utilitarians*, what matters is not the intention of the action, but its effects, results or consequences. A just moral action constitutes an action whose consequences are righteous, insofar as it contributes to maximizing the happiness of as many individuals as possible. Fundamentally, the utilitarianism of Bentham (Bentham, 1789) and Mill (Mill, 1968) is established on a hedonistic postulate that the purpose of life is to pursue pleasure and maximize happiness for all.

Starting with Morin, a so-called theory of the ethic of "trust", strongly developed by *consequentialism*, takes shape, because, according to him, the concept of self-ethics or individual ethics is built on two commandments: the discipline of egocentrism and the development of altruism.

The author understands ethics in its complexity as a "moral requirement that manifests itself in an imperative way" (Morin 2004): that is, an ethic of trust, which has its roots in the *individual-society-species troika*, which constitutes the three dimensions of the common thread of Morin's thinking (Morin, 2004). The ethics of trust represent a form of "*ethics of complexity*", according to Morin's complex thinking. The concept can be divided into three layers of ethics: an individual ethic or "*self-ethics*", a community ethic or "*socio-ethics*" and an "*anthropo-ethics*" (Morin 2004).

As mentioned earlier, Norbert Wiener is considered the founding father of IT/IS ethics in the late 1940s. Wiener was one of the first authors to explore the ethical and social implications of information technology, in a context that coincides with the very first developments of these technologies. However, his work in the field of ethics did not resonate with the researchers and practitioners of the time. It lasted until the 1980s, when Maner's work, which laid the foundations of a domain that has since been called *Computer Ethics*, perceived as a branch of ethics applied to technology. Another perspective, that of Gotterbarn, places IT ethics as a branch of professional ethics (*professional deontology*) regarding good practices and codes of conduct for IT professionals.

Ethics related to the impact of IT based on the study of specific issues of the field was initiated by Mason's work. He was the first to identify the four fundamental pillars of IT, namely confidentiality, integrity, ownership and accessibility. Since then, new facets have been identified and debated by a relatively rich literature. These include, but are not limited to, personal data protection (Sviokla and Gentile, 1990), misuse of computer equipment (Dorf, 1999), illegal downloading and computerized crime (Balzan and Philips, 2008), artificial intelligence, biotechnology and nanotechnology (Brey, 2012).

It is generally accepted that the ethics of information technology and systems as a field of study began in the late 1940s with the development of the first information technologies, at the behest of Norbert Wiener and his work in the field of cybernetics. But it was not until the 1980s that researchers and practitioners such as Maner, Johnson,

Gotterbarn became interested in the ethical implications of information technology to lay the groundwork for "a booming discipline" (Kefi, 2015).

Norbert Wiener, who can be considered the pioneer of ITS ethics, believes that principles such as: freedom, equality, goodwill and the principle of least violation of freedom should serve as a framework for analyzing information on ethics issues – "the principle of freedom, the principle of equality, the principle of goodwill, the principle of the minimum infringement of freedom." (Wiener, 1954; Wiener, 1964) This is also true for the pairs of fundamental values of the human being: life and health, work and wealth, creativity and happiness, democracy and freedom, peace and security (Wiener, 1954; Wiener, 1964).

In genere, the evolution of this discipline can be analyzed in accordance with the four phases of the development of computer technology and the ethical issues involved (Tavani, 2008; Tavani, 2013). *The first phase* corresponds to the first developments in technology and computers and lasts from 1950 to 1960; ethical questions were mainly related to the consequences of the development of artificial intelligence and the issue of privacy protection. *The second phase* coincides with the development of computer technology, the marketing of the first personal computers and their networks (*via* private networks). The ethical issues associated with this phase, which lasted from the 1970s to the 1980s, are confidentiality, intellectual property and computer (informational) crime. *The third phase* actually constitutes the "*age of Internet*", which includes the increased availability and accessibility of the Internet to the public. The proliferation of web-based technologies and applications raises, in fact, issues related to freedom of expression, confidentiality, personal data, computer crimes, *etc.* which adds to the existing problems. *The last phase, the fourth*, which reflects the present moment and the near future, corresponds to the convergence between information and communication technologies and nanotechnology, biotechnology, connected objects, *etc.* Ethical questions relate in particular to artificial intelligence and genetic modification. In addition to problems related to "*big data*"[35], robotics and its

[35] *Big data* is an area that deals with ways to analyze, systematically extract information, or treat sets of data that are too large or complex to be handled by traditional data processing applications.

consequences on certain sectors of activity, there are as well to be pondered the physiological and genetic changes in people subjected to genetic changes, etc.

In the literature, ITS ethics is described as a branch of applied ethics that studies ethical problems "aggravated, transformed or created" (Maner, 2004) by technology and computers. Information ethics examines the issues raised by ITSs and analyzes their ethical and social implications. Thus, ethical traditions of moral philosophy such as Bentham and Mills's utilitarianism or Kantian deontology could be used to analyze and identify these new problems (Maner, 2004).

Mason was one of the first authors to ask questions about identifying ethical problems related to the use of ITS. This author's work represents the basis of the famous acronym "PAPA" of ITS ethics - Privacy, Accuracy, Property, Accessibility – *i.e.* confidentiality, integrity, ownership and accessibility (Mason, 1986). The genesis of Mason's theory originates from the idea of a "new social contract" (Mason, 1986) of the information society, in which it would be appropriate to ensure that the use of technologies and the information that goes through them, can participate in improving the dignity of a person. Hence, we are dealing with a moral concept that revolves around the central concept of a person's dignity (Mason, 1986). In other words, ITSs should not violate individual confidentiality, should be viable and reliable, protect intellectual property and be accessible to all.

Ethical issues refer to all questions and moral or ethical problems rose by ITSs in a concrete situation generated by their use.

Manners of use refer to the way ITSs are utilized because, in general, within an organization distinctions are made between professional and private or personal use. Professional use corresponds to the use of equipment within the strict framework of the organization's activities and assigned tasks. Private use, as the name suggests, refers to the use of the material for personal purposes and outside the activity of the organization.

Usage control refers to the various surveys and monitoring mechanisms put in place by an organization to control its staff activity. From a legal point of view, the organization has the right to control and monitor the activity of its employees during

the work schedule, provided that employees are informed in advance about the implementation of this control system. The use of clandestine surveillance methods is illegal (*unlawful*).

"Good practice" principles refer to all rules and behaviors that aspire to an eminently correct use of ITS. These may be rules or regulations from individual or collective sources intended to guide actions and behaviors towards an appropriate use of ITS. Workforce dynamics and contemporary society dictate the need to transform educational processes according to the development of information technologies and their adaptation in order to ensure fluency and effortless usage and updating.

Continuous development of information technologies and their widespread application in most human activities have radically changed the face of many industries and inevitably raise thorny ethical questions about the use of these instruments.

Indeed, if one consider ethics, from a conceptual point of view, as a reflection and a process that tends to orient behavior towards "correct and good or righteous actions" (Hoffe, 1993), it is deemed important to understand what realities create the scaffolding of the ethics of information technology in terms of individual and organizational use, in terms of moral positioning and in terms of the type of use, accurately adopted, by "a technology that can lead to socio-technological change" (Hoffe, 1993).

Ethical aspects of certain cyberspace-specific phenomena must be taken into account, starting with the *politicization of cyberspace*, which also includes the ramifications of the phenomenon of "*camping in cyberspace*", followed by *astroturfing*, information dissemination and the phenomenon of *fake news*, which gains more and more informational territory.

In regard to the politicization of cyberspace, the first ethics problems that appear are related to the difficulty of attributing a cyberattack, which can be exacerbated by the existence of so-called "*false flags*"[36], *i.e.* manipulations by an attacker of the technical traces of his attack, so-called "*artifacts*" - to deceive investigators about the

[36] *False flag* operations are covert operations, which are designed to mislead the public, so that operations appear as if they are being performed by other entities. The name derives from the military concept of *flying with false colors*, namely, the ship flies the flag of another country, other than its own country.

true origin of the cyberattack. Unfortunately, there are many techniques available to cyberattackers: modifying malware metadata, specific instruments they create and use - falsifying logs in the victim's infrastructure, controlling them, reusing malware or mimicking the *modus operandi* of a another group of cyberattackers, but also the opportunism in choosing a target, taking advantage of the existence of a so-called "*suspect on call*", taking into account the geopolitical situation.

Nowadays political campaigns (cyberspace) are particularly easy targets. They are inherently temporary and transient, lacking the time or money to develop long-term, well-tested security strategies. A large number of new staffers are often employed for short time-span, without a training period, staffers that can bring along both their own hardware from home but also unwanted malware. Events are moving fast, the stakes are high, and people feel they don't have time to worry about cybersecurity. There are a lot of opportunities for something to go wrong.

At the same time, campaigns are increasingly based on proprietary information about voters, donors and public opinion. Sensitive documents such as opposition research, vulnerability studies, staff verification documents, policy documents and emails from various servers are stored on such platforms. The risks of a potential attack are increased and so are the consequences of a cyberattack, and the ethical problems that such a situation can generate are many and intricate.

Analysis of the ethical dimensions of *astroturfing*[37] (if it existed!) would have been created in order to meet the agenda of a corporation, by manipulating public opinion and disregarding scientific research, thus, representing a serious breach in ethical behavior.

While legally or ethically the phenomenon of "*astroturfing*" can be downright shocking, in business its use benefits the companies. For example, for a company like Microsoft that "fights" in a competitive market for staggering billions of dollars,

[37] *Astroturfing* is the practice of masking the sponsors of a message or organization (for example, politics, advertising, religious or public relations) to make it appear as if it were original and is supported by core participants. It is a practice designed to give credibility to statements or organizations by retaining information about the source's financial connection. The term astroturfing is derived from *AstroTurf*, a brand of synthetic rugs designed to look like natural grass, as a play on the word "basic". The implication behind the use of the term is that, instead of a "true" or "natural" basic effort, there is a "false" or "artificial" aspect of support behind the activity in question.

spending a few million on *astroturfing* seems to be a smart strategy. The earning potential is huge; especially, if based on *astroturfin*g efforts, the company's rivals can be tried and brought before inquiry commissions, either of a judicial or regulatory nature.

It could even be said that *astroturfing* simply represents an intrinsic part of the "professional league of companies". Political parties practice *astroturfing*, why not companies? Furthermore, almost all big companies make donations to nonprofits, many of them with openly aggressive agendas. In this case, *astroturfing* could only be considered an extension of this practice.

The problem that arises is that while *astroturfing* can help companies, it harms the public's ability to understand the complicated problems of information technology, enveloping them in a veil of mystery just a step away from the most imaginative conspiracy theories. Many people still do not trust the information technology sector, and saturating the news with misinformation, a completely unethical approach, only deepens the public's suspicion.

Digital technology encourages the dissemination of knowledge and know-how. Its ability to influence socio-economic structures also means that it gives power and competitive advantage to those who design their applications over those who only use them. Ethics, which represent a form of critical thinking in the architecture and social tradition that shape the life of societies, aim to question the morality of the information dissemination process and provide the opportunity to make choices based on real information (*informed choices*).

Digital libraries belong to a new emerging digital culture. The existence of this information plethora raises new questions about the production, collection, classification and dissemination of knowledge. How can the integrity, validity and durability of these digital collections be guaranteed and, in particular, is the dissemination of information ethical without regard to copyright and proprietary data/ information?

Information technology is now *ubiquitous* (*Ubiquitous Computing*)[38] in the lives of people around the world. These technologies take many forms, such as personal computers, smartphones, the Internet, web and mobile applications, digital assistants, and cloud computing. In fact, the list is constantly growing and new forms of these technologies are operating in every aspect of daily life. By allowing the digital environment to develop chaotically and unregulated, the level of cybersecurity has actually been reduced, resulting in a deterioration and pollution of our *infosphere*. This constitutes the desired result - entertainment, cheaper goods, free news and juicy online gossip – but not the deeper understanding, dialogue or education that would have served much better and benefited much more in the long run.

In the case of previous media outlets (*e.g.* newspapers, physical media in general), there has been a constant concern about maintaining standards, respecting accuracy and the presence of a necessary informed public debate. Now we are confronted with the same problem when dealing with the misinformation practiced online. These types of digital, ethical problems are a defining challenge of the XXIst century. They include violations of privacy, security and safety, property and intellectual property rights, trust, fundamental human rights, and the possibility of exploitation, discrimination, inequality, manipulation, propaganda, populism, racism, violence and hate speech.

The lack of proactive ethics predicts decision-making as quickly as the cybersphere develops, undermines real-time management practices, and harms global digital innovation strategies. The quasi instantaneous spread of digital information makes misinformation difficult to track and almost impossible to correct in real time, especially when trust is undermined (*Emotional Trust in a Hyperconnected world*).

How do we establish trust through credibility, transparency and accountability - and a high degree of patience, coordination and determination? Will this goal be

[38] *Ubiquitous computing* is a paradigm in which the processing of information that is related to each activity or object encountered. This involves connecting electronic devices, including incorporating microprocessors to communicate information. Devices that use ubiquitous computers are constantly available and fully connected. Ubiquitous computing focuses on learning by removing the complexity of computing and increasing efficiency while using computing for various daily activities. Ubiquitous computing is also known as ubiquitous computing and environmental intelligence.

achieved with the development of an ethical *infosphere* capable of saving the world and ourselves?

Increased attention is being paid to the impact of the phenomenon of *fake news* on democracy and society in general. Researchers in many fields are trying to determine who is behind the propaganda efforts with fake news, what are the effects and how to address this phenomenon using technological means. The studies also analyze the ethical problems raised in the fight against false news. In developing a scheme of a pragmatic media ethic, one examines the labyrinthine ethical complex of the problem, which like Ariadne's thread can get us out of the maze of fake news. In addition, the pragmatist approach to fake news also allows us to highlight the discordant values and results of the stakes, in attempts to conceptualize and eradicate this new ethical challenge so present in social media. Such an intuitive involvement in the phenomenon of fake news represents an essential first step in diagnosing ethical challenges and potential solutions.

It can be assumed that the term "*fake news*" has a simple meaning or can be interpreted by analyzing the sum meanings of the words that form the compound noun (Tandoc et al., 2018). The conundrum originates from the fact that the term "news" means information that should be verifiable for the benefit of the public, and any information that does not comply with these standards does not deserve the news label. In this interpretation, then, "fake news" represents an oxymoron that lends itself to undermining the credibility of information that really meets the threshold of verification and public interest - that is, real news.

In order to better understand cases involving manipulation of language exploitation and news genre conventions, these acts of fraud must be treated as what they are - a particular category of falsified information, clad in the cloak of misinformation, increasingly diverse and widespread, including in entertainment formats such as visual memes.

The fact that "fake news" is usually free rises to the maximum alert level - which means that people who can't afford to pay for quality journalism or who don't have

access to independent public service media are particularly vulnerable to misinformation as well as to false information.

The spread of misinformation and false information is largely possible through social media and social messaging, which addresses the question of the need for regulation and self-regulation of companies providing these services. In terms of their nature as intermediate platforms, rather than content creators, these companies have so far only been subject to extremely lax regulations, with the exception of copyright. However, in the context of increasing pressures on these media outlets, as well as the threats posed on freedom of speech by over-regulating, important - albeit timid - steps have been taken in the area of self-regulation (Manjoo, 2018).

In 2018, the UN Special Rapporteur on Freedom of Expression and Opinion focused on this issue, urging internet companies to practice self-regulation in the media and to better align with UN standards on the right to distribute, search and receive information.[39] In this multitude of rapidly evolving measures, taken by both states and companies, journalists and the media play a very important, if not paramount, role.

The development of journalistic strategies to combat misinformation should therefore be undertaken given that the manipulation of information has been present in the life of society for millennia, while the evolution of journalistic professionalism constitutes a relatively recent phenomenon (Posetti and Matthews, 2018). As journalism has evolved, playing a normative role in contemporary society, the media has largely managed to function outside the world of fabricated news and covert attacks, protecting and promoting journalism that aspires to high professional standards, that respects factual truth and verification of sources, verification methodologies and public interest ethics.

At the present moment, even taking into account the great variety of "journalism" types, it is still possible to identify the narrative diversity of true news that bears the distinct label of ethics in communication and tries to be editorially independent of

[39] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. UN Human Rights Council 6 April 2018. A/HRC/38/35. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement (accessed at 15/08/2020).

political and commercial interests. But before the evolution of such standards, there were few rules (norms) on the integrity of information in mass circulation.

In this context, the time has come for the media to relate more closely to professional standards and ethics, to stop publishing unverified information and to distance themselves from information that may be of interest only to a certain category of public, but which does not represent public interest.

Therefore, the press must remember the period when all news institutions and journalists, regardless of their political orientations, avoided spreading misinformation and false information. In today's media, the elimination of positions that ensure the internal verification of information has led to some extent to the role now attributed to "*the Fifth Estate*"[40] of bloggers and other external actors who expose the mistakes made by journalists - unfortunately, after they are already disseminated.

The International Communication Development Program (ICDP) funded and developed by UNESCO, offers a new resource, a unique and holistic view of the different dynamics of the disinformation process, along with strengthening practical skills to complement the knowledge and understanding of the information presented.[41] The program represents part of the UNESCO tradition of encouraging optimal performance and self-regulation by journalists themselves, as an alternative to the risks of state intervention in tackling perceived problems in the realm of freedom of expression.

Professional standards for ethical and responsible journalism are the first line of defense against misinformation and fake news. The norms and values that represent the framework for the professional training of journalists have evolved over the years to give journalism its mission and a new *modus operandi*. In turn, they support verified information and informed comments shared in the public interest. These factors underlie the credibility of journalism and counteract the phenomenon of fake news. *Ergo,* they are woven into the very intimate fabric of ethical journalism.

[40] Fifth Estate is a socio-cultural reference to groups of different and critical points of view in contemporary society and is associated with bloggers, journalists, etc. which publish in non-mainstream media and social media.

[41] The 61st meeting of the ICDP Bureau in 2017 decided to support the Global Initiative for Excellence in Journalism Education, allocating funds specifically for the development of new programs on key topics for journalism. Progress was made at the 62nd meeting of the IPDC Bureau in 2018, which allocated an additional amount to support this curriculum.

6. Conclusions

One of the cyber security trends that need to be taken into account represents the constant desideratum to see the continuous evolution of the relevant cyber security regulations. The dynamic and fast-moving nature of cybersecurity becomes a significant area for regulation, which is far too slow to be considered a benefit and could restrict security by building a culture of compliance and a false sense of security against agile, motivated and smart enemies.

The ethical use (individual or otherwise) of information technology translates into the use in accordance with the proposed purpose of the technology, in compliance with the integrity and security of the system and is based on the implementation of general principles of good conduct, such as responsibility, vigilance and respect towards others in the daily use of ITS.

It is also of crucial importance to emphasize the contextual nature of individual ethical use. Ethical judgment regarding certain common behaviors has been largely influenced by the "professional" or "private" context in which these behaviors take place. The perception of the ethical use of ITS is much stricter in the professional context than in the social context in general, where a certain elasticity or even a laxity of the concept of ethical use is entertained. This is the case of illegal (*unlawful*) downloads which is considered morally wrong when done at work but acceptable in private life.

In addition, we consider that the pragmatic view seems to be more representative, because, without denying or dwarfing in importance the normative aspect of ethical use, users place particular emphasis on the practical consequences of acts that are expressed in the form of adopted conduct on the use of these specific instruments. In conclusion, the individual ethical use of ITSs does not constitute, as we might expect, a more or less rigorous application of moral prescriptions derived from ethical theories of philosophy or legal obligations.

If we were to conclude on the definition of the ethical use of information technology, we should take into account the architectural design of both users and the organization, and also include the different dimensions of ITS ethics. This would be a

consistent use of the technology, complying with the legal requirements, integrity and security of the system, which would take into account the interests of the parties involved and the application of general principles of good conduct such as vigilance in the daily use of technology.

Bibliographical references

[1] Apel K. O., 1994, *The Ethics of Discussion*, CERF 1994.

[2] Baltzan, P., and Phillips, A., 2008, *Business driven information systems.* New York: McGraw-Hill Irwin, 2008.

[3] Bentham J., 1789, *Introduction to the Principles of Morality and Legislation*, London, 1789.

[4] Brey, P. A. E., 2012, Anticipating ethical problems in emerging IT. *Ethics and Information Technology, 14*(4), 2012, pp. 305–317.

[5] Carl von Clausewitz, *On War*, 2018, ISBN-10: 1420957198, ISBN-13: 978-1420957198.

[6] Courdarcher M., 2008, *Kant: pas à pas*, Ellipse, 2008.

[7] Debar, Hervé, 2018, "*Intelligence artificielle, risque ou opportunité pour les cyber-défenseurs?"* Telecom, Number 190, Oct. 2018.

[8] Desai, M., Von Der Embse, T.J. and Ofori-Brobbey, K., 2008, *„Information technology and electronic information: an ethical dilemma"*, SAM Advanced Management Journal, 2008, p. 18.

[9] Dorf, R.C., 1999, *Technology management handbook*, Boca Raton, Florida: CRC Press, 1999.

[10] Gotterbarn, D., 1991, *"Computer Ethics: Responsibility Regained"*, National Forum: The Phi Beta Kappa Journal, 1991.

[11] Habermas J., 1992, *On the Ethics of Discussion*, Cerf 1992.

[12] Höffe, O., 1993, *Petit dictionnaire d'éthique*, Saint-Paul, 1993.

[13] Jonas H., 1979, *The principle of responsibility, the ethic for technological civilization*, Cerf, 1979.

[14] Jones, T.M., 1991,*"Ethical decision making by individuals in organizations: An problem-contingent model"*, Academy of Management Review 16(2), 1991, p. 367.

[15] Kant E., (Orig. 1789/1971), Foundation of the Metaphysics of Morals, trad. V. Delbos, Paris Delgrave, 1971.

[16] Kefi, H. (ed), "*Information Technology Ethics: Concepts and Practices in the Digital World"*, Cambridge Scholars Publishing, 2015.

[17] Kemp, Simon, 2020, Digital trends 2020: Every single stat you need to know about the internet, https://thenextweb.com/growth-quarters/2020/01/30/ digital-trends-2020-every-single-stat-you-need-to-know-about-the-internet/.

[18] Kempf, Olivier, 2012, „*Cyberstategy*", Paris, Economica, 2012.

[19] Levinas E., 1995, *Altérité et transcendance*, Montpellier, Fata Morgana, coll. "Essais", 1995.

[20] Maner, W., 2004, *"Unique Ethical Problems in Information Technology"* in T. Bynum and S. Rogerson (eds.), *Computer ethics and Professional Responsibility*. Malden, MA: Blackwell, 2004.

[21] Manjoo, F., 2018, *What Stays on Facebook and What Goes? The Social Network Cannot Answer*, New York Times, 19 July, 2018. https://www.ny times.com/2018/07/19/technology/facebook-misinformation.html (accessed on 15 August 2020).

[22] https://www.rt.com/usa/432604-youtube-invests-reputable-news/ (accessed on 15 August 2020).

[23] https://youtube.googleblog.com/.

[24] https://sputniknews.com/asia/201807111066253096-whatsapp-seeks-help-fake-news/.

[25] Mason, R. O.,1986, „*Four ethical issues of the information age"*, MIS Quarterly, IO (1), 1986, pp. 5-12.

[26] Mill, J. S., 1968, *Utilitarianism*, translation G. Tanesse, Paris, Garnier-Flammarion, 1968.

[27] Morin, E., 2004, The method: Ethics, Seuil, 2004.

[28] Paulette Perhach, 2018, The Mad Dash to Find a Cybersecurity Force, https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html.

[29] Posetti, J and Matthews, A, *A short guide to the history of 'fake news': A learning module for journalists and journalism educators,* ICFJ https://www.icfj.org/news/short-guide-history-fake-news-and-disinformation-new-icfj-learning-module (accessed on 15 August 2020.

[30] Reix R., 2002, *Sistemul informațional și managementul organizațiilor*, Vuibert, ediția a IV-a, Paris, 2002, p. 4.

[31] Sviokla. J.J., and Gentile, M.,1990, *Information technology in organizations: Emerging issues in ethics and policy*, Harvard Business, 1990.

[32] Tallinn Manual 2.0, Cambridge University Press, 2017.

[33] Tandoc E; Wei Lim, Z and Ling, R., 2018, "Defining 'Fake News': A typology of scholarly definitions" in Digital Journalism (Taylor and Francis) Volume 6, 2018 - Issue 2: „Trust, Credibility, Fake News".

[34] Tavani, H.T., 2007, *Ethics & Technology: ethical issues in an age of information and communication,* Wiley 2nd edition 2007.

[35] Tavani, H.T., 2013, *Ethics & Technology: controversies, questions and strategies for ethical computing*, Wiley, 2013.

[36] Weber M., *The Scholar and Politics*, Paris: Union Gén. d'Éditions, 1963.

[37] Wiener, N., *Cybernetics: or Control and Communication in the Animal and the Machine*, New York: Technology Press/John Wiley & Sons, 1948.

[38] Wiener, N., *The Human Use of Human Beings: Cybernetics and Society*, Boston: Houghton Mifflin; Second Edition Revised, New York, NY: Doubleday Anchor 1954.

[39] Wiener, N., *God & Golem, Inc.: A Comment on Certain Points Where Cybernetics Impinges on Religion,* Cambridge, MA: MIT Press, 1964.

[40] Wiener, N., 1964, *The Human Use of Human Beings: Cybernetics and Society*, Boston: Houghton Mifflin; Second Edition Revised, New York, NY: Doubleday Anchor 1954; *see also* Wiener, N., *God & Golem, Inc.: A*

Comment on Certain Points Where Cybernetics Impinges on Religion, Cambridge, MA: MIT Press, 1964.

[41] United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, available at: https://www.refworld.org/docid/3ae6b3930.html (accessed on 23 August 2020).

[42] Directive 96/9 / EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

[43] Law 8/1996 of March 14, 1996 on copyright and related rights published in the Official Gazette. no. 60/26 Mar. 1996.

[44] European Parliament resolution on the murder of journalist Jamal Khashoggi at the Saudi consulate in Istanbul (2018/2885 (RSP)).

[45] „UNESCO Science Report: towards 2030", uis.unesco.org/sites/default/files/documents/unesco-science-report-towards-2030-ex-sum-en.pdf.

[46] Resolutions of the Human Rights Council on "Promotion, protection and observance of human rights on the Internet", 20/8 (2012), 26/13 (2014), 32/13 (2016) and 38/7 (2018).

[47] European Parliament resolution of 14 January 2009 on the development of the UN Human Rights Council, including the role of the EU (2008/2201 (INI)).

[48] Resolution no. 26/9 of 26 June 2014 of the UN Human Rights Council in which it was decided to "establish an unlimited intergovernmental working group on human rights and transnational corporations and other enterprises, whose mandate is to develop an international instrument legally binding in order to regulate, in international human rights law, the activities of transnational corporations and other undertakings."

[49] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", UN Human Rights Council 6 April 2018. A/HRC/38/35. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement (accessed on 15 August 2020).

The Impact of Digital Change on the Educational Needs of Young People in Romania[1]

Eliza VAȘ, Bogdan MUREȘAN
European Studies Unit, European Institute of Romania, Romania
eliza.vas@ier.gov.ro, bogdan.muresan@ier.gov.ro

Introduction

Natural resistance to change is less visible in times of crisis when the emphasis is more on resilience and adaptation. The new context brings along a transformation in the way of thinking and acting, among governments and citizens. This allows continuity and can generate innovations where possible from the disruptive moments. Already a truism, we must not forget that in any crisis lies a latent opportunity.

Against the backdrop of the COVID-19 pandemic and the changes determined by it in terms of the use of digital technologies, we intend to analyse in the present chapter, in a non-exhaustive way, a series of phenomena and the effects they can produce with regards to adjusting the educational needs of young people in Romania.

We start by showing the general context of digital changes in education in Romania in 2020 and we refer to how the act of teaching-learning-assessment was adapted with the help of digital technologies. Subsequently, we select two phenomena that can have an impact on the development of young people's educational needs in Romania and we suggest an understanding of the framework and a series of recommendations for relevant stakeholders.

The two phenomena concern online disinformation, respectively cyberbullying. The reason for selecting these phenomena results from the high frequency of their

[1] The opinions expressed are binding only on the authors and cannot be considered as representing an official position of the European Institute of Romania. This article does not in any way engage the responsibility of the European Institute of Romania.

incidence in the public space, respectively from the attention paid to the topics by the European decision-makers.

Regarding disinformation, the European Commission has repeatedly stated that it is a major challenge for the European Union[2]. On the topic of cyberbullying, the European Parliament's Research Service[3] noted that although the phenomenon also affects adults, it has an alarming frequency among children and young people.

The context of digital change in education

Globalization, accompanied by the 4th industrial revolution and unprecedented advances in technology and artificial intelligence, is exponentially transforming the world we live in. They will continue to do so by raising new challenges and opportunities. The 21st century technologies exert power mainly because they contain rules that users must learn and follow, but also due to (or because of) access to latter's personal data. New technologies are global not only in terms of their proliferation but also in terms of their direct or indirect, tangible, or psychological consequences. Artificial intelligence systems, computer viruses, or real pathogens represent a proof of the increasingly porous nature of classical geographical borders and the complex interdependence of human societies.

The pandemic caused by the new SARS-CoV-2 coronavirus has clearly confirmed this reality and, among other things, has accelerated digitization in all public and private areas, from health, administration, and education. Lockdowns, life in isolation, and social distancing have highlighted the importance of adapting to a context in which our lives, work, and education are increasingly dependent on the digital environment. In her State of the Union 2020 address, European Commission President Ursula von der Leyen affirmed that one of EU's priorities is to be at the

[2] *Tackling online disinformation*, The European Commission, 2020, available online at https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation, accessed on 09.11.2020.
[3] *Victims of Cyberbullying*, European Parliamentary Research Service Blog, 2018, available at https://epthinktank.eu/2018/10/28/victims-of-cyberbullying-what-europe-does-for-you/, accessed on 09.11.2020.

forefront of the digital transformation, focusing on data, technology, and infrastructure.[4]

Furthermore, according to a report by the World Economic Forum, the rapid pace of implementation of new technologies, automation, and digitization in many areas will be doubled by a development of remote working processes and learning in the online environment[5]. The time spent online will be a measure of both our need and our dependence on new technologies, while digital infrastructure, and tech skills will play a key role in this equation. Concepts such as 'digital literacy' or 'information and media literacy' will be increasingly integrated into aspects of public policymaking, and education will remain the common denominator.

At the time of writing this paper (November 2020), through empirical observation and the consultation of mainly primary sources, we aim to present a series of preliminary remarks. These observations focus on the impact of digitalization on the learning needs and interests of young people in Romania, as well as the transformation of formal learning/teaching in times of pandemic:

- the transition to online teaching was initiated after the state of emergency decree from March 16, 2020; this process has drawn on a series of negative effects both on the quality and frequency of online classes, but also on the possibility for students to fully participate in digital learning sessions.
- problems related to digital infrastructure were common among schools in small towns or rural areas, and access to learning was imperilled, with increasing inequalities between students; 40% of Romanian children live in poverty or are at risk of social exclusion (UNICEF, 2020).
- a study conducted by World Vision Romania between May and June 2020 shows that around 40% of rural students have not attended online classes, and 36% of teachers have not organized online sessions; furthermore, it is shown

[4] The European Commission, "State of the Union Speech 2020", September 16th, 2020, available at https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2020_ro, accessed on 08.11.2020.
[5] World Economic Forum, "The Future of Jobs Report 2020", October 20th, 2020, available at https://www.weforum.org/reports/the-future-of-jobs-report-2020, accessed on 08.11.2020.

that over 55% of parents could not provide digital devices for each pupil in the family (World Vision Romania, 2020).

- the framework for online education and hybrid education is still in an experimental stage more than seven months after the transition to online learning and is expected to undergo further changes until it returns to a situation as close as possible to the pre-crisis "normality"[6].
- the lack of a coherent plan for the development of teachers' digital skills has led to even greater inequalities between students who benefit from online learning from trained teachers and those who receive less quantitative materials from teachers who do not know how to use digital tools; a recent analysis[7], showed that the proportion of teachers who teach in privileged schools and have digital skills is at 89%, while in the case of teachers who teach in disadvantaged schools only 54% of them have digital skills (data available for Sweden).
- less abrupt effects could be observed on the large universities in Romania, which showed flexibility and adapted quite quickly to the new context: online courses, tests, and verifications, bachelor or dissertations on the Internet, and remote admission sessions.

If we refer to the PISA results as an indicator of the national education system performance, we should be worried by the fact that Romania registered the lowest score in the 2018 PISA tests from the last nine years, according to the evaluation published by the Organization for Economic Cooperation and Development (OECD)[8]. In a significant decline and with an average of 44% functional illiteracy, today's children and young people could bring complications for the country's social assistance system

[6] *Ordinance 5.545/2020, published by The Ministry of Education on September 11th,2020,* regulates the way of carrying out the didactic activities through technology and the internet, containing the responsibilities of the students, the attributions of the teachers, and the parents within this process.

[7] Andreas Schleicher, "Advancing schooling beyond coronavirus – new insights from PISA", September 29th, 2020, available at https://oecdedutoday.com/advancing-schooling-beyond-coronavirus-new-insights-from-pisa/, accessed on 09.11.2020.

[8] OECD, "PISA 2018 Results (Volume I)", December 3rd, 2019, available at https://www.oecd.org/pisa/publications/pisa-2018-results-volume-i-5f07c754-en.htm, accessed on 08.11.2020.

in the future, and the disorderly transition to online education has the potential to exacerbate this problem.

As most functionally illiterate students come from low-income families and underprivileged environments, they often do not have access to the devices or internet connection needed for remote learning. And functional literacy is an essential condition for digital literacy, the new language of operation and communication of the 21st century. Added to all of this is the need to develop digital literacy skills and literacy among teachers and parents. As it can be seen in Table 1, only 10% of Romanian citizens have digital skills above the elementary level. Our ability to learn from the COVID-19 crisis, characterized by unprecedented use of technology in education and training, as well as to shape a new education system appropriate to the digital age, remains dependent on the elements mentioned above.

Tab. 1. *The level of digital skills among people (16-74 years) in Romania*[9]

Skills level	Romania DESI 2018 value	Romania DESI 2019 value	Romania DESI 2020 value	European Union DESI 2020 value
At least basic digital skills %	**29%** 2017	**29%** 2017	**31%** 2019	**58%** 2019
Above basic digital skills %	**10%** 2017	**10%** 2017	**10%** 2017	**33%** 2019

The purpose of this section was to identify some of the digital changes in education that occurred because of the pandemic. Given that we are tackling an ongoing event and dynamic processes, we have pointed out preliminary elements regarding the changes produced and have shown where there are vulnerabilities. In the following sections, we will focus on the recognition of malign factors present in the information society and how they can generate a paradigm shift in education. Thus, we considered relevant issues related to disinformation in the online space (including the emergence of deepfakes), respectively online harassment.

[9] Source: Index of the digital economy and society (DESI) 2020 Romania.

Disinformation in the online space and the impact on young people

The social distancing measures implemented by the authorities during the pandemic fuelled the need for people to "take refuge" in the online space, where they were exposed to the COVID-19 infodemia, a specific and very dangerous instance of disinformation, which fully benefits from the technical possibilities offered by new technologies and digitization. According to the European Union's working definition, disinformation activities involve "a series of verifiably false or misleading information, which is created, presented and disseminated for economic gain or to deliberately mislead the public"[10]. A March 2018 Eurobarometer survey showed that 85% of European citizens perceived fake news as a problem in their country and that 83% considered it a problem for democracy in general[11]. Becoming aware of the problem is always the first step towards solving it. It should be noted that, at that time, out of the total number of EU respondents, Romanians had the highest level of trust in the information they accessed through social networks and instant messaging applications.

If we assume that the "medium is the message", instant messaging applications, such as WhatsApp, can be not only a channel for sharing disinformation and wrong information (misinformation) but it can also provide content for them. In the virtual environment, disinformation campaigns, initiated by both state and non-state actors, can be orchestrated with the help of remote-controlled bots or "troll armies", which can work remotely, have low costs, ensure rapid dissemination, and have significant impact. The primary purpose of disinformation happening in the EU, regardless of its sources and channels of dissemination, is to undermine citizens' trust in national and European institutions, destabilize democratic systems and open societies, by distorting public debate. It is different from misinformation, in which the sender's intent is not to purposely deceive the receiver.

[10] The European Commission, "Questions & Answers – The EU Intensifies the Action against Misinformation", December 5th, 2018, available at https://ec.europa.eu/commission/presscorner/detail/ro/MEMO_18_6648, accessed on 08.11.2020.
[11] The European Commission, "Flash Eurobarometer on Fake News and Online Disinformation", March 2018, available at https://ec.europa.eu/digital-single-market/en/news/final-results-eurobarometer-fake-news-and-online-disinformation.

Case study - *deepfakes*

Given the increasing capacity of data processing, a booming phenomenon is that of deepfakes, which is closely linked to institutionalized disinformation. Through deepfakes, people with a high degree of notoriety are credited with false messages in a way that is extremely credible to the general public.

The process of making deepfakes involves using artificial intelligence to create an overlap between a person's image (recreated from a volume of data that the program receives) and a possible message that it would send (made from existing data about elements of para-verbal language).

In the absence of specialized knowledge about the traceability of a public speech/message (from the time it was issued to the time it was made public), many citizens may fall into the trap of sharing deepfakes. Children and young people can easily come in contact with such materials, given the high amount of time they spend online. In fact, among the dangers posed by the proliferation of deepfakes we can mention:

- Influencing democratic processes and public opinion;
- Propagation of false messages among various target groups;
- Influencing decision in various fields (e.g., political, economic, and military).

The deepfakes phenomenon has also attracted the attention of the US government, which, through the Defence Advanced Research Projects Agency, is working with several research institutes to identify deepfakes and develop programs capable of differentiating between authentic and manipulated.

Textbox 1. *Advanced methods to create fake news and messages*[12]

Although disinformation does not occur exclusively online, it has so far managed to exploit with remarkable success the vulnerabilities of the digital space and the weaknesses of human nature under its influence. Disinformation campaigns aim to hack the emotions of internet users and are interested less in appealing to their reason or critical thinking, which they often skilfully bypass or subtly discourage. As individual users share their opinions online, they become co-authors of the original message, often going beyond the status of mere consumers of information. Young people, including Romanians, as the main consumers and creators of information via

[12] Source: CNN, 2020.

social media, are the favourite vulnerable group in the face of the scourge of disinformation.

In a ranking of the most resilient countries to disinformation, published in November 2019 by the Open Society Institute Sofia, Romania placed 28th out of 35 countries analysed relative to their respective levels of media literacy. The report emphasized the quintessential importance of education and quality media for mitigating shortcomings[13]. "There is a need to integrate information and media literacy into the formal education system and to develop national policies and strategies dedicated to information and media literacy", according to an expert from the United Nations Educational, Scientific and Cultural Organization (UNESCO).[14]

Combating disinformation in the social media and online platforms era should be the product of the combined and coordinated efforts of all relevant and targeted actors, from national authorities and European institutions to academia, journalists, and, last but not least, individual consumers of virtual information. Formal and non-formal education are two sides of the same coin, and they have a complementary role when it comes to training young people and students in the perspective of making informed decisions online, being fully aware of the deeper dangers of misinformation.

On the other hand, young people not only can benefit from these programs but can be trained and co-opted to become catalysts and vectors of positive change. This can be done with the goal of developing critical thinking and emotional intelligence among consumers of virtual information. To this end, UNESCO has launched the "Capacity Building on MIL for Youth Organizations" initiative, dedicated to youth organizations and young leaders to make them aware of the importance of information literacy and media and to promote it through non-formal education.

In this way, they will be able to fully engage as active digital citizens and bring their own contribution to the academic debate on misinformation and strategic

[13] Open Society Institute, "Just think about it. Findings of the Media Literacy Index 2019", Policy Brief no. 55, November 2019, available at https://osis.bg/wp-content/uploads/2019/11/MediaLiteracyIndex2019_-ENG.pdf, accessed on 08.11.2020.

[14] Deutsche Welle, "Empowering young people - and adults - to tell fake news from facts", October 6th, 2020, available at https://www.dw.com/en/empowering-young-people-and-adults-to-tell-fake-news-from-facts/a-55128051, accessed on 08.11.2020.

communication, by preserving values such as freedom of expression and democracy. Although these endeavours are still at an early stage in Romania, if properly supported, Generation Z and not only has the potential to limit the pernicious influence of social networks, which rewards virality and emotional commitment, thus having a natural affinity for dis- and misinformation. And, why not, it could develop new applications such as "Shield", a 100% Romanian project that fights false news and misinformation at the European level and which reached the final of the EU Datathon 2020.

Online harassment and the impact of on children and young people

The pandemic has caused a series of visible changes in society and the behaviour of citizens. It has also generated a number of effects, some of which are long-term (e.g., flexibility in education) and some potentially irreversible (e.g., increased use of new technologies).

In the first part of this paper, we showed how online disinformation has become more widespread and we have developed a series of correlations with regard to educational needs of young people. Closely related to the phenomenon of disinformation is that of deepfakes, which we have studied in the context of the negative effects it can generate for influencing public opinion or launching fake news.

In this part of the article, we will focus on the analysis of another phenomenon that characterizes the digital space and that can have an impact on the paradigm shift of the educational needs of young people in Romania: online harassment (cyberbullying). The pandemic was a favourable context for the spread of various phenomena, and one of the factors underlying these changes is the increase in the time spent on the Internet among users.

Studies[15] conducted in different states show increases of up to 100% in the time children spend online. An effect of this is represented by the increase in the frequency of using social media platforms. A study conducted in the United States shows that out of 609 respondents over the age of 18, more than 67.6% of them spent extra time on

[15] COVID-19 Impact: Screen time up by 100% for children, *The Economic Times*, June 15th, 2020, available at https://economictimes.indiatimes.com/industry/services/education/covid-19-impact-screen-time-up-by-100-for-children/articleshow/76383951.cms, accessed on 09.11.2020.

social media platforms, ranging from 1-3 hours or even more (Figure 1). In this context, various researchers have pointed out that time spent online during the pandemic is a public health issue[16] and should be addressed through specific measures.

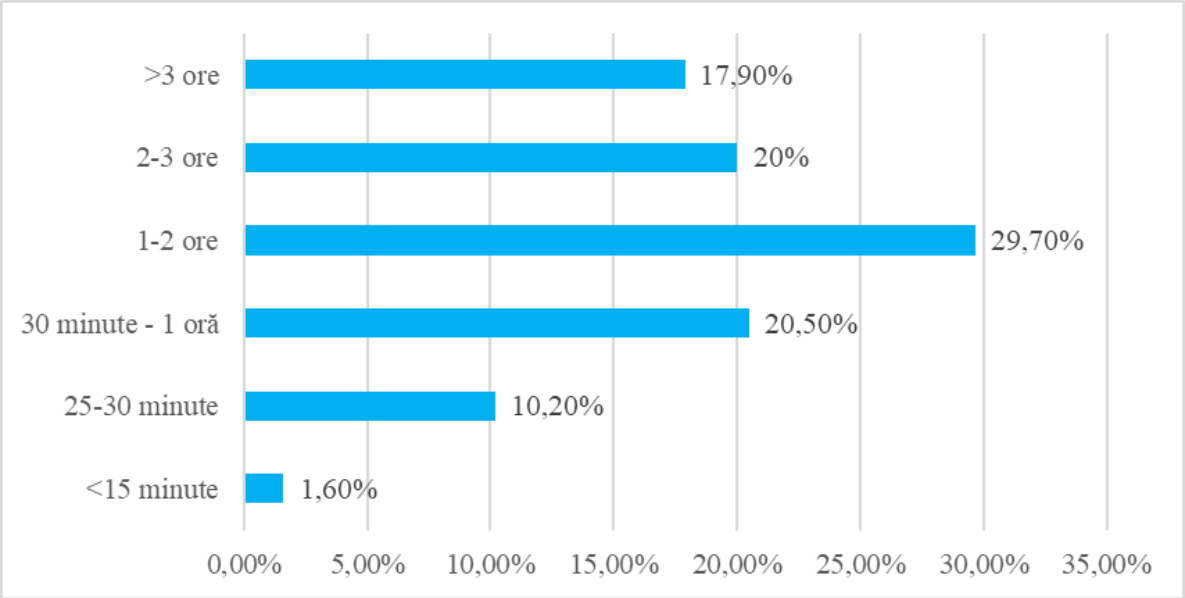


Fig. 1. *Extra time spent on social media platforms following the pandemic*[17]

Among the effects[18] that long-term accessing of digital content can generate are for children and young people, we mention: sleeping disorders, reduced school performance, lack or insufficiency of physical activity, decreased self-confidence, fear of missing out, alienation from close family, etc.

With the increased time spent online, there are more risks and dangers to which users are exposed to either directly or indirectly. One issue is the phenomenon of cyberbullying, which refers to harassment by using devices connected to the Internet. According to the platform stopbullying.gov (associated with the United States government), the most commonly used ways to trigger cyberbullying situations are social media platforms (Facebook, Instagram, Snapchat, and TikTok), SMS, and

[16] Sultana, Abida & Tasnim, Samia & Bhattacharya, Sudip & Hossain, Md & Purohit, Neetu. (2020). *Digital screen time during COVID-19 pandemic: A public health concern*, September 2020, DOI: 10.31235/osf.io/e8sg7, accessed on 09.11.2020.

[17] Additional daily time spent on social media platforms by users in the United States due to coronavirus pandemic as of March 2020, *Statista*, May 2020, available at: https://www.statista.com/statistics/1116148/more-time-spent-social-media-platforms-users-usa-coronavirus/, accessed on 09.11.2020.

[18] Screen time and children, *American Academy of Child and Adolescent Psychiatry*, no. 54, February 2020, available at https://www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Children-And-Watching-TV-054.aspx, accessed on 09.11.2020.

messaging applications (WhatsApp, Messenger, etc.), instant/direct messaging platforms or those that allow online chat, online forums and online discussion groups (e.g., Reddit), email, online gaming communities.

The phenomenon of cyberbullying manifests itself in various forms, and the most common are: harassment (refers to behaviour intended to assault/threaten a person by using digital tools), mockery (occurs when a person becomes the explicit target of derogatory messages published online), stalking (refers to the situation where a person is constantly tracked by the same user and all his actions are being monitored on one or more platforms), fraudulent use of online identity (occurs when another person has access to a user's account and associated data and takes advantage to send messages on behalf of that person), blackmail (refers to the situation in which the aggressor owns personal information about the victim, such as sensitive photos and threatens to make them public).

Children and young people are the age groups most often affected by the phenomenon of cyberbullying, and the contexts in which it can occur are both formal (e.g., in the online class group) and informal (on the platforms/applications used). In a recent study by Light, a start-up that develops artificial intelligence solutions for children's online safety, the authors show that the number of messages inciting hatred and intolerance among children and adolescents has increased by 70%, on groups of online discussion. The same study signals that the level of toxicity on online gaming platforms, such as Discord, has increased by 40%.[19]

In Romania, the data provided by the Child' Helpline Association[20] mentions that in the first six months of 2020 more than 2445 cases of abuse were registered, an increase of 15.1% compared to 2019. Among reported cases, there were instances of denigrating messages, intimidation by spreading rumours, false information, blackmailing by using images with victims in inappropriate situations, or distributing online pages with inappropriate content to minors.

[19] Rising Levels of Hate Speech & Online Toxicity during This Time of Crisis, L1ght, 2020, available at https://l1ght.com/Toxicity_during_coronavirus_Report-L1ght.pdf, accessed on 09.11.2020.
[20] Child' Helpline Association is a non-governmental organization that provides a dedicated phone line for reporting child abuse.

Given the incidence of these cases, as well as the growth of negative issues arising from the increased time spent on the Internet, online safety needs to become a cross-cutting theme in educational policies. Children and young people, teachers and parents are exposed to the dangers and risks associated with the use of devices connected to the Internet mainly due to the sheer volume of data they generate. Sometimes data end up being used for immoral or illegal purposes, violating fundamental rights of users. Therefore, one of the pillars of online education should be the safety of the internet and the certainty that every young person is in a safe space when accessing the internet.

Conclusions

Through this article, we aimed to identify those phenomena that can have an impact on adjusting the educational needs of young people, such as disinformation and harassment in the online environment. For each section, we provided contextual elements, chief among resides the COVID-19 pandemic and its impact on the acceleration of those phenomena. In the last part of the material, we draw a series of conclusions that can serve as recommendations for concrete actions by the interested actors.

Highlighting pre-existing issues

With regard to the education sector, the pandemic highlighted problems that already existed, accelerating their general level of visibility. Thus, the vulnerabilities arising from the online schooling were based on the poor development of the digital infrastructure, respectively the low level of digital skills among teachers, parents, and even students.

The ongoing transition to online education

The lack of a clear plan to make the transition to online and hybrid education has led to disruptive times for millions of students and teachers in Romania. For the next period, it would be useful to analyse the vulnerabilities and lacks in the education

system found during the pandemic, an analysis that should be done both centrally and locally. It would also be useful to identify the positive changes that have occurred in the teaching-learning-assessment process (such as the creation of digital teachers' communities, facilitating communication between students and teachers). We need to learn on the go to overcome the current crisis and recognize the positive effects so that we can turn them into long-term achievements.

Disinformation is popular

Young people, as the main consumers of information on social media, represent the preferred targeted group in the face of the scourge of disinformation. In this regard, it would be useful to introduce media literacy courses and the development of critical thinking both in pre-university education and in the curricula of some profile faculties. Countries such as Finland, Sweden, and the Netherlands have introduced digital literacy and critical thinking classes against disinformation since primary school, and the results show.

Online safety as a cross-cutting theme in education

Although online security was a challenge even before the pandemic, this dimension has grown exponentially in complexity given the high volume of data collected about users. In this regard, activities for the development of digital skills and knowledge of online security features are recommended[21]. These can be done in partnership with non-governmental organizations that have the expertise to work non-formally with young people.

[21] More details about such an activity carried out by the Young Initiative Association in 2020 can be found in the report Safe Net Builders - Summer School on Cyberbullying for Adolescents, Young Initiative Association, September 2020, available at https://www.younginitiative.org/wp-content/uploads/2020/09/Raport_Safe-Net-Builders.pdf, accessed on 10.11.2020.

References

[1] Additional daily time spent on social media platforms by users in the United States due to coronavirus pandemic as of March 2020, *Statista*, May 2020, available at https://www.statista.com/statistics/1116148/more-time-spent-social-media-platforms-users-usa-coronavirus/, accessed on 09.11.2020.

[2] Andreas Schleicher, "Advancing schooling beyond coronavirus – new insights from PISA", September 29th, 2020, available at: https:// oecdedutoday.com/advancing-schooling-beyond-coronavirus-new-insights-from-pisa/, accessed on 09.11.2020.

[3] Young Initiative Association, *Safe Net Builders – summer school on cyberbullying for teenagers*, September 2020, available at https://www.younginitiative.org/wp-content/uploads/2020/09/Raport_Safe-Net-Builders.pdf, accessed on 10.11.2020.

[4] The European Commission, "State of the Union Speech 2020", September 16th, 2020, available at https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2020_ro, accessed on 08.11. 2020.

[5] The European Commission, "Flash Eurobarometer on Fake News and Online Disinformation", March 2018, available at https://ec.europa.eu/ commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183, accessed on 08.11.2020.

[6] The European Commission, "Questions & Answers – the UE the Action against Misinformation", December 5th, 2018, available at https://ec.europa.eu/commission/presscorner/detail/ro/MEMO_18_6648, accessed on 08.11.2020.

[7] COVID-19 Impact: Screen time up by 100% for children, *The Economic Times*, June 15th, 2020, available at https://economictimes.indiatimes.com/industry/services/education/covid-19-impact-screen-time-up-by-100-for-children/articleshow/76383951.cms, accessed on 9.11.2020.

[8] Deutsche Welle, "Empowering young people - and adults - to tell fake news from facts", October 6th, 2020, available at https://www.dw.com/en/empowering-young-people-and-adults-to-tell-fake-news-from-facts/a-55128051, accessed on 08.11.2020.

[9] OECD, "PISA 2018 Results (Volume I)", December 3rd, 2019, available at https://www.oecd.org/pisa/publications/pisa-2018-results-volume-i-5f07c754-en.htm, accessed on 08.11.2020.

[10] Open Society Institute, "Just think about it. Findings of the Media Literacy Index 2019", Policy Brief no. 55, November 2019, available at https://osis.bg/wp-content/uploads/2019/11/MediaLiteracyIndex2019_-ENG.pdf, accessed on 08.11.2020.

[11] Ordinance 5.545/2020, published by The Ministry of Education on September 11th, 2020, regulates the way of carrying out the didactic activities through technology and the internet, containing the responsibilities of the students, the attributions of the teachers, and the parents within this process.

[12] Rising Levels of Hate Speech & Online Toxicity during This Time of Crisis, L1ght, 2020, available at https://l1ght.com/Toxicity_during_coronavirus_Report-L1ght.pdf, accessed on 09.11.2020.

[13] Screen time and children, *American Academy of Child and Adolescent Psychiatry*, no. 54, February 2020, available at https://www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Children-And-Watching-TV-054.aspx, accessed on 09.11.2020.

[14] Sultana, Abida & Tasnim, Samia & Bhattacharya, Sudip & Hossain, Md & Purohit, Neetu. (2020). Digital screen time during COVID-19 pandemic: A public health concern, September 2020, DOI: 10.31235/osf.io/e8sg7, accessed on 09.11.2020.

[15] Tackling online disinformation, The European Commission, 2020, available online at https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation, accessed on 09.11.2020.

[16] Victims of Cyberbullying, European Parliamentary Research Service Blog, 2018, available at https://epthinktank.eu/2018/10/28/victims-of-cyberbullying-what-europe-does-for-you/, accessed on 09.11.2020.

[17] World Economic Forum, "The Future of Jobs Report 2020", October 20th, 2020, available at https://www.weforum.org/reports/the-future-of-jobs-report-2020, accessed on 08.11.2020.

From the Privacy Paradox to Collective Action. Challenges of a Privacy and Data Protection Course

Prof. univ. dr. Răzvan RUGHINIȘ
Faculty of Automatic Control and Computers,
University Politehnica of Bucharest,
Romania
razvan.rughinis@upb.ro

Introduction

The issue of the use and protection of personal data is becoming increasingly relevant. On the one hand, big data is the key to innovation and the creation of solutions to complex social and economic problems. On the other hand, the exploitation of personal data on an increasingly large scale raises previously unsuspected risks, from diminishing the personal autonomy of citizens and consumers, to undermining the organization of democracies and competitive markets. In this context, the importance of cultivating the thematic sensitivity of the public and developing the skills of future experts, who will create and implement data use and security strategies, is growing. In this article I will discuss the challenges of a university course on privacy and data protection, a course I developed within the Advanced Cybersecurity master's program at the Faculty of Automatic Control and Computers, University Politehnica of Bucharest[1].

The first challenge that a professor must overcome in creating such a course is the so-called "privacy paradox". Although users of digital technologies usually state that the protection of privacy is very important, in practice they often provide their diverse and sensitive personal data in exchange for minor rewards [1]. In other words, there is a systematic gap between words and actions, when it comes to the protection of personal data. This gap is exacerbated by the fact that users are often unaware of the

[1] More information on the Advanced Cybersecurity master program is available online at https://acs.pub.ro/en/academics/master-of-science-studies/ and http://acs.pub.ro/doc/master/ro/short_description/SAS-short-en.pdf

data they transfer to the digital service providers they interact with, or of the data movement or use once it has been transmitted [2]. Last but not least, the privacy paradox also reflects the aggressive policies of collection, consolidation, and use of personal data of the companies interested mainly in the profitability of their products and services, and less in the transparency for users [3].

The privacy paradox is not only a scientific construct, but it captures very well the ambivalent reactions of students to this topic. On the one hand, they accept the importance of the discussion, but on the other hand, they do not feel the risks or costs of collecting and misusing data as their own, personal problems. The risks and costs of violating privacy are perceived as distant concerns, of other people (possibly more technologically naive), or problems with an abstract bureaucratic connotation. Students in computer science and engineering feel even more in control of their own actions about digital technologies, compared to other young people, given their expertise and immersion in this world. The first challenge of a course on privacy and data protection, therefore, is to translate the issue of privacy into up-to-date questions and answers for students, which resonate with their current experiences and concerns.

The solution I have gradually developed and tested since 2018 in the course of Privacy-Enhancing Technologies is to anchor the discussion in four key points of direct interest to students: equity, free choice, dependence, and friendship or community. These are specific manifestations of four distinct analytical perspectives, through which students can better capture what is at stake when talking of privacy and data protection, beyond their direct and personal relevance: the ethical perspective, economic perspective, psychological perspective, and sociological perspective. Hereafter I will briefly discuss each of these perspectives, concluding with the lessons I have learned so far, while developing and teaching this class.

Ethical Perspective

Why would we care about the protection of private data? The data we provide, more or less consciously, on the digital platforms and applications we use daily does not appear to us as a real, tangible loss - while the free use of these services is a valuable

benefit. However, in recent years it has become clear, both in the scientific literature and in the debates of legislators and public controversies, that an important price we pay for free digital services is to reduce our autonomy of individual and collective action [3], [4]. Personal data is the main ingredient in what Shoshana Zuboff calls "predictive products" [4], those specific interventions in the user's attention span designed to influence their behavior - whether it's buying, watching, or voting on a particular element, to the detriment of another. As each of us becomes more predictable to technology giants and all organizations that use their data-based prediction services, we lose our individual freedom of choice and our social capacity for democratic governance. Predictive algorithms have the power to approach each of us individually and adaptively. This is unlike the advertising of previous eras, such as posters or TV commercials, which evenly addressed a wide audience and could not detect in real-time the individual reactions. The resulting diminishment of personal autonomy, in the sphere of consumer behavior but, especially, in the sphere of civic and political behavior, is a strong ethical argument in favor of controlling the massive flow of data available to interested organizations to control our behavior. The critical dramatization The Social Dilemma [5], released in 2020, is a useful resource for students, both through the clarity of a persuasive synthesis of critical views on the impact of social networks and by bringing to the fore some visionaries and technical entrepreneurs who signal the current risks of data capitalism. Students in computer science and engineering can thus see that the issue of privacy protection is acute for the elites of IT engineering and entrepreneurship, with whom they resonate more than with other professional categories. Interviews given over the years by prominent personalities in the evolution of the digital sphere, such as Tristan Harris, Jaron Lanier, Tim Kendall, and Justin Rosenstein, available online, are an attractive source of information for students.

However, there is an even more resonant ethical consideration with the current sensibilities of young people than the degradation of freedom of choice, namely the issue of equity. Evidence of unfair treatment arouses emotions of indignation and a desire to react, to punish, and to correct - as shown by numerous psychological studies

[6]. The first dimension of the injustice induced by the new data capitalism consists in the asymmetries of information and control between digital platforms and the companies participating on these platforms, which is related to the economic logic of the degradation of free competition. The second dimension of injustice refers to the power asymmetries between large corporations and individual users, which is mainly related to the psychological and sociological perspectives.

Economic Perspective

The increase in economic power and the influence of the big technology giants are easy to notice in synthetic indicators, such as turnover, number of users, or their share in a given market. All the more remarkable is the consolidation of their economic power during the global crisis triggered by the COVID-19 pandemic. Technology platforms create markets on which significant proportions of the world's population play as bidders or consumers - from information markets created by search engines like Google, Bing or Yahoo, to digital application markets like Google Play or App Store, to retail markets such as Amazon Marketplace, real estate markets such as Airbnb or Booking.com, transportation markets such as Uber or Lyft, as well as crowdsourcing or micro-jobs labor markets such as Amazon Mechanical Turk or Yandex.Toloka. Over the years, repeated investigations have documented abusive practices of dominating the competition and gaining greater market share through non-competitive methods, including three EU decisions against Google [7] and, more recently, the report on the results of the US parliamentary inquiry of the United States on Amazon, Apple, Facebook and Google [8]. People working on crowdsourcing platforms gain flexibility, but lose the security and stability of a minimum wage income, insurance, and other protection measures granted in modern labor states.

A market is competitive and allows freedom of choice if many bidders and buyers are present, offering comparable goods under relatively symmetrical information [9]. Information asymmetry is the key to concentrating power in the new data capitalism, given that platforms and big players have access to large volumes of real-time information, both about the competitors playing in the markets they create

and about individual buyers. This blatant asymmetry of information limits individual freedom of choice and action in a cumulative process, as markets become increasingly digitized and focused on platforms that monopolize access to data. Moreover, at the second level of degradation of individual autonomy, we observe the transformation of users into resources, our attention and time being exploited, leading to the emergence of new forms of digital dependence. These processes are further explored from a psychological perspective.

Psychological Perspective

If large platforms create markets where there are both arbitrators and players, disadvantaging participants to gradually promote their own products and market shares, the power asymmetry is even greater in the relationship between digital service providers, especially social media networks, and their individual users. Business models based on converting time spent on platforms into monetizable clicks and stimulating an increasing amount of attention invested in these platforms lead to the emergence of new forms of dependence [10], [11]. Studies on large adolescent populations in the US and the UK show that intensive use of social networks significantly increases the risks of psychological problems and suicide, the association being higher for girls than for boys [12]. Perpetual fragmentation of attention reduces the depth of thought [13] while easy access to information offers the possibility or, more often, the illusion of cognitive amplification, with the risk of misinformation and manipulation [14]. The considerable benefits that digital technologies bring in streamlining organizational processes and overcoming time and space boundaries cannot be denied. At the same time, the benefits do not negate the costs, and understanding the risks and their evolution is necessary for a better balance of the impact of technologies in personal and professional life.

Sociological Perspective

Individual vulnerabilities amplified by dependence on digital technologies and business models that convert online time into advertising revenue are aggregating into

new relationships and social structures. Social networks redefine friendship, dating applications redefine intimacy [15], [16], collaborative platforms redefine knowledge [17], and even posthumous existence is transformed into new digital configurations [18]. These new social structures are associated with processes of distorting reality through content bubbles [19] and polarizing discourse on political, scientific, and public health issues, such as vaccination [20] or managing the COVID-19 pandemic.

Public policies on data protection and privacy technologies do not, in fact, refer only to private life, but also to public life. As Helen Nissenbaum observes, we cannot talk about the existence of a clear private/public border, but rather about information flows that cross both fields, respecting certain social and legal norms of relevance and adequacy to the context [3]. However, the author notes that the new data capitalism has disrupted these flows, with personal data being collected, marketed, and aggregated in markets where the initial context of the collection is erased. Through a unique identifier (marketing ID), the data are consolidated in an individual profile, which is completed by inferences starting from the actions of other individuals who are similar to us, and by predictive models that classify individuals and detect patterns (see Fig. 1).

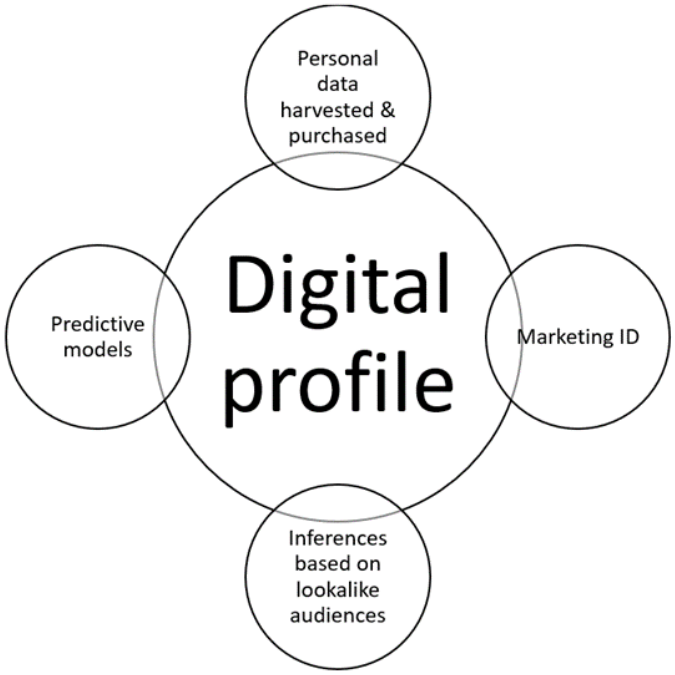


Fig. 1. *The structure of digital profiles*

In data markets, the traces of our actions become a commodity, and, implicitly, human users become products. Therefore, Zuboff [4] denounces surveillance

capitalism as a form of social organization that commercially exploits human behavior to a new level. By turning the traces left by our online choices into predictive products designed to change consumer or voter behavior in the profitable directions chosen by corporations, the new form of capitalism affects political and economic freedom of choice and transforms human societies into continuously measured and predictively monetized resources (idem).

Through the discussions conducted during the course, I encourage students to observe three main drivers of data capitalism, highlighted in the literature (see Fig. 2).

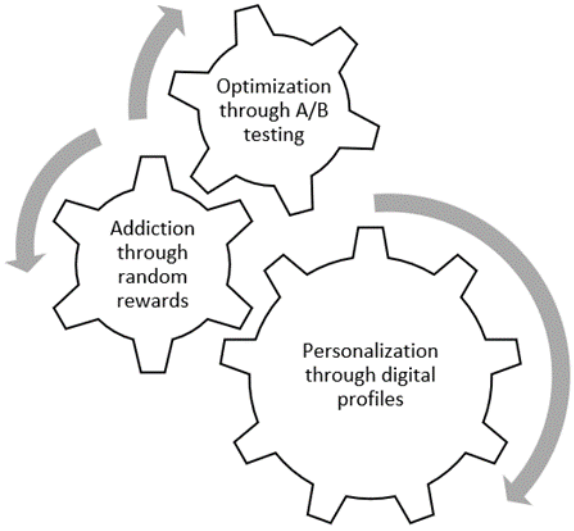


Fig. 2. *Drivers of data capitalism and digital predictions*

The most important component is the collection and use of massive personal data by aggregating digital profiles and using them to personalize content [4]. The second consists of the continuous, experiment-based optimization of the content of digital platforms and products through "A/B testing" [21], aiming at maximizing organizations' predictive efficiency and control over the users' actions. Last but not least, social networks and other digital products use techniques from the gaming industry, such as randomly distributed rewards, to create a psychological addiction and increase the time and attention invested in such products [22]. The three mechanisms increase the power asymmetry between organizations offering digital products and their users.

Conclusions

A course dedicated to privacy and the protection of personal data risks placing students in the position of passive victims, powerless in the face of the force of the great digital giants. This position is neither truthful nor constructive, sparking off rejection reactions from young people, who are driven primarily by a passion for technology and the desire to transform society for the better, through the power of digital innovation. Throughout the course, it is essential to emphasize students' possibilities for action concerning new technologies. We can envision at least three available roles. First of all, as users of digital technologies, we can use various tools to protect ourselves from intrusions and to manage our digital profile in the spirit of the identity we want to make public. Secondly, as experts in the design and development of these technologies, we can closely follow the direction taken by the products created by the corporations we work with, reacting to possible anticipated negative consequences, including through whistleblowing actions. Non-governmental organizations make it possible to involve experts in collective action, from monitoring new technologies, to reporting their abuses in court and to formulating legislative proposals. Last but not least, students are also the future designers of public policies, as civil servants or politicians, being able to consider the possibility of creating new regulations on the flows of personal data and their legitimate uses. We are talking here about both private data protection policies, such as the GDPR, and about building infrastructures through which individual users can directly benefit from their own data - such as the concept of "data trust" or a regulated and fair market for personal data [23], which would allow individuals to capitalize on data by mediating their relationships with organizations interested in processing them.

Therefore, the general message of the course is to sharpen our spirit of observation through sensitizing concepts, as a prerequisite for individual and especially collective action. We will thus arrive in a better position to redirect digital technologies in support of democracy and competitive markets through informed positions and collective actions of users, experts, and public policy designers.

Bibliography

[1] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," Computers and Security, vol. 64. Elsevier Ltd, pp. 122–134, 2017.

[2] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," Science, vol. 347, no. 6221. AAAS, pp. 509–514, 2015.

[3] H. Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press, 2010.

[4] S. Zuboff, The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books, 2019.

[5] J. Orlowki, The Social Dilemma. SUA: Netflix, 2020.

[6] D. T. Miller, "Disrespect and the Experience of Injustice," Annu. Rev. Psychol., vol. 52, no. 1, pp. 527–553, 2001.

[7] European Commission, "Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising," 2019.

[8] J. Nadler and D. N. Cicilline, "Investigation of Competition in Digital Markets. Majority Staff Report and Recommendations," 2020.

[9] L. Herzog, "Markets," The Stanford Encyclopedia of Philosophy. 2017.

[10] C. S. Andreassen, "Online Social Network Site Addiction: A Comprehensive Review," Current Addiction Reports, vol. 2, no. 2. Springer, pp. 175–184, June 1st, 2015.

[11] D. J. Kuss și M. D. Griffiths, "Online Social Networking and Addiction - A Review of the Psychological Literature," Int. J. Environ. Res. Public Health, vol. 8, no. 9, pp. 3528–3552, 2011.

[12] J. M. Twenge și G. N. Martin, "Gender differences in associations between digital media use and psychological well-being: Evidence from three large datasets," J. Adolesc., vol. 79, pp. 91–102, 2020.

[13] N. Carr, The Shallows. What the Internet is Doing to Our Brains. New York: W. W. Norton & Company, 2010.

[14] C. Voinea, C. Vică, E. Mihailov and J. Savulescu, "The Internet as Cognitive Enhancement," Science and Engineering Ethics, vol. 26, no. 4. Springer, pp. 2345–2362, 2020.

[15] M. V. Stoicescu, S. Matei, and R. Rughinis, "Sharing and privacy in dating apps," in Proceedings – 2019, 22nd International Conference on Control Systems and Computer Science, CSCS 2019, 2019, pp. 432–437.

[16] M. V. Stoicescu and C. Rughinis, "Learning about self and society through online dating platforms," in eLSE 2020 eLearning & Software for Education, 2020, pp. 513–522.

[17] C. Rughiniș, "Citizen science, gallaxies and tropes: Knowledge creation in impromptu crowd science movements," in Proceedings of the Networking in Education and Research: RoEduNet International Conference 2016, pp. 1-6.

[18] Ș. Matei, "Responsibility beyond the grave: Technological mediation of collective moral agency in online commemorative environments," Design Issues, vol. 34, no. 1, pp. 84–94, 2018.

[19] E. Pariser, The filter bubble: What the Internet is hiding from you. London: The Penguin Press, 2011.

[20] N. F. Johnson et al., "The online competition between pro- and anti-vaccination views," Nature, vol. 582, no. 7811, pp. 230–233, 2020.

[21] M. Esteller-Cucala, V. Fernandez, and D. Villuendas, "Evaluating Personalization: The AB Testing Pitfalls Companies Might Not Be Aware of—A Spotlight on the Automotive Sector Websites," Front. Artif. Intell, vol. 3, p. 20, Apr. 2020.

[22] T. Haynes, "Dopamine, Smartphones & You: A battle for your time," Science in the news, 2018. [Online]. Available at: http://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/. [Accessed: 05-Jan-2020].

[23] A. Artyushina, "The EU is launching a market for personal data. Here's what that means for privacy," MIT Technology Review, Aug-2020.

Cybersecurity for Online Learning

Prof. univ. dr. Răzvan BOLOGA, Assist. univ. dr. Tiberiu-Marian GEORGESCU
The Bucharest University of Economic Studies, Bucharest, Romania
razvanbologa@ase.ro, tiberiugeorgescu@ase.ro

Abstract: This article approaches the subject of cybersecurity in universities. It describes the main threats, actors, and solutions for the e-learning platforms' owners. Another contribution of the article is the identification of methods to protect the educational digital assets, which consist of all digital resources which facilitate the educational process in an institution. Without these assets, the educational process is significantly affected. In the last section, the authors describe a real cyberattack that took place against a Romanian university in late 2020. The article explores the main causes, presents the impact, and proposes solutions to prevent such incidents in the future.

1. Introduction

In the last two decades, the popularity of e-learning platforms gradually increased as a natural result of constant digitalization growth. In the early 2000s, educational institutions started to modernize teaching methods by implementing e-learning platforms. However, these electronic resources complemented traditional methods and usually did not play an essential role in the teaching process. With the decrease in internet service costs and the spread of internet usage on a large scale, e-commerce platforms became essential tools in many institutions. However, the peak of the importance of online learning has been reached after the implementation of the lockdown measures caused by COVID-19 pandemic. In that context, the teaching process in many institutions started to take place only on the internet environment and relied on e-learning platforms.

2. Cybersecurity particularities of the e-learning platforms

Cyber attacks on e-learning platforms have been spread since 2 decades ago. Articles [1], [2] and [3] describe the main aspects of these attacks. Usually, these incidents involved some impact, but since the educational process usually did not rely only on e-platforms, the damage was not critical for most of them.

Usually, the main three types of e-learning platforms users are students, lecturers, and admins. Article [4] discuss the main threats from each user's perspective. Generally, cyber incidents can be classified into several categories by the type of loss: confidentiality, integrity, or availability. Legally, protecting the data confidentiality of e-learning systems became of great importance only in 2016, when the European Union adopted the General Data Protection Regulation (GDPR).

3. Security challenges on e-learning platforms arising from COVID-19 pandemic

During the Coronavirus pandemic, the risks caused by e-learning cybersecurity attacks dramatically increased since the educational process is based mainly or entirely on online platforms. The integrity and availability of electronic educational resources are now crucial whereas in their absence the teaching activity is not possible.

Important steps have been taken in recent years to create an appropriate legislative framework to ensure an optimal level of cybersecurity in the EU. At the present, for the European Union, the most important legislative change can be considered the NIS Directive (The Directive on Network and Information Systems Security) on "some measures for a high common level of security of networks and information systems". The premise of its adoption is based on the socio-economic importance of cybersecurity, based on the consideration that "networks together with information systems and services play a vital role in society and their reliability and security are essential for economic and societal activities and, in particular, for the functioning of the internal market". "The NIS Directive provides for minimum security measures and security incident reporting requirements with a significant impact on

operators of key services in seven sectors: energy, banking, health, water, transport, financial market infrastructure, and digital infrastructure" [5].

According to [1], in many national strategies, the education infrastructure which consists of students, teachers, schools, universities, libraries, and all the other elements of the educational structure of a state is considered a critical infrastructure. Since the teaching process is now conducted mainly online, new cybersecurity measures for educational institutions are necessary.

The current context requires a paradigm shift in how we perceive and manage educational resources. A new approach is necessary, which pays much more attention to digital educational resources. These resources can be called **educational digital assets**.

4. The cyberattack use case of a university in Romania

In October 2020, the system of the Bucharest Universities of Economic Studies stopped working. Both the university governance systems and the administrative IT systems suddenly become unavailable. Professors were not able to log-in to the university's online platform, students were unable to download materials and accountants were unable to view the financial records.

It was a ransomware attack. The university took some time to understand what was happening and no ransom was paid. As a consequence, the entire data has been lost. The attackers did encrypt some of the back-up servers as well which reflects careful planning of the attack.

The steps of the attack

The attack exploited the most vulnerable part of the system: the human users. It was not a sophisticated attack at all. A bot simply scanned the web surface and identified vulnerabilities on one or more personal workstation which were remotely connected to the key components of the university's platform.

The university did have cybersecurity systems in place. It used a complex set stack of technologies to protect its systems. The only problem was that many professors

from the university found these systems uncomfortable and openly demanded the deactivation of the VPN (Virtual Private Network) and asked the security personnel to enable remote desktop connections.

As a historical note, the online platform of the university has been in use since 2012. However, using the online platform was optional and only some faculty members used it. During the COVID-19 lockdown that was implemented in Romania in March 2020, all faculty members had to use it for all lessons.

This has created a situation where a large number of faculty members had to invest additional efforts in connecting to the systems of the university. The university governance system for storing the grades of the students was only accessible via a VPN. This security measure comes under fire. Numerous faculty members asked for the removal of the restrictions to connect via the remote desktop connection.

At some point, during the summer, there were hundreds of remote desktop connections that were open on various computers inside the university. The number grew from just a few two hundred in a matter of months. This happened in spite of the IT Departments' strong recommendations to avoid such insecure connections.

It was not difficult for an attacker to use one of these remote desktop connections to enter the network of the university. The attackers took their time to understand the structure of the network in order to identify the various components, including the back-up servers.

The duration of the attack was not known. It is estimated based on some empirical observations that it took several weeks from the moment of the initial penetration of the network until the moment when the servers were encrypted.

The final part of the attack was carried out in a moment when the visibility was at its peak. The servers were encrypted a few days after the new academic year started. This shows that the attackers wanted to maximize the impact of their actions.

The main problem was the encryption of the digital assets of the university. Over the years, the university produced substantial amounts of courseware that was located on various machines located in the data center. The courseware included constant, collections of code, custom educational platforms, and many others.

The malware code that encrypted the digital assets of the university created a major disruption. Many faculty members were unable to get in touch with their students and all systems were down including the email servers.

The university did not have only a single institutional repository to store the digital assets, but many. Each faculty member created a version of his/her digital assets and only a part of them had up-to-date back-ups. Even after the recovery of the systems, some digital assets (such as courses, pieces of code, videos, etc.) could not be restored.

No ransom was paid by the university. The process of recording the data took about 6 weeks and some elements were never recovered. There were major issues in terms of obtaining some financial information and the human resources department had to reconstruct a large part of its database. Apart from losing some of its digital assets, the university had to cover substantial losses due to the time spent by its personnel in order to retrieve the lost data. The situation was further complicated by a peak of infections that took place in November in Romania. This limited access to the premises of the university. The main causes that were identified and are discussed below.

Security measures often conflict with a system's performance or user experience. Due to poor user experience, many faculty members refused to use the secure access methods that were provided. This shows that the user experience is an important component of the process of protecting the network of an organization against cyberattacks.

Using remote desktop connections was certainly not a good idea. This was known to cybersecurity experts. However, regular users had a different opinion and the latter prevailed.

The improperly updated systems that some faculty members used in their homes were another major security vulnerability. Even if the systems of the universities were properly maintained, the cyberattackers were able to easily penetrate into the home computers of some faculty members.

The lack of proper training was another major issue. Should faculty members have been better trained, the chances of the attackers would have been considerably reduced.

5. Conclusion

In conclusion, we can say that it is essential to consider the user-friendliness of the security software that is installed in organizations. As the above events show, software that offers a poor user experience will not be accepted by its users even if it is related to cybersecurity. For many years engineers have created cybersecurity software thinking mostly about ways to maximize technical performance and security. It is also important to create user-friendly software that normal users are willing to accept.

References

[1] Udroiu, A. M. (2017). The cybersecurity of elearning platforms. In *Conference proceedings of» eLearning and Software for Education «(eLSE)* (Vol. 3, No. 01, pp. 374-379). "Carol I" National Defence University Publishing House.

[2] Mihai, I. C., Pruna, S., & Petrica, G. (2017). A Comprehensive Analysis on Cyber-Threats Against Elearning Systems. In *The International Scientific Conference eLearning and Software for Education* (Vol. 3, p. 344). "Carol I" National Defence University.

[3] Zalaznick, Matt (2013). Cyberattacks on the rise in higher education. *University Business* (2013).

[4] Defta, C. L., Serb, A., Iacob, N. M., & Baron, C. (2014). Threats analysis for E-learning platforms. *Knowledge Horizons. Economics*, *6*(1), 132.

[5] European Parliament and of the Council (2016), The NIS Directive, Available on https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC, Accessed on November 21, 2020.

The Challenges of the Digital Revolution in Politics. Education for a Digital Society[1]

Mihai SEBE, PhD
European Institute of Romania
mihai.sebe@ier.gov.ro

To better analyze the shape of things that will come, we must first start from certainties, namely: you can always rely on the fact that the future that will come inexorably and will affect us all, whether we want to or not. To understand it, it is important to offer a series of **conceptual clarifications**. When we talk about the **digital revolution**, a useful definition would be that we are talking about a "general acceleration in the pace of technological change in the economy, driven by a massive expansion of our capacity to store, process and communicate information using electronic devices". Originating in the 1950s-60s, the digital revolution will be accelerated by the invention of the microprocessor in the 1970s [1].

By **digital age**, I mean the "a historical period marked by the widespread use of digital technologies in different aspects of human activity, including the economy, politics and most forms of human interaction. This widespread use of digital technologies implies a profound transformation of social, economic and political systems, in the same way as the steam engine or electricity transformed past societies" [1]. The digital revolution is marked by a series of inflections in society:

1. *The digital revolution is leading to periodic "revolutions" in the methods and tools used in the economy rather than following linear and incremental trends.*
2. *There is a time lag between the initial big bang of innovation provoked by a technological revolution and its full transformation of the socioeconomic structure.*

[1] The opinions expressed are those of the author only and should not be considered as representative of the European Institute of Romania's official position.

3. For a technological revolution to produce valued and shared and benefits to society, the institutional framework has to significantly change in order to deal with the broad socioeconomic implications of the new forms of economic activity. [1].

The digital age has thus witnessed the evolution of the concept of democracy, more precisely the emergence of what is called ***e-democracy***. From the multitude of definitions available, I opt for the following definition of the e-democracy "is defined as the support and enhancement of traditional democracy by means of ICT, and which can complement and reinforce democratic processes by adding elements of citizens' empowerment through different online activities that include, amongst others, **e-government**, **e-governance**, **e-deliberation**, **e-participation** and **e-voting**" [2].

We have specified in the above definition the necessary elements of a digital democratic system, elements that need to be detailed, each of which sometimes involves a different level of digital skills and facilities offered by the public system.

For example, we have the case of **e-participation**, which often involves the development of **central electronic portals** designed to provide a range of services such as information provision, consultation platforms, electronic services, etc. [3].

A good example of this is that of Estonia and the e-participation tool developed within this country - **Osale**. This participation portal allows open consultation and inclusive policy development, the purpose of the government portal being to allow bilateral communication between voters and decision-makers.

This portal has three basic functions:

1) deliberation - citizens and interest groups can launch initiatives for new legislative proposals, present ideas and critique to government and submit petitions;
2) participation – citizens can participate in public consultations/hearings;
3) information - government agencies publish information about forthcoming policy decisions and relevant public consultations [4].

However, all these digital transformation processes are useless or inefficient if they do not provide a minimum set of conditions "to avoid any kind of discrimination on the grounds of digital skills or lack of resources and infrastructures" [5].

This brings us to **the importance of digital education** and the recommendations that the Member States and the EU need to:

- ✓ "provide educational and technical means for boosting the democratic empowerment of citizens and improving ICT competences, and to supply digital literacy and equal and safe digital access for all EU citizens in order to bridge the digital divide (e-inclusion), for the ultimate benefit of democracy;
- ✓ integrate the acquisition of digital skills into school curricula and lifelong learning, and to prioritise digital training programmes for elderly people;
- ✓ supports the development of networks with universities and educational institutions to promote research on and implementation of new participation tools;
- ✓ promote programmes and policies aimed at developing a critical and informed appreciation of the use of ICT" [6].

An important milestone is provided by an analysis dedicated to digital education, developed for the European Parliament, which offers a series of recommendations and policy options. We thus have four key actors in the process of rethinking digital education, namely: policy-makers and public administration; students and parents; educators and trainers, respectively businesses and employers, each with their own strengths and weaknesses [7].

Among the mentioned options we have the following:

First option – Incorporating education in the digital age into existing and future research frameworks to further promote evidence-based policy

Topics covered: teaching methods for the digital age; impact and useful applications of artificial intelligence in education, including personalized learning content; applied research to guarantee the scientific foundations of teaching software; acceptance research on how teachers can be encouraged to adjust teaching methods to the requirements of the digital age.

Second option – Supporting the creation of a knowledge-sharing platform for education in the digital age

The platform in question could: provide information, methodologies, data, expertise, good practice examples and advice and guidance; align the resources and strategies of different stakeholders; promote a collaborative environment with mutual learning, transnational cooperation, and innovation partnerships; incorporate helpful tools such as maps, catalogs, visualisations, etc.

Third option – Simplifying and harmonizing the recognition and validation of lifelong learning

Promote the coordination of existing structures in a single system comprising a simplified and harmonised certification process aligned with all major stakeholders in the education sector, including new digital learning providers and public administration in the Member States.

Fourth option – Offering a harmonised, yet versatile cloud solution for the provision of high-quality (open) educational resources

One way to support educators and students in integrating digital technologies into the learning process would be to reduce opacity by supporting harmonised, yet versatile standards and interoperability [8].

This short intervention concludes that we are witnessing a process in motion, with numerous mobile targets, but which interest us all as citizens. A first direction must be represented by a good definition of the concepts. We need an additional effort from political scientists to adapt the old definitions to the elements of technical evolution. Secondly, the staff involved in education will have to realize the importance of this transition and their role in defining the character of future citizens. The politics of the future and education are important enough that we all need to get involved and not leave them exclusively to ICT experts or interest groups of any kind.

References

[1] Enrique Fernández-Macías, *Automation, digitalisation and platforms: Implications for work and employment*, Eurofound, Publications Office of the European Union, Luxembourg, 2018, p. 1, available at https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef18002en.pdf. Last accessed on November 20th, 2020. A preliminary version of this material is also partially available in Mihai Sebe, "The implications of the digital revolution on the labor market. Socio-political aspects. Consequences for Romania" in Radu Puchiu, Marius Stoian, Marcel Foca (coordinators), *Digital Romania. Concepts and operational tools*, Club România Publishing House, Bucharest, 2018, pp 601 - 602, available at http://www.mentoringproject.ro/wp-content/uploads/2019/12/CD3-ROMA%CC%82NIA-DIGITALA%CC%86.pdf (available in Romanian language). Last accessed on November 20th, 2020.

[2] The European Parliament, *REPORT on e-democracy in the European Union: potential and challenges*, (2016/2008 (INI)), available at https://www.europarl.europa.eu/doceo/document/A-8-2017-0041_EN.html. Last accessed on November 20th, 2020.

[3] The European Center for Non-Commercial Law, *CIVIL PARTICIPATION IN DECISION-MAKING PROCESSES A review of standards and practices in Council of Europe member states, 2016*, p. 38, available at https://ecnl.org/sites/default/files/files/CoE-ECNL-overview-paper-on-participation-standards_Ro_final.pdf. Last accessed on November 20th, 2020.

[4] Hille Hinsberg, *Awards - Osale: the Estonian eParticipation tool (Osale)*, 2009, available at https://joinup.ec.europa.eu/collection/eparticipation-and-evoting/document/awards-osale-estonian-eparticipation-tool-osale. Last accessed on November 20th, 2020.

[5] The European Parliament, *REPORT on e-democracy in the European Union: potential and challenges*, (2016/2008 (INI)), available at https://

www.europarl.europa.eu/doceo/document/A-8-2017-0041_EN.html. Last accessed on November 20th, 2020.

[6] The European Parliament, *REPORT on e-democracy in the European Union: potential and challenges*, (2016/2008 (INI)), available at https:// www.europarl.europa.eu/doceo/document/A-8-2017-0041_EN.html. Last accessed on November 20th, 2020.

[7] Anette Braun, Anna März, Fabian Mertens, Annerose Nisser, *Rethinking education in the digital age*, The European Parliament, 2020, p. 3, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641528/EPRS_STU(2020)641528_EN.pdf. Last accessed on November 20th, 2020.

[8] STOA Options Brief based on the Anette Braun, Anna März, Fabian Mertens, Annerose Nisser, *Rethinking education in the digital age*, The European Parliament, 2020, pp. 2-4, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641528/EPRS_STU(2020)641528(ANN1)_EN.pdf. Last accessed on November 20th, 2020.

Building a Resilient Ecosystem for Cybersecurity in Education

Costel CIUCHI, PhD
Associated Professor at "POLITEHNICA" University of Bucharest
Information Technology and Digitalization Directorate,
General Secretariat of the Government
costel.ciuchi@gov.ro

1. Introduction

Internet threats are one of the most important challenges facing all organizations regardless of their field of activity. To combat these threats, organizations have invested in defense technologies and implemented standards to ensure the security of information systems. Thus, the main vector of attack on information systems has become the human resource within an organization. Technological vulnerabilities coupled with the lack of user education and cybersecurity management knowledge are serious threats that can compromise the organization's data and/or influence managerial decisions.

The security policies implemented at the organization's level are technical and, in most cases, the users do not respect them. This is often because security policies use standards that are not customized and are written in a difficult way to read and understand.

The development of cooperation between academia, the private sector, and public administration to conduct courses and programs in the field of cybersecurity is the foundation of a successful model. The introduction of specialized courses and specific programs (technical, awareness, legislation) of continuous training is a model of the educational framework (formal, non-formal, etc.) that ensures the development of a secure and secure organizational environment.

For example, the implementation of frequent training/information sessions at the level of public administration staff can be a solid foundation for the development of

customized programs, decision-makers included. The high degree of cybersecurity culture in any organization ensures the development of a secure ecosystem by ensuring the essential attributes associated with cybersecurity decision-making.

2. The current state of shaping the educational process in the field of cybersecurity

To diversify the concept of education and training comes from the need to acquire new skills (digital and cybersecurity) which is a consequence of a constantly dynamic global competition and the growing demand for a better-skilled workforce adapted to accelerated technological changes.

The educational process underwent a series of transformations with the digital revolution. Adopting new ways of achieving educational goals requires updating classical models and systems. In the field of cybersecurity, components that require the development of skills both horizontally and vertically concerning other areas of activity are needed.

At the international level, in the field of cybersecurity, several initiatives have been launched regarding the educational component that approach the field from several perspectives, such as:

- NIST model (focused on processes and specialists);
- initiatives at the European level (smart specialization, education, and training without borders through the recognition and certification of learning outcomes acquired abroad, and social and personal development on lifelong learning, etc.).

2.1. NICE Cybersecurity Workforce Framework

The National Initiative for Cybersecurity Education (NICE) [1] Cybersecurity Workforce Framework (NICE Framework) developed by the National Institute of Standards and Technology (NIST) is a concentrated resource that establishes a unitary taxonomy and lexicon to describe the cybersecurity processes and the specialists, regardless of the particularity of the cybersecurity subdomain in which it operates.

Modeling essential activities and associated tasks requires the development of the necessary steps to be taken in ensuring cybersecurity.

The NICE framework consists of the following components:

- categories (7) - the main grouping of common cybersecurity functions;
- specialized fields (33) - distinct fields associated with activities;
- working roles (52) - the most detailed working groups in the field of cybersecurity which include the specific knowledge, expertise, abilities, and skills needed to perform tasks in a working role.

The 7 main categories include the basic principles as a starting point for the development of a complete educational ecosystem for all stages of management regarding the assurance of cybersecurity:

Tab. 1. *General competency categories according to the NICE Framework*

Categories	Description
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

In an ever-expanding and up-to-date area, the field of cybersecurity requires specialists with a strong portfolio of expertise to help organizations perform cybersecurity functions.

As organizations identify the skills needed to properly manage current and future cybersecurity risks, decision-makers need to consider the capabilities and demands of education and training.

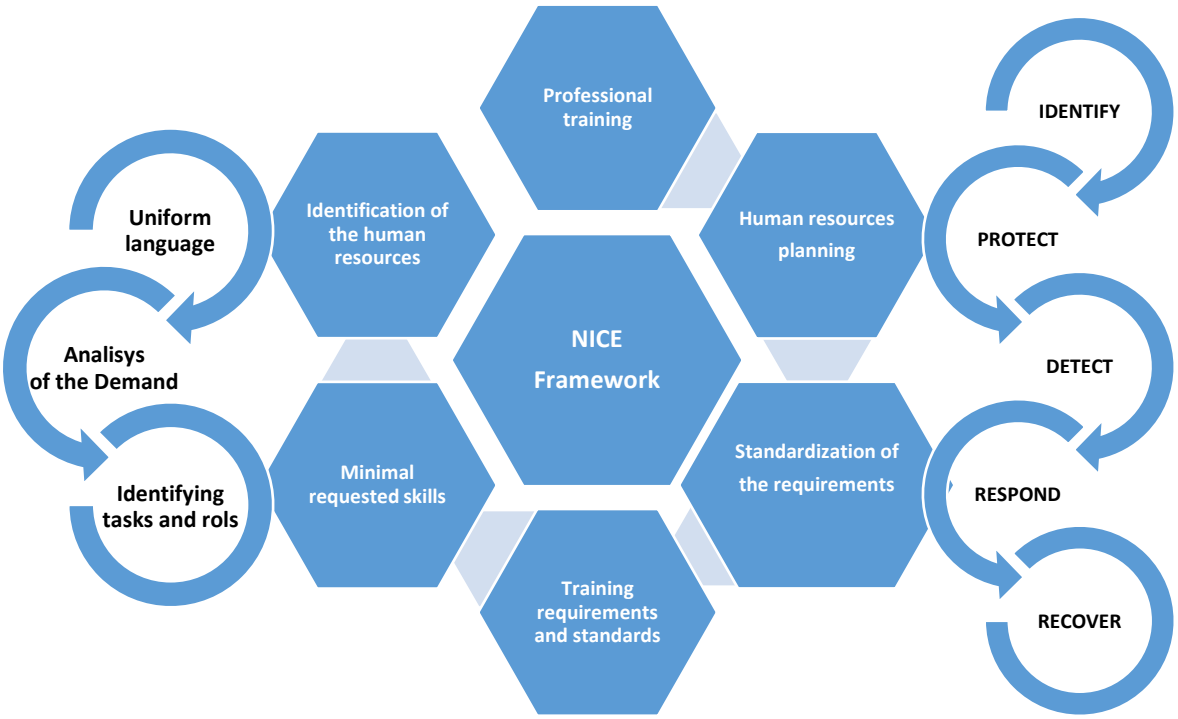


Fig. 1. *Training and development model of skills*

2.2. EU Framework for Digital Education and Cybersecurity

A number of initiatives have been launched at the European level to develop a uniform framework for the minimum cybersecurity expertise needed to ensure a common understanding of the roles, skills, abilities, and knowledge used by and for employees, employers, and training providers in all EU member countries to address the cybersecurity skills shortage.

The European Cybersecurity Skills Framework initiative provides the necessary framework for the development of a strengthened cybersecurity growth strategy that goes beyond existing education and training policies, by promoting and ensuring an active role for employers in the development of a workforce. in accordance with their needs.

One of the new challenges in acquiring knowledge and building skills at the EU level is the achievement of a common set of skills and qualifications in education and training in all 27 EU Member States [2].

The European Cybersecurity Skills Framework recommends developing cybersecurity skills by:

- the impact of the certification of diplomas in the field on the lack of skills in cybersecurity (the extent to which knowledge and skills are improved);
- promoting cybersecurity programs by updating the database at the European level (as the main source of information for citizens, especially for secondary and tertiary education students who want to further develop cybersecurity knowledge and skills with higher diplomas);
- the requisites in terms of years of professional experience, education, and certification that employers require, especially for juniors or intermediate level.

The European Commission has also initiated a debate for The Digital Education Action Plan (2021-2027) [3] which is structured around two strategic priorities:

- promoting the development of a high-performance digital education ecosystem;
- improving skills and competencies for digital transformation.

The actions taken to achieve priorities show a unified approach to cybersecurity education as a supporting component in ensuring secure infrastructures, platforms, and capabilities that respect confidentiality and ethical standards:

- transparency and recognition of skills and qualifications to facilitate certifications;
- horizontal and vertical cooperation to ensure the performance and excellence of vocational education and training systems.

The modernization of education and skills requires the development of flexible and open programs, able to stimulate creativity among children and strengthen the links between public/private education systems, business, and society.

The development of a knowledge society requires ensuring excellence in all stages of the educational process, constantly updating the skills base as needed, and creating a social, economic, and regulatory environment that can stimulate research, creativity, and innovation [4].

3. Development Mechanisms of Education in Cybersecurity

The implementation of a resilient organizational ecosystem requires the adoption of an educational model based on the multidimensionality attribute associated with resilience. In this sense, the development of such an educational model takes into consideration 3 dimensions - human resources, processes, and technology.

The cybersecurity education component based on education and lifelong learning can provide the organization's systems with a high probability of survival and a minimization of the risks of malfunctions and/or incidents.

An important aspect is the inclusion in national cybersecurity strategies of an important pillar such as professional education and training. The educational component of the strategies emphasizes the need for coordination between the various forms of cybersecurity education.

According to the methodology of the National Cyber Security Index developed by the Governance Academy of Estonia, the educational component takes into account all levels of education (primary, secondary, high school, university), but also professional training programs that ensure a high level of specialization of specialists in cybersecurity. The analysis of existing capacities in the field of education and training in the methodology of measuring the readiness of countries to prevent cyber threats and to manage cyber incidents as a general indicator with an important contribution (5 indicators) [5] suggests a unified approach to the cybersecurity education process.

The development of an educational model in the field of cybersecurity is a challenge due to the associated characteristics that make it difficult to teach at all levels of education, cybersecurity being a "multidisciplinary field, addressing political, economic, awareness and public education issues, along with new technical challenges." [6].

In order to develop cybersecurity skills in areas such as law, public administration, medical and finance, it is necessary to cooperate between the various fields that should consider cybersecurity not as a single monolithic discipline in higher education, but rather as a field that crosses and looks very different in many disciplines.

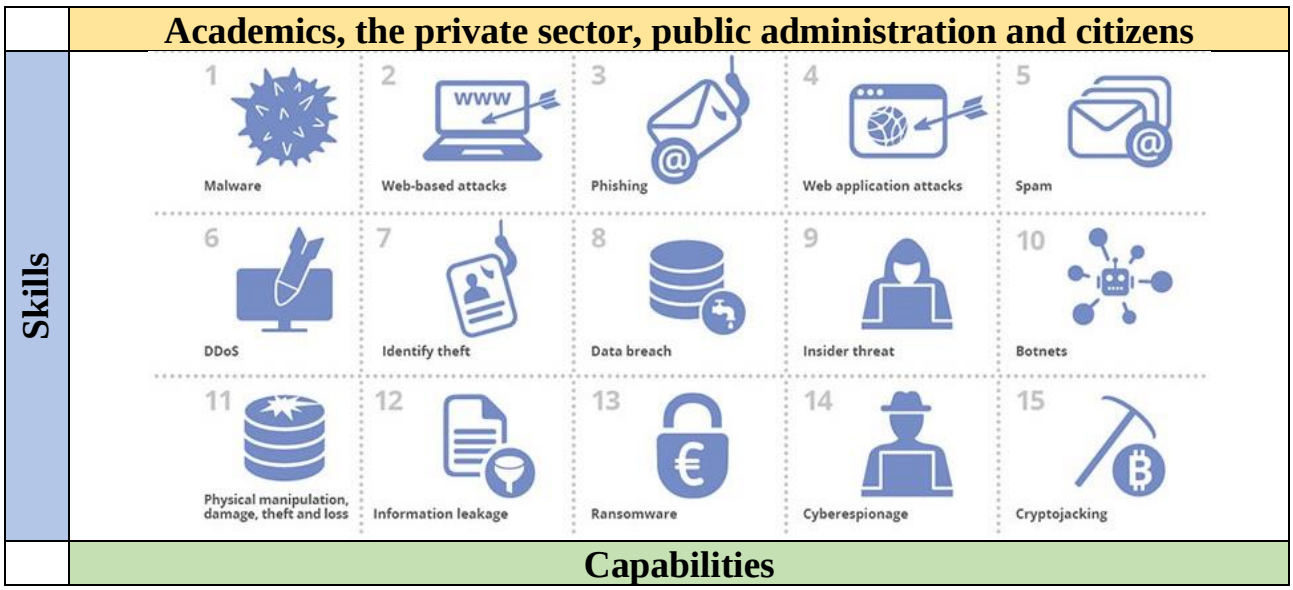


Fig. 2. *Cyber threats - modeling the necessary skills and abilities* [7]

A challenge for the university environment is represented by the international cooperation with both academic and private partners, in the development of an adequate and constantly updated curricular area.

The spectacular evolution of threats by diversifying attack vectors and customizing them for various areas of activity requires a specific approach. The importance of cybersecurity education is evidenced by the need for cooperation between universities, the private sector, public administration, and citizens. Relevant and quality skills and competencies are elements that need to be developed in accordance with the level of criticality associated with threats.

The need to update the educational mechanisms that can be adopted in order to develop complex models can be achieved considering the development of:

- **key (technical) competencies** through specialized courses, certifications, and alternative forms of learning (competitions, national/international competitions, internship programs, etc.).

If personalized training courses are not carried out, novice experts with general experience in the field, but without knowledge and skills specialized in cybersecurity, cannot further develop the intellectual, managerial, and technological skills necessary to carry out their daily activities. Also, if an adequate training program is not provided, professionals will probably not be

able to keep up with the constant pace of innovation and the evolution of cyber threats/vulnerabilities.

- **cross-cutting competencies**

Developing cross-cutting competencies is one of the major challenges in terms of the lack of cybersecurity skills. There is a need to redefine and/or re-evaluate learning plans and educational pathways. In fact, the major difficulty lies in identifying and developing appropriate cybersecurity capabilities and skills in specific areas of the field.

Tab. 2. *Cross-cutting competencies*

	CROSS-CUTTING COMPETENCIES
ADEQUACIES (QUALIFICATIONS)	EVALUATION, COMMUNICATION, ANALYSIS, INVESTIGATION
ESSENTIAL SKILLS	INTUITION, CREATIVITY, ADAPTABILITY, CONTINUOUS LEARNING

In order to adopt a model, it is also necessary to set short and long-term objectives that should be achieved in order to validate the educational model, as follows:

- short-term objectives:
  - close collaboration between universities, companies, and government and international cooperation;
  - increase the interest in cybersecurity programs and continuing education activities;
  - involvement and support at all levels of education from the private sector.
- long-term objectives:

- increase the number of qualified cyber security graduates entering the labor market and improving the basic knowledge of cyber security of graduates from other fields of activity (legal, economic, energy, industry, etc.);
- develop and promote a process of continuous professional training for decision-makers;
- conduct research projects that contribute to the national cybersecurity strategy and scientific priorities in order to increase the results.

4. Conclusions and perspectives

In the current context, with an increased number of activities transferred in the online environment, cyber threats have experienced an explosive diversification, some of which can be classified as global epidemics due to the high speed of spread in the virtual environment. The intensified use of electronic services has highlighted new surfaces and attack vectors, which has led to an intensification of attacks and an increasing degree of sophistication of the forms of deployment.

The development of a resilient educational ecosystem in the field of cybersecurity needs to be focused on the mechanisms/work processes associated with the technical support systems, especially on all components of a resilient model (human resource, processes, technology).

In terms of education, initial and continuing professional training, awareness, and cooperation in the field of cybersecurity, a new approach is needed by adding new directions on the objectives of information systems by:

- **anticipation** - development of strategies for detecting attacks and assessing possible losses;
- **resistance** - implementing systems capabilities to repel attacks by adopting various technologies for defense mechanisms at different levels;
- **recovery** - adoption of operational procedures/measures to maintain essential services and components during an attack, to limit the degree of deterioration, and to fully restore the functional capacity of the services;

- **adjustment** - to the new threats that appear in the virtual space not only from a technical point of view but also from the point of view of the administration of systems through public policies, public-private partnerships, cooperation.

Research and training in cybersecurity must become priorities in the development of educational policies by adapting existing learning plans and educational pathways to current needs.

Strengthening cybersecurity research, improving education, and developing a trained workforce is key to achieving the overall objectives of cybersecurity policy. Research and education policies will only be effective if they include the multilateral and multidisciplinary nature of cybersecurity as a fundamental and ubiquitous element in culture, approaches, processes, systems, and technical infrastructures [8].

The development of specialized technical courses adapted for all educational levels based on modeling of flows and processes, correlated with legislation adapted to the current technological context, doubled by coherent cybersecurity management policies at the national level are actions necessary to be included at universities.

Professional training in the field and the implementation of awareness/ understanding programs in the field at the level of decision-makers in public administration are necessary aspects to be developed at the university level.

The development and implementation of models whose main level of support is a cooperation between the basic components of society (academia, public administration, the private sector, and civil society) ensure the development of a sustainable and competitive educational ecosystem.

State authorities have a sole responsibility to facilitate and stimulate the growth of the cybersecurity workforce, as inadequate manpower and poor education of citizens expose a state to serious consequences for other components such as economic and national security [9].

Lifelong learning, creativity, and innovation, including entrepreneurship, are strategic elements that need to be developed at all components of society in order to ensure a high degree of cybersecurity.

The national defense strategies of the states in the current global context highlight the importance of the field of cybersecurity and the fact that it is a priority direction for action for most countries in the world. Technological developments and the complexity of cyber incidents require the development of a resilient ecosystem for education and cooperation mechanisms at the European level in the field of cybersecurity.

References

[1] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), NIST Special Publication 800-181, National Institute of Standards and Technology, July 28, 2020, https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

[2] European Cooperation in the Field of Education and Professional Training (ET 2020) https://eur-lex.europa.eu/summary/RO/legissum-:ef0016.

[3] Digital Education Action Plan (2021-2027), European Commission, COM(2020) 624, https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en.

[4] Publications Office of the European Union (2010). Europe 2030 project. Challenges and opportunities. Report to the European Council of the Reflection Group on the future of the EU 2030. Luxembourg, https://www.consilium.europa.eu/en/documents-publications/publications/project-europe-2030-challenges-opportunities/.

[5] National Cyber security Index, e-Governance Academy Foundation (eGA), Estonia, https://ncsi.ega.ee/.

[6] Interdisciplinary Pathways towards a More Secure Internet, National Science Foundation, Report on the Cybersecurity Ideas Lab, Arlington, Virginia, February 10-12, 2014.

[7] ENISA Tweet 12 November 2020 - Top 15 Cyber Threat.

[8] Current challenges in the field of cybersecurity – the impact and Romania's contribution to the field, Ioan-Cosmin MIHAI (coord.), Costel CIUCHI, Gabriel-Marius PETRICĂ; The European Institute of Romania. - Bucharest, 2018.

[9] Cybersecurity Workforce Development: A Primer, Laura Bate, 2018 (newamerica.org, Cybersecurity Initiative Center on Education & Labor), https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/.

Five Decades of Higher Technical Education in the Field of Dependability in Romania

Professor Ioan C. BACIVAROV, PhD
Director - EUROQUALROM - ETTI, "Politehnica" University of Bucharest, Romania
President - Romanian Association for Information Security Assurance (RAISA)
ioan.bacivarov@upb.ro

Introduction

Dependability, viewed in the interaction of its components - *reliability, maintainability, availability, survivability,* and ***security*** - is a relatively new field compared to traditional technical fields: the first studies in the field of reliability date back to the 50s of last century, when were developed the first American military regulations, due to the specialists from the famous regulatory group in the field of reliability AGREE[1].

Systematic concerns in the field of systems *security* appear at the end of the sixth decade of the last century, and those in the field of *information security* - starting with the eighth decade of the same century.

Globally, the first educational programs in the field of reliability appeared only in the early '60s of the last century. The Master's program in *reliability engineering*, started in 1962 at the US Air Force Institute of Technology in Dayton, Ohio, U.S.A. - intended for military personnel and the US administration - is considered the world's first educational program in the field.

After 1965, several reliability education programs were developed at various American universities, including the Air Force Institute of Technology Dayton, Ohio, U.S. Naval Post-Graduate School Monterey, California, University of Phoenix, Arizona, Princetown University, New Jersey and Columbus University, New York. "*At least one course in statistics and probabilities and one in the field of reliability must*

[1] AGREE - Advisory Group on Reliability of Electronic Equipment

be included in the curriculum of all technical universities," said Professor *D. Kececioglu* in an article published in the prestigious journal *IEEE Transactions on Reliability* in 1984 [1].

In this context, it is noted that in Romania, especially within the Polytechnic Institute (since 1992, "Politehnica" University) of Bucharest (P.I.B. / P.U.B.) - the largest technical university in Romania - there have been valuable educational initiatives in the field quality and dependability, which places it at the forefront at European and even global level.

In this paper will be highlighted the main research and educational programs in the field of dependability, developed under the auspices of the Department of Electronic Technology and Reliability (ETR) of the P.U.B., which celebrates in 2021 five decades since its establishment.

After five decades of higher technical education and scientific research in the field of dependability in electronics and telecommunications, we can speak today of a real "*Romanian school*" in the field, whose achievements are known and appreciated both nationally and internationally: research and courses that initially focused primarily on reliability and maintainability have also addressed security over the past 15 years, from risk analysis to the study of information security.

Higher Technical Education in the Field of Quality and Dependability in Electronics and Telecommunications in Romania - Some Historical Milestones

In line with the global trend, research in the field of quality and reliability in the electrical field (and especially in the field of electronics) has generally been 10… 15 years ahead of those in other fields.

In Romania, the pioneers of the field of *reliability* are professors **Vasile M. Cătuneanu** (for the electronic and telecommunications field) and **Vasile Nitu** (for the energy field). In the late 1970s, courses in quality and reliability began to be introduced at other faculties in the P.I.B. (especially in the electrical ones), and after the '90s - also

in other universities in Romania, especially under the aegis of some European educational projects[2].

Next, in this analysis we will refer only to the field of electronics and telecommunications. Professor Cătuneanu published - in the mid-1960s - the first articles in the field of operational reliability [2], based mainly on Russian technical literature; he also introduced at the end of the ’60s the first reliability chapters in the "*Materials*" course taught to the students of the profile faculty of the Polytechnic Institute of Bucharest.

Fig. 1. *Professor V.M. Cătuneanu, together with some of his collaborators from the new Department of Electronic Technology and Reliability (1972)*

In 1971, Professor ***V. M. Cătuneanu*** - as of Dean of the Faculty of Electronics and Telecommunications (El&Tc) from P.I.B. - has the excellent idea, and at the same time the necessary levers for the establishment of the Department of ***Electronic Technology and Reliability (ETR)***, starting with October 1st, 1971. For this purpose, he selected the best graduates of the 1971 promotion of the Faculty of Electronics - young men and women dedicated to study and research, speakers of several languages of international circulation, as mentioned by *D. Stoichițoiu* and *V. Vodă* in their excellent "*History of quality*" [3].

[2] These courses and educational projects are not analyzed in this paper.

Among those who were called in 1971 to "break up" education and research in the field of quality and reliability in the new department we mention ***Ioan C. Bacivarov*** (Valedictorian of the "*Telecommunications*" section of the faculty), as well as ***Angelica Dogaru*** (married ***Bacivarov***) and ***Adrian Mihalache***, two of the best graduates of the "*Applied Electronics*" section.[3]

They began a pioneering work, based primarily on the study of fundamental works in the Anglo-Saxon technical literature, which existed at that time in the "richest" technical libraries in the country: *INID* and *IFA*. In addition to those mentioned above, ***Marieta Georgescu*** (married Dragomirescu) - a graduate of the El&Tc Faculty since 1966 - and, in the late 1970s, ***Florin Popențiu*** were also included in the *Quality & Reliability Team* of the Department.

Professor ***Cătuneanu*** and his collaborators have the merit of understanding that the training of future electronic engineers can be complete only if the analytical program of the faculty takes into account the entire life cycle of systems and basic concepts of quality and dependability (reliability, maintainability, security) engineering, as well as the notions regarding design for quality, reliability, security, testability, etc., and technological design, must be learned from the faculty benches. They militated for this idea their entire activity, despite many constraints and contrary opinions, coming even from some colleagues or even decision-makers from the faculty.

The first chapters in the field of quality and reliability had already been introduced in the analytical curriculum of the Faculty of Electronics and Telecommunications in the early 1970s (as part of the *Materials* course). The young teachers of the ETR Department prepare new courses, corresponding to each specialization: *Reliability of telecommunications systems, Reliability of electronic equipment*, *Reliability of electronic components*, etc.), which are successively introduced in the specialized sections, starting with 1973. At the same time, the first technological courses are introduced in the faculty, because in the vision of the new

[3] When established, in 1971, the Department of Electronic Technology and Reliability from IPB had three main teams: Quality and Reliability, Materials, and Electronics Technology; in this work will be considered only the activity and achievements of the first team.

ETR Department, the design for reliability and maintainability had to be correlated with the technological one to develop high-performance systems.

It should be noted that, unlike the "traditional" technical fields (such as mathematics, physics, electrical engineering, etc.), for which there was already a serious background and many fundamental works published, the field of *quality and reliability* was new, and it was effectively "developed" by the members of the profile team from the ETR Department: from the elaboration of the didactic programs to the writing of some specialized books and textbooks, as well as by arranging and equipping specialized laboratories.

During the difficult period of 1975 - 1990, the sprouts of a *Romanian school of reliability* are already emerging, in which the members of the reliability team of the ETR Department had an important role: fundamental works in the field are published [4]…[9] and scientific research contracts are concluded to solve real industry reliability and profile research issues, such as increasing the reliability of electronic TVs and computers, analyzing and increasing the reliability and security of electronic equipment in shipping and the chemical industry, making equipment for testing electronic components and computer systems, etc.[4]

Fig. 2. *Professors Adrian Mihalache, Angelica Bacivarov, and Ioan Bacivarov at the Pan-European Conference "e-learning Society" (2002)*

[4] A selective list of the main scientific - national and international - research contracts in the field of quality and reliability within the ETR Department, as well as the works elaborated by them is given on the EUROQUALROM Laboratory website, www.euroqual.pub.ro.

Among ***the new didactic*** and ***scientific research fields*** developed and imposed in Romania by these professors, we mention: *the reliability of telecommunication systems, the analysis of the reliability and security of highly functional importance systems, the dependability management, human reliability (**Ioan Bacivarov**), reliability and security of computer systems* - both *hardware and software, fault-tolerant systems / computers, automatic testing and technical diagnosis (**Angelica Bacivarov**), uncertainty theory (**Adrian Mihalache**), reliability optimizations (**Florin Popențiu**).*

The new **ETR** Department consolidates its presence and the leading role of the field in the Romanian scientific landscape of that period also by organizing several scientific events, the most important of which is, of course, the *National Symposium "Electronic Technology and Reliability"*. The first edition of the symposium was organized at P.I. Bucharest in November 1977 (president: *V.M. Cătuneanu*, scientific coordination: *Ioan C. Bacivarov*), and several scientific and administrative personalities of the moment spoke in the opening. A wide selection of the over 120 papers presented at the symposium was included in a large volume published by the Didactic and Pedagogical Publishing House [10]. The symposium "*Electronic Technology and Reliability*" had 10 more editions, in different university centers, until 1990, when it ceased to exist and was replaced by other conferences in the field, among which of course the most important will be the *International Conference on Quality and Dependability, CCF*, now at the 16th edition.

During the '80s, Professor Cătuneanu and other members of the specialized team from the ETR Department are involved in organizing and coordinating quality-reliability sections of various national conferences and symposia (Romanian Academy sessions, national conferences on electronics and telecommunications, SACEP symposia, etc.).

Despite the restrictions of that period, members of the reliability team in the ETR Department are becoming increasingly visible internationally, by publishing articles in prestigious international scientific journals such as *IEEE Transactions on Reliability, Reliability Engineering & System Safety, Microelectronics and Reliability*, etc., or by

submitting papers to well-known international reliability conferences held in England, France, or Hungary.

Fig. 3. *Romanian and foreign participants in the International Conference on Quality and Dependability - CCF 2014*

As editors of the few Romanian scientific journals that appeared until 1989, Prof. ***V. Cătuneanu*** *(Automatica si Electronica / Automation and Electronics, Telecomunicatii / Telecommunications)* and Dr. ***Ioan Bacivarov*** *(Calitate, Fiabilitate, Metrologie / Quality, Reliability, Metrology)* contributed to the highlighting of the most important results of local scientific research in the field.

After 1990, Professor ***Ioan Bacivarov*** became involved in the establishment and editorial coordination of specialized international journals (including *Asigurarea Calitatii - Quality Assurance*, since 1995, *Calitatea - Acces la succes / Quality - Access to Success*, since 2000, and the *International Journal of Information Security and Cybercrime - IJISC*, since 2012). As Editor / member of the Editorial Board of some prestigious international journals in the field, including *Quality Engineering* (USA) and *Reliability Engineering & System Safety* (Elsevier, UK), he has contributed to the better international visibility of Romanian research in the field of quality and dependability.

The Postgraduate Academic Program "Quality, Reliability, and Maintainability of Complex Systems"

An important moment for the development of profile education was the launch in 1972, under the coordination of Professor ***Cătuneanu***, and with the substantial contribution of his young collaborators, of *the postgraduate program* in the field, the first promotion obtaining graduation diplomas in 1973.

This postgraduate program ran uninterruptedly for 36 years, from 1972 to 2008, with about 1600 students graduated, specialists with higher education, mainly in the technical field (over 95% of graduates), but also in the economic field. It is, without a doubt, one of the most successful postgraduate technical education programs with the longest existence in Romania. Between 1976 and 1980, the course coordinator was Prof. ***Vasile Corlățeanu****, PhD* and since 1981 the courses have been coordinated by ***Ioan C. Bacivarov****, PhD.*

Initially, this postgraduate program focused mainly on the field of *reliability* (being, in fact, originally referred to as *"Postgraduate courses in reliability"*) and, partially, on *maintainability*, but after 1982 the courses' scope was extended, successively, to all aspects of *dependability* (reliability, maintainability, security). After 1990 it began to address the *entire issue of quality*, seen in the synergy of its sides. The issue of security was addressed in the course *"Reliability and security of highly functional importance systems"*, held by Prof. ***Ioan Bacivarov*** between 1985 and 2008.

Many of the prestigious Romanian specialists in the field of quality and dependability in Romania have contributed, over the years, as professors in the postgraduate academic program "*Quality, reliability, and maintainability of complex systems"*. We are very pleased to mention, working in the early stages of the courses, the names of the university professors ***Vasile Cătuneanu, Vasile Corlățeanu, Vasile Nitu, Cezar Ionescu, Tudor Baron***, as well as those of the associate professors ***Dan Stoichițoiu, Eugeniu Diatcu, Ulrich Wiener, Dumitru Niculescu*** and others.

We can mention among the specialists who, for a longer or shorter period, taught courses in the postgraduate program in the field of quality and dependability, organized under the auspices of the Department of Electronic Technology and Reliability: Prof.

Angelica Bacivarov, PhD (testing and technical diagnosis, fault tolerance), ***Marius Bâzu,*** PhD (reliability of components), Prof. ***Marieta Dragomirescu,*** PhD (reliability of electronic equipment), Prof. ***Adrian Mihalache,*** PhD (theory of renewal, mathematical foundations of quality and reliability), Prof. ***Gheorghe Oprișan***, PhD, Assoc. Prof. ***Rodica Tomescu,*** PhD (mathematical foundations of quality and reliability), ***Dan Stoichițoiu,*** PhD (assurance and certification of quality), Prof. ***Sorin Ionescu***, PhD, ***Traian Teodoru,*** PhD (quality management), Prof. ***Ioan Bacivarov,*** PhD (fundamentals of dependability, modern approaches in reliability and maintainability, reliability and security of highly functional importance systems, assurance and certification of quality and dependability).

From the above name list, it is noted that some of the most important Romanian specialists in the field in the last 5 decades have contributed to the training of students, from industry and research (before 1990), as well as from companies and ministries (after 1990), and, what it is perhaps more important, to make them aware of the importance and theoretical and practical aspects of implementing quality and dependability.

The European educational project TEMPUS S_JEP-11300 "EUROQUALROM" and later the European educational program ERASMUS / SOCRATES exerted a particularly positive influence on this postgraduate academic program, as well as on the master's programs that followed it. Thus, the curricula / syllabuses have been reconfigured to be in line with those of prestigious universities in the European Union (and especially with those of the *European Program in Quality of Complex Integrated Systems - EPIQCS*).

In fact, considering the level of these postgraduate courses and - later - of the master's program in the field, the "Politehnica" University of Bucharest was accepted as an associate member of the *European EPIQCS Program,* completed with the *European Masters for the Quality of Complex Integrated Systems* [11].

TEMPUS Project - EUROQUALROM - Anchoring Specialized Postgraduate Education at European Coordinates

The largest and most important project developed within the Department of Electronic Technology and Reliability in the '90s was, of course, the European project ***TEMPUS S_JEP-11300 "EUROQUALROM"*** (international coordinator: Prof. ***Ioan Bacivarov***, PhD, contractor: Prof. ***Marin Drăgulinescu,*** PhD), a program whose results were also appreciated by the European Commission's education bodies, which considered it a "model project in the field".

The educational project ***"EUROQUALROM"*** was developed within the European program ***TEMPUS - PHARE*** between 1996 and 1999 and it involved partners with brand achievements in the field of quality and dependability, mainly from the university environment. The interface with the sphere of industry and services was ensured through two of the main Romanian non-governmental organizations in the field of quality assurance and management at that time, namely the *Romanian Society for Quality Assurance (SRAC)* and the *Romanian Foundation for Quality Promotion (FRPC)*.

If we refer to local universities, we must mention the participation of the main Romanian universities in the **technical** field (the *"Politehnica" University of Bucharest - Faculty of Electronics and Telecommunications* and *Faculty of Power Engineering* - both faculties with notable achievements in engineering, quality assurance and reliability) and the **economic** one (*Bucharest Academy of Economic Studies*, also with important contributions in the field of quality control and management), as well as two other technical universities active in this field, respectively the universities of *Oradea* and *Pitești.*

Among the prestigious universities in the European Union participating in the **TEMPUS S_JEP-11300 project "EUROQUALROM"** is worth mentioning the *National Polytechnic Institute of Grenoble* (France), coordinator of the European Educational Program on the quality of complex integrated systems - EPIQCS, *University of Piraeus* (Greece), coordinator of the Program European Educational Center for Total Quality Management - EMPTQM, the *Institute for Strategic Quality*

Management at the *Erasmus University in Rotterdam* (Netherlands), the *Polytechnic Institute of Turin* (Italy), and the universities of *Angers* and *Paris - ENSAM* (France), *Barcelona* (Spain), *Lisbon* (Portugal), *Paisley* (United Kingdom).

The main objective of the **TEMPUS** project **"EUROQUALROM"** was the *reconfiguring of curricula* in technical (especially electrical - electronic and energy) and economic faculties, to include in educational programs the *issue of quality* (seen in the interaction of its components, static and dynamic) and in particular *quality assurance, control, certification*, and *management*, following the requirements of economic organizations and Romania's desire to participate in Euro-Atlantic structures, which also involved an alignment with European standards in this vital area [12].

The aim was also to *reorganize courses* in the field of quality and dependability, in line with those taught in elite universities in European Union (EU) countries, as well as to *modernize the teaching methods* used in this field (mainly through the intensive use of *computer-assisted training* and *multimedia systems*). The issue of *ensuring and managing the educational process in higher education* was also considered, including the development of appropriate models and metrics for its *monitoring* and *evaluation*. This project was one of those that laid the foundations of the local system of ensuring and certifying the quality of technical and economic higher education.

Fig. 4. *The coordinator of the European educational project TEMPUS, Professor Ioan Bacivarov, opening one of the workshops TEMPUS - EUROQUALROM dedicated to higher education in the field of quality and reliability with professors Ioan Constantin, Marin Drăgulinescu, Vasile Cătuneanu, Bernard Dumon, and Tudor Baron (1998)*

The first stage of the project aimed at the elaboration of a ***strategy*** *to approach quality* in higher education - technical and economic - in Romania, in cooperation with the EU partners, following the system used by the profile universities in the European Union.

To achieve the objectives of the TEMPUS project "EUROQUALROM", several *working groups* were formed with goals related to the development of optimal strategies for the introduction of quality issues in higher education. Among the most active working groups, we mention those having as object of study the implementation of quality in technical and economic higher education, respectively the quality assurance, the quality engineering, the quality management, the industry-education interface, the specific problems of small and medium universities, specific problems of quality assurance in higher education, etc. The conclusions of the work meetings were presented in several debates / round tables and meetings organized under the auspices of the TEMPUS project S_JEP-11300-96 "EUROQUALROM", including the workshops *"Strategy for Addressing Quality in Technical and Economic Higher Education in Romania"* (*Bucharest*, November 30, 1997), *"Strategies for Romanian and European Union Universities on Higher Education in the Field of Quality"* (ENSAM Paris, April 3 - 4, 1998) and *"Romanian and European University and Postgraduate Programs in Quality and Reliability"* (Oradea, May 17 - 18, 1999).

It should be noted that the attention of the Steering Committee of the TEMPUS Project "EUROQUALROM" has always been on t*he best possible dissemination of the results obtained*, both nationally and internationally, a fact achieved through the 6 books and over 60 articles and scientific communications published as a result of this project.

From the educational point of view, the restructuring of undergraduate and postgraduate courses at partner universities has been carried out following current European requirements. As a result of this project in particular in the Faculty of Electronics and Telecommunications of the P.U.B., the postgraduate academic program in the field was modernized, and starting with 1996 the first in-depth study program (Master's degree) *"Quality and reliability engineering"* began to operate.

The curricula of the postgraduate and master's educational programs coordinated by the ETR Department have been continuously improved, to be following the existing norms and regulations at the national and international level in the fields of quality and dependability. Particular emphasis was put on the issue of quality assurance, certification and management, reliability and security, several courses with this topic being introduced. The norms from the ISO 9000, ISO 14000, ISO 27000, CEI 300 series, the integrated quality, environment and safety management systems, the modern tools of total quality management, the Six Sigma method, etc. have started to be studied in this context.

It should be noted that since the late 1990s - including through European TEMPUS programs of this type - quality and reliability courses (university and postgraduate) were introduced at most faculties in the P.U.B. and most important technical universities in Romania; this has of course helped to complete the training of students with the requirements of real technical systems, as well as those of manufacturing companies.

Master's Programs in the Field of Quality and Dependability

Starting with 1996, based on the experience gained through the postgraduate academic program *"Quality, reliability, and maintainability of complex systems"*, the individual TEMPUS programs, as well as the TEMPUS program - EUROQUALROM, in the ETTI Faculty, P.U.B. was implemented the master's program ***"Quality and Reliability Engineering" - ICF***, the first master's degree in the field in Romania (lasting 1 year). This master's program, which has been operating successfully for a decade, was coordinated by Prof. ***Angelica Bacivarov.***

Starting with 2006, taking into account the new requirements of higher education related to the implementation of the "Bologna cycle", the master's program ***"Quality and Dependability in Electronics and Telecommunications" - ICSFET***, started to operate in the Faculty of ETTI - P.U.B., coordinated successively by professors ***Angelica Bacivarov*** and ***Ioan Bacivarov***; it was based on the experience and improvements made - for a decade - to the ICF master's degree. Given the high

competition since admission, as well as the favorable evaluations on the satisfaction of master's students and employers, the ICSFET program can be considered as one of the successful master's programs developed within the ETTI Faculty of P.U.B.

The master's students appreciated the fact that this program provided them with the specialized knowledge in fields little or not at all approached in the undergraduate studies, but necessary for the exhaustive training of the future engineers. It is important to mention that most graduates of this master's program were employed - mostly in the *Quality - Reliability - Safety and/or Testing - Diagnosis* - departments of Romanian or multinational enterprises and companies, their training being favorably appreciated by employers.

Among the teachers from the Department of Electronic Technology and Reliability within ETTI - P.U.B. who contributed to the success of these master's programs we mention professors ***Ioan C. Bacivarov, Angelica Bacivarov, Adrian Mihalache, Norocel Codreanu, Alexandru Vasile, Orest Oltu, Iulian Năstac, Lucian Milea*** and others.

Fig. 5. *Class of 2017 of the ICSFET Master's program, ETTI - PUB*

It should be mentioned that some of the specialized courses on quality assurance and certification and reliability, quality management, the security of information systems, standardization and legislation in the field, quality control of technological

processes, etc. were taught by well-known specialists in the field from the *Romanian Society for Quality Assurance - SRAC (**Dan Stoichițoiu**, PhD, **Cristinel Roncea**, PhD and others), the Institute for Microtechnologies - IMT (**Marius Bâzu**, PhD), Police Academy „Al. I. Cuza" Bucharest (Assoc. Prof. **Ioan-Cosmin Mihai**, PhD), the Romanian Association for Information Security Assurance - RAISA (**Gabriel Petrică**, PhD, **Sabina Axinte**, PhD) or other institutions (**Luminița Copaci**, PhD, **Costel Ciuchi**, PhD)*. This allowed the linking of the courses taught with the real problems of the European economy and society, in general, and of the Romanian ones, in particular, and contributed to the rapid integration of the graduates in the profile companies.

Following the example of the European universities that the *EUROQUALROM Laboratory (ETR - ETTI)* has been collaborating with for over three decades, we can say that successful master's programs can only be achieved through close cooperation with renowned organizations and companies with activities related to the field (in some universities in the EU, over 50% of the courses are taught by associate professors) and that is why we want to develop this cooperation in the future.

Fig. 6. *Members of the commission for the dissertation exam at the ICSFET Master's program within ETTI - PUB (June 2016): Prof. I. Năstac, Prof. Angelica Bacivarov, Prof. I.C. Bacivarov (chairman of the commission), Prof. A. Manea, Prof. A. Mihalache*

Thanks to the European educational mobility programs *ERASMUS / SOCRATES*, about 50 ICSFET master's students were able to carry out educational internships of 3 months each at universities in the European Union (especially at *ISTIA - the University of Angers* and *TIMA - INP Grenoble*, France, with which the Laboratory *EUROQUALROM - ETTI - P.U.B.* has excellent relations of educational and scientific collaboration), where they elaborated, in co-tutelage, the dissertation

works. At the same time, 18 French students from the University of Angers completed their ERASMUS internships at the EUROQUALROM Laboratory in the last decade.

Over the last decade, the focus of security concerns has shifted to security, and in particular to cybersecurity, which has been reflected in the restructuring of the ICSFET program. At the same time, especially at the Faculties of Electronics and Automation of UPB, other master's programs have been developed that include, to a greater or lesser extent, this issue: a particularly positive fact, given that the demand for cybersecurity specialists is constantly growing.

PhD in Reliability

The first professors who, after 1971, received the right to conduct doctorates in reliability in I.P.B., in the field of electronics and respectively, automation, were ***Vasile M. Cătuneanu*** (*Electronics*) and, later, ***Dumitru F. Lăzăroiu*** (*Automation*). Under their leadership, young professors from the university environment completed their doctorates: *Ioan Bacivarov* (1978), *Adrian Mihalache* (1979), *Angelica Bacivarov* (1980), *Ioan Hohan*, and others, but also young researchers in the field, including *Dan Stoichițoiu*, *Eugenie Stăicuț*, and *Ioan Tutoveanu*.

After the political changes of December 1989, there was a revival in higher education: after a decade of stagnation, advances in higher education were permitted and high-performing teachers received the right to conduct doctorates in reliability since 1991: *Ioan Bacivarov* in telecommunications (under the patronage of ICTc), *Angelica Bacivarov* and *Adrian Mihalache* in electronics (under the patronage of ICPE, respectively ICE). Under their leadership, important researchers in the field are finalizing their doctoral theses, among which *Marius Bâzu, Traian Teodoru, Marcu Buşe*, and others.

After 2000, in the context of the restructuring of technical higher education following the "Bologna cycle", there is also a restructuring of doctorates and, unfortunately, *reliability* disappears as a doctoral specialty. However, Professor ***Ioan Bacivarov*** has been accredited to conduct doctorates in the field of "*Electronic Engineering and Telecommunications*" since 2000. Under his leadership are completed

several valuable doctoral theses in the field of quality, reliability, and security, such as those developed by *Alin Mihalache, Florina Băbuș, Răzvan Lupan* (doctoral theses coordinated in co-tutoring with professors from the Quality - Reliability Department of the University of Angers, France)[5] and more Romanian theses in the field.

Fig. 7. *Professors B. Dumon and A. Kobi (ISTIA - University of Angers, France) and I.C. Bacivarov ("Politehnica" University of Bucharest) with two of the PhD students they coordinated in co-tutoring, R. Lupan and A. Mihalache (Angers, 2004)*

Among the valuable doctoral theses in the field of reliability and security of information systems coordinated by Prof. ***Ioan Bacivarov*** and completed in the last decade are those developed by *Ioan-Cosmin Mihai, Luminița Copaci, Costel Ciuchi, Gabriel Petrică, Sabina Axinte, Ionuț-Daniel Barbu* and others[6]; they then contributed to the training in the field of IT security, both in the projects / workshops organized by RAISA and in the ICSFET master's program. Noting the value of doctoral theses, as

[5] **Alin-Gabriel Mihalache**, *Modélisation et évaluation de la fiabilité des systèmes mécatroniques: application sur système embarqué*, Thèse de Doctorat, Directeurs de thèse: Prof. **Fabrice Guerin** et Prof. **Ioan Bacivarov,** Université d'Angers, 2007.
Florina Băbuș, *Contrôle de processus industriels complexes et instables par le biais des techniques statistiques et automatiques***,** Thèse de Doctorat, Directeurs de thèse: Prof. **A. Kobi** et Prof. **Ioan Bacivarov**, Université d'Angers, 2008.
Răzvan Lupan, *Évaluation de la performance financière et organisationnelle des politiques qualité,* Thèse de Doctorat, Directeurs de thèse: Prof. **Alain Capiez** et Prof. **Ioan Bacivarov**, Université d'Angers, 2009.

[6] **Ioan-Cosmin Mihai**, *Contributions to the study of the survivability of information systems*, Doctoral thesis, P.U.B., 2011.
Luminița Copaci, *Contributions to ensuring and increasing the quality and safety of information systems*, Doctoral thesis, P.U.B., 2011.
Virgil-Liviu Ilian, *Reliability and dependability issues for autonomous robots*, Doctoral thesis, P.U.B., 2012.
Costel Ciuchi, *Contributions to the development of an IT system for decision-making processes. Computer systems security modeling*, Doctoral thesis, P.U.B., 2012.
Gabriel Petrică, *Contributions to security assurance of information systems in online environment*, Doctoral thesis, P.U.B., 2019.
Sabina Axinte, *Research on verification and validation techniques for information systems*, Doctoral thesis, P.U.B., 2020.
Cătălina Gherghina, *Contributions to the improvement of the quality and security of IP based services in intelligent telecommunications networks*, Doctoral thesis, P.U.B., 2020.
Ionuț-Daniel Barbu, *Cyber security: the vulnerabilities of future information systems*, Doctoral thesis, P.U.B., 2020.

well as other works in the field of cybersecurity developed by these Ph.D. students (whom he had the opportunity to meet at the *CCF 2016* international conference), Professor ***A. Birolini***, who is considered a "guru" of European reliability, said that, in his opinion, "the future of the field is assured in Romania".

Fig. 8. *Ph.D. students in the field of cybersecurity, coordinated by Prof. I. Bacivarov, who presented papers at the CCF 2016 international conference, together with professors A. Birolini (ETH Zurich) and Angelica Bacivarov (P.U.B.)*

Final Considerations

This paper was intended to be a review of the main didactic and scientific programs in the field of quality and dependability developed under the auspices of the Department of *Electronic Technology and Reliability (ETR)* of the P.U.B. in its five decades of existence. It is also intended to be a modest tribute to the multitude of Romanian specialists in the field who contributed to the implementation of these programs, some of which, including the founder of the ETR Department, Professor ***V.M. Cătuneanu***, have already passed into eternity…

At this milestone, we can say that beyond the technical, economic, or managerial knowledge they transmitted to students, the postgraduate courses and master's programs in quality and dependability organized under the auspices of the specialized team in the ETR Department have the merit *to raise awareness* among a large number of graduate and postgraduate students in the technical, economic or of services fields about the importance of modern tools and approaches, as well as the legislation in this topical interdisciplinary field.

After five decades of higher technical education and scientific research in the field of quality and reliability in electronics and telecommunications, we can speak today of a true "*Romanian school*" in the field, whose achievements are known and appreciated both nationally and internationally. Important international specialists in the field, including professors *A. Birolini, A. Barreau, Ton van der Wiele, E. Zio, Michele Cano, A. Goncalves, A. Kobi, L. Balme and others*[7] confirmed these achievements at important international conferences in the field (including *ESREL, QUALITA, CCF*).

An argument in this direction is represented by the 50 or more books and 700 articles and scientific communications published in the country and abroad by the members of the *Quality - Reliability Team* of the ***ETR Department***, as well as more than 60 national and international scientific research contracts coordinated by them. Also, the numerous technical journals they have created / coordinated and the specialized national / international conferences they have initiated and led also support this statement.

This paper also wanted to emphasize that there is already, at least at the level of the Faculty of ETTI - P.U.B., and not only, a solid basis for the implementation of new educational programs at the master's level in the field of dependability and especially in the field of cybersecurity, for which there is an acute lack of specialists, especially in the current context in which most activities have moved in the online environment. However, these programs can only be developed through the close cooperation of specialists in the field from universities, companies, and other specialized institutions.

References

[1] D. Kececioglu, Reliability Education. An Historical Perspective, *IEEE Transactions on Reliability*, vol. R-33, pp. 20-24, 1984.

[2] V. Cătuneanu, Calculul siguranței în funcționare a aparaturii electronice, *Telecomunicații*, no. 2, 1966, pp. 10-14.

[7] Many of these prestigious European professors, with whom we collaborated in the TEMPUS project "EUROQUALROM", gave guest lectures in the field of quality and dependability in various workshops, symposia, and educational programs (master's and doctorates) organized under the patronage of ETR - ETTI.

[3] D. Stoichițoiu, V. Vodă, *History of Quality*, Mediarex, 2002.

[4] V. Cătuneanu, O. Iancu, I. Bacivarov ș.a., *Reliability theory and statistical control*, IPB Publishing House, 1973.

[5] V. Cătuneanu, I. Bacivarov, *Reliability of telecommunications systems*, Military Publishing House, 1985.

[6] V. Cătuneanu, Angelica Bacivarov, *High reliability electronic structures. Fault tolerance*, Military Publishing House, 1989.

[7] V. Cătuneanu, O. Iancu, M. Drăgulinescu, I. Bacivarov, Angelica Bacivarov a.o., *Materials for Electronics*, Did. and Ped. Publ. House, 1982.

[8] V. Cătuneanu, A. Mihalache, *Theoretical bases of reliability*, Academy Publishing House, 1984.

[9] V. Cătuneanu, F. Popențiu, *Optimizing systems reliability*, Academy Publishing House, 1989.

[10] V. Cătuneanu, P. Svasta, I. Bacivarov (coord.), *Research in electronic technology and reliability*, Didactic and Pedagogical Publ. House, 1979.

[11] L. Balme, I. Bacivarov, European Program in Quality of Complex Integrated Systems (EPIQCS), *Quality Engineering*, 8, 4, 1996, pp. 675-680.

[12] I. Bacivarov, T. van der Wiele, Special Issue: Modern Approaches in Quality Engineering, Assurance, Management and Education. European Dimensions, *Quality Assurance*, no. 12-13, 1998.

[13] I.C. Bacivarov, L. Balme, A. Goncalves, *Quality Management, Assurance and Education. European Dimensions,* Inforec Press, 1999.

[14] Angelica Bacivarov, I.C. Bacivarov, A. Mihalache, *Reliability and maintainability of electronic systems*, Electronica 2000 Publ. House, 2003.

[15] I. Bacivarov, L. Balme (coord.), Quality Efforts in Europe, Special issue of the journal *Quality Engineering*, vol. 8, no. 4, 1996.

[16] I.C. Bacivarov, Angelica Bacivarov, Computer-Aided Education in Quality and Dependability at the Politehnica University of Bucharest - A Breakthrough, in Proceedings of the 4th International Conference in Reliability, Kishinew, 1996, pp. 24-29.

[17] I. Bacivarov, 45 Years of Postgraduate Technical Education in Quality and Reliability in Romania, *Quality Assurance*, vol. XXIII, 2017, pp. 2-10.

Growing the Cybersecurity Ecosystem: A Higher Education Perspective

Cătălin MIRONEANU, Simona CARAIMAN
"Gheorghe Asachi" Technical University of Iași, Romania
catalin.mironeanu@tuiasi.ro, simona.caraiman@tuiasi.ro

1. Introduction

Cybersecurity is a topic with many implications in all aspects of social and economic life. It does not affect only the telecom companies, the cloud resource providers and data centers or banks. It concerns and affects the entire economy and the entire society. Starting with our children who surf the web and play online games, to the networking specialists, and to our parents and grandparents who recently discovered social media and online payments, the digital activities of every person require a form of protection in the cyber space. However, there is a severe gap between the social, economic and policy needs of the cybersecurity field and the availability of specialized human resources. Moreover, the SARS-Cov2 pandemic context added up to this situation and widened this gap even more as more. In the accelerated technological development context, education represents one of the main pillars of the cybersecurity ecosystem. Consequently, many fingers are pointed at universities as they are expected to play their role in supporting and contributing to the growth of this ecosystem. Still, the Romanian universities are currently struggling to develop and integrate specialized study and research programs, as they are themselves victims of the lack of trained specialists.

The "Gheorghe Asachi" Technical University of Iasi (TUIASI) is among the oldest and most renowned public higher education institutions in Romania, having an important tradition in engineering, scientific and cultural education. TUIASI is a high-end research institution. Its mission is to carry out specific activities to create, to exploit and to transfer knowledge to the society in fundamental areas – Technical Sciences,

Architecture and Urbanism – as well as in interdisciplinary and complementary fields, involving the local community, as well as regional, national and international levels. It comprises 11 faculties, carrying out academic activities with more than 16000 students.

The cyber related ecosystem of TUIASI is mainly outlined around two of its faculties - the Faculty of Automatic Control and Computer Engineering and the Faculty of Electronics, Telecommunications and Information Technology – and the University's Data Center. Within this ecosystem, TUIASI provides two postgraduate study programs on Cybersecurity at the two mentioned faculties and is also affiliated to the European Doctoral School on the Common Security and Defense Policy. The cybersecurity related academic and Data Center activities are supported by specialized teaching and training staff, with formal certifications: Cisco Certified Network Associate Routing and Switching, Huawei Certified Network Associate, Huawei Certified Network Associate – Storage, Certified OpenStack Administrator, Amazon Web Services Certified Solutions Architect, Rittal Data Centre Infrastructure Specialist, Fortinet Network Security Professional. TUIASI runs training activities covering the topics of operating system, network and security layers within four specialized academies: Red Hat Academy, Huawei ICT Academy, MikroTik Academy and Fortinet Network Security Academy. A significant contribution to the University's objective of growing the cybersecurity competences and community is provided by the recent implementation of the Orange Educational Program with a particular emphasis on providing related training resources as well as supporting collaborative diploma, dissertation, doctoral and entrepreneurial projects.

The didactic and training activities related to cybersecurity are complemented by several research endeavors, such as the development of an Experimental Cyber Attack Detection Platform. The ECAD framework, which will be described in more detail in the following section, represents a valuable resource for both educational and research activities in the prospect of TUIASI's immediate objective to expand its academic programs with more specific and dedicated cybersecurity related curricula.

2. Experimental Cyber Attack Detection Platform at TUIASI

Nowadays, the acronym DX - 'Digital Transformation' has been used more and more often, related to the idea of digitizing the business area as much as possible, which means that much of the operational approach of organizations will migrate to the digital area. This transformation will lead not only to the migration of applications to servers, which is already happening, but also to the automation of many tasks. It is now a reality that jobs as system engineer or network engineer are being replaced by DevOps engineer jobs. Another aspect of DX is given by the exponential growth, within organizations, of 'smart' equipment - microprocessor equipment that is connected to the organization's network via an IP. Practically, it is the transition from the Internet-of-Things (IoT) to the Internet-of-Everything (IoE) paradigm. According to Cisco's definition in the publication Global Private Sector Economic Analysis, 'The Internet of Everything (IoE) brings together people, processes, data, and things to make networked connections more relevant and valuable than ever before - turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries.'[1]

In the IoT paradigm, the 'smart' devices create a new attack zone in the network, becoming a 'jump station' from which attacks can be proliferated. In the IoE paradigm the acronym SX - 'Security Transformation' occurred, in which one does not digitize everything for the sake of being digitized, but trying to provide security while digitization. This is transposed into a code of good practice, because we must provide protection when it is intended to introduce any equipment into the system, especially a 'smart' one, which can be a vulnerability. Obviously, it is an utopian idea to believe that all equipment will come from manufacturers with a sufficient degree of protection against attacks, so that the desire to protect the system, as a whole, can be achieved by other means. Thus, the integration of security in all digitized areas has led to the reiteration of the concept of Security Architecture, strengthening the principle of continuous assessment of trust. Building an efficient Security Architecture should take into consideration numerous aspects that are continually changing and must be adapted

[1] https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf

to arising reality. Let's remember here what Bruce Schneider said, as security guru: 'Security is a process, not a product.'

We consider as an outdated approach the quite usual strategy in which a single security point is built at the entrance of the network - a firewall through which we try to protect ourselves. The general approach is that smarter security starts with understanding how cybercriminals work. A 0-day attack that passes the entry point, without control and visibility at OSI level 2, will be allowed to spread within the organization, where traffic flows through switches. This is why we are developing a security framework, ECAD (Experimental Cyber Attack Detection), as part of Ph.D. research at the faculty of Automatic Control and Computer Engineering.

From our point of view, a sustainable security architecture must provide a safety background that ensures the visibility and security to all physical or virtual devices that compose the computer system. On the other hand, it must also provide security alerts related to security events from the involved areas, and therefore leading to certain decisions that must be provided to affected areas. We believe that with this approach we can demonstrate the effectiveness of a mechanism by which a large part of attacks can be isolated directly and automatically when they are detected. The detection rate will strongly depend on the 'intelligence degree' of the attachable components and mostly on the way in which the extracted knowledge and the security decisions taken are communicated between them.

The trigger that determined this perspective was the study of systemic vulnerabilities that contributed to the success of the WannaCry ransomware attack in May 2017, when research into the design of the ECAD framework took another turn. Shortly, WannaCry is a cryptolocker as a payload on a virus that was taking advantage of a vulnerability in the Server Message Block (SMB), which allowed it to spread to the network at OSI level 2. The spread was achieved through the EternalBlue exploit and the implant through the DoublePulsar backdoor, both developed by the National Security Agency (NSA). From the perspective described above, the lack of an automatic network segmentation decision system was the spreading factor, a security mechanism that would have worked regardless of the presence of SMB vulnerability.

Once this perspective was defined, a NAC (Network Access Control) module became vital to be integrated into the proposed security architecture, with the role of automatically profiling all network equipment and dispatching security decisions. From this perspective, the focus moves from APIs built by other security solution developers and connectors to cloud platforms, to DevOps, through scripts that automate configurations and give flexibility to the proposed security architecture.

Security decisions are made by a traffic analyzer processor which collects data from all equipment from the network. The vision is to employ services that are able to provide an IoC (Indicator of Compromise). These services also have the role of analyzing the knowledge and metadata extracted from the past traffic. It is possible that a past traffic, seemingly legitimate, in a new context with more data and knowledge accumulated, could be now considered harmful. Many 0-day attacks start from valid internet domains, on which there were no suspicions, but as phases of the attack take place, the analyzer can suspect that something is wrong and decide that the starting domain is suspicious.

Basically, the current traffic analyzer takes into account the past traffic to some extent, using levels of suspicion, and through a biunivocal relationship, the past traffic acquires a new relevance in the context of the current traffic. Equipment that has been significantly involved in communicating with that now-suspected area, which may not currently have traffic to or from that area, is considered compromised and may be isolated by automation commands or even through the network segmentation. It is an analogy of the sandbox principle in which suspicious files are detonated in an isolated environment, and if they prove to be harmful, a signature is extracted.

Most attacks are no longer made with known viruses, in which to rely on an antivirus signature. Without knowing the virus, we can't get its signature and we can only decide:

- based on vulnerabilities, if they try to take advantage of them - a path similar to signature-based detection, but in this case, that vulnerability must be known;

- if heuristic detection has been done, but this is an area to which our research is not directed. The disassembly, reverse-engineering and malware code analysis is done by specialized teams of antivirus solution providers;
- based on the behavior of the equipment in the network.

We must mention that all of these are estimates.

Completing the analogy with the sandbox, just as a virus can be labeled with a signature, we believe that a cyber attack can receive a signature, but a more complex one. In this sense, the designer of the ECAD security framework was inspired by the discussions with Alexandre Dulaunoy and Andras Iklody, two of the developers of the MISP platform (Malware Information Sharing Platform). The factor that triggered the development of the MISP platform was the automation of the process of distributing the knowledge gained from studying a harmful action in cyberspace. The process starts from storing IoC in a structured form, then disseminating to other instances from other communities and correlating information to all the beneficiaries of the platform to face an attack in a unitary way. For this reason, the architecture of our security framework will integrate the MISP platform under CC BY-SA 3.0 license (see Figure 1).

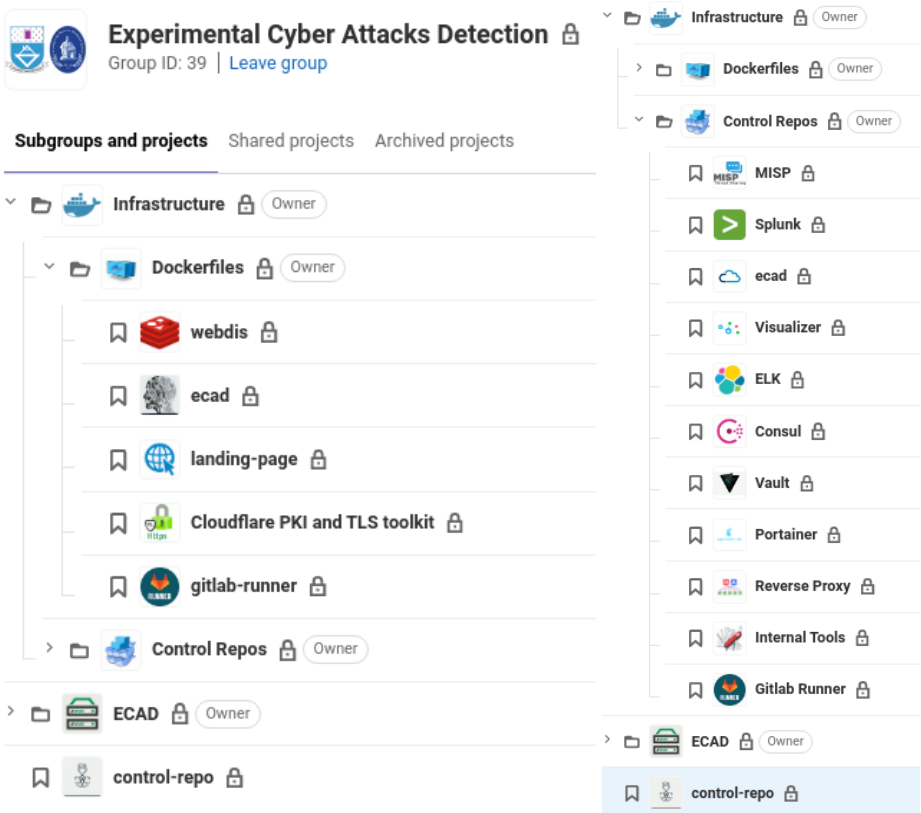


Fig. 1. *The ECAD infrastructure (ver. 20200601)*

Our intention for the proposed security architecture is that when an attack is detected, the entire infrastructure would be informed and thus protected through automated DevOps commands. The main principle used is Infrastructure as Code in software-defined environments, accelerated with advanced container security. The infrastructure has two types of components: stacks and images. The stacks are the part one can orchestrate. The images, as microservices, represent how components are built.

For orchestration we need a state (e.g. 'control-repo') that indicates which plugins are needed and where. In fact, this indicates the current state of the infrastructure. When the state is changing, the infrastructure is also changing.

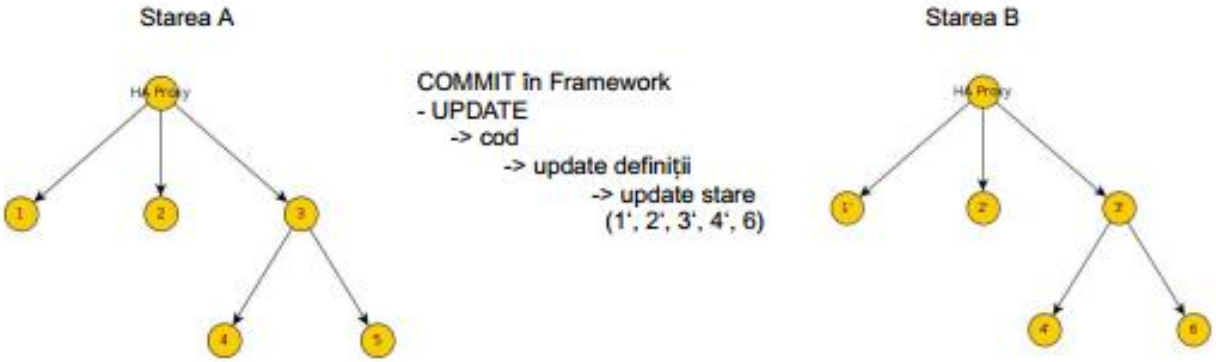


Fig. 2. *Infrastructure orchestration example*

Through an open platform, we can benefit from knowledge provided by other platforms with which we want integration, and, in turn, we can provide knowledge to them. Nevertheless, investing in a more advanced threat correlation approach will increase the level of effort required for threat actors to evade detection. Although no cyber security approach is completely safe, we hope, through this under development framework, to contribute to a security ecosystem and community.

As an open platform, ECAD will be available for exploitation as an educational resource in the current and future academic programs related to cybersecurity. All virtualization is performed on an OpenStack cloud computing platform, hosted by the computing resources of our University. Students will be able to develop modules that bring new functionalities, will be able to test ideas in which to measure the performance

in case of replacing modules built on other open source technologies and, especially, they will have access to a security framework open to any contribution.

3. Concluding Remarks

With the advent of the digital transformation of societies and economies, the role of universities in ensuring the required level of awareness and education regarding the horizontal and vertical cybersecurity topics is of utmost importance. In this context, TUIASI, as a technical university, has the clear vision of the requirement to provide professional and research skills and to foster the cybersecurity culture in the society.

The capacity building objective is first addressed by investing in the growth of its own community of specialists in the field. Moreover, this comes from a two-folded perspective: the university as an employer looking to ensure its own required human resource to support the academic programs and the operational activities in the Data Center, considered a strategic resource, as well as the university as a provider of solutions to the entire cybersecurity ecosystem. To this end, the development of research and educational resources, such as the ECAD platform, represents a very relevant field of investment. Still, such resources need to be further extended and supported, especially by collaborative projects with industrial partners.

Proposal for Practical Approaches to Information Security Education

Larisa GĂBUDEANU
Babeș-Bolyai University, Romania
larisagabudeanu@gmail.com

Given the significant changes in the technology sector, it has become clear that certain approaches to teaching should be further adapted to meet the industry demand for cybersecurity professionals. [1] The shortage of well-prepared professionals has been highlighted by industry reports in the past years. In addition, in other fields than the information technology or information security ones, basic knowledge in this domain are necessary for performing one's activity.

One manner in which the need for cybersecurity skills is analysed is through reviewing the ecosystem in which the student enter after graduating university and the specific real-life scenarios and situations that will be encountered by the students during their professional life.

The below sections explore potential steps forward that can be considered, while each university can decide the best approach from its perspective, given existing curricula and resources. [2] Further, in view of changing existing approaches, there may be certain legislative shortcoming that have to be adjusted, updated and correlated in order to include some of the below proposals and to allow proper implementation of such proposals.

Moreover, for some of the proposals, the involvement of multiple persons/entities from different areas is needed in order for the cooperation to be useful and efficient for all relevant parties. Such cooperation can be achieved in a centralised manner, through legislation and specific legal norms or can be left to the discretion of each educational establishment.

Of course, in order to ensure proper addressing of the training model, the below can be integrated in the teaching framework and strategy at the national level or at the university level, as appropriate. This ensures that students are brought in a cybersecurity community appropriate to their interest, their level of expertise and the relevant user-level cybersecurity knowledge needed.

1. Cooperation with public or privacy entities

The cooperation with public or private entities can bring advantages to universities, especially in terms of hands-on (e.g. practical exercises reflecting real scenarios), useful and up-to-date content for the courses. There are various approaches that can be taken and we have listed a couple below.

An easy to implement and efficient approach for providing constantly updated curricula in line with current business environment entails industry invitees in the course. [3] This may also prove useful in terms of hands-on exercises and case studies provided to the students which are beginning to be used by universities.

In terms of bachelor and master (LLM) thesis/dissertation, an implementation option entails the cooperation between the university and a private/public entity. In this scenario, the students can have a specific and practical topic for their thesis/dissertation (e.g. a project pertaining to the R&D or business development of the private entity).

In this manner, the students gain insight into real-life use cases of frameworks and methodologies that they are trying to use for the thesis or dissertation. Further, they cooperate within the business environment with experts from their particular field and gain valuable knowledge (and references) for future employment opportunities or projects.

From the private entity’s perspective, it obtains useful research input from the students that can be used on the short and long term. In addition, these entities have the chance to know the students in an actual working environment, making it easier for them to identify the students that best fit into the company in the future and to offer future job opportunities to appropriate students.

Further, the university obtains recognition in the student community for providing practical knowledge to students and also in the academic community for having useful (and state-of-the art) research outputs. This approach may lead to an increase in the number of students that opt for master or PhD studies.

2. Usefulness of inter-disciplinary approach

As in the business or public sector environment, cybersecurity should be viewed in the wider context. Thus, aside from specific technical aspects, legal, management (e.g. project management, process management) and economical points are also useful for students in view of a broader understanding of the role of cybersecurity in the business environment and public sector.

Further, in order to look at information security in context, there is a need, on the one hand, to analyse the technical aspects and, on the other hand, to analyse the matters concerning the integration with the organisation processes. Such integration includes matters concerning information security management, risk analysis in terms of information security and the methodology related thereto, as well as project management aspects.

On the correlation between legal requirements and technology, privacy engineering can bridge the gap between privacy-by-design, security-by-design and privacy-by-default requirements and existing curricula on software development, together with an integration of these requirements with the software development life cycle, both for waterfall and agile type of development methods. [4] This has begun to be implemented over the past years by certain universities and it is catching on as an inter-disciplinary model. Such interaction is emphasised also by current standardisation and certification discussions at the European Union level.

3. The moment at which information security concepts are presented to pupils/students

The moment at which students are introduced to cybersecurity concepts, either only for personal use or for future career prospective, should match the moment they

are introduced to technology, as the two are correlated also from a user perspective in order to ensure safe use of online tools.

This is relevant, as they have to possess the relevant knowledge to protect themselves and their devices properly. [5] Given the current society habits in this respect, the need for such information occurs before the student enters university. In this section, we outline a couple of approaches to consider in this respect.

In certain cases, for entry-level cybersecurity concepts, it may be useful to approach high school students or even students before they enter high school. This ensures that these pupils/students have actual knowledge about information technology/information security before choosing a specialisation in university. Further, such entry-level knowledge helps with raising awareness in each individual that is using or will be using IT applications and IT systems. Having knowledge about information security from a young age (e.g. middle school, high school) can contribute also to increasing the number of female students in universities having an information technology or information security specialisation.

A certain level of cybersecurity knowledge in universities with non-IT background also ensures that the human factor in the cybersecurity ecosystem is better prepared for real-life challenges in this respect.

Further, in universities having domains not related to IT, specific points relating to cybersecurity (and their relevant applicability in the context of information technology and in the technology landscape) should be included from the outset in order to properly prepare the students for the future. For instance, in case of medicine students, aspects relating to e-Health information technology solutions or approaches and related security measures concerning the e-Health solutions should be included in the curricula in order to prepare students for working in an environment that has an increasing level of technology elements embedded in the day-today activity of medical professionals. For law students, IT and related cybersecurity aspects should be presented in order for them to be able to translate the implemented IT/cybersecurity points by reference to legal requirements. Understanding the principles of information technology solutions and architectures, together with the information security

approaches, governance and implementation are essential in order to analyse contracts or litigation cases from all relevant factual angles.

Another approach taken in recent years is to have a bachelor in cybersecurity instead of the previous approach which included a general IT bachelor degree with a master program to go in more details on the security side of the IT components and concepts learnt during the bachelor years. This may prove a useful approach, depending on the curricula, in order to embed the security part alongside the IT course (e.g. for software development also secure coding practices). Emphasising the principles and approaches to source code writing taking into account software security ensures that the software developed by students after graduating university have security embedded in it from the design phase.

Involvement of private and public entities can take the form of a mentorship program, in which mentors for certain specific projects are information security professionals, including alumni of the respective university.

Of course, irrespective of the options chosen by the students in the private/public domain, the emphasis is also on courses or interactions with professors, with the aim of updating continuously the level of knowledge of professors with new elements from the business environment.

4. Cooperation between universities

In terms of course projects or thesis/dissertation, as different universities approach IT topics in various manners, it may also be useful to create inter-universities cooperation and exchange of experience. This can take the form of a framework agreement, with specific national/international programs to which universities can apply. [6] In both situations, the actual projects completed together are established on a case by case basis, depending on the need to analyse a specific topic that is relevant from a research perspective at that moment.

This form of cooperation is useful not only at the national level, but also at the international level. At the moment, the cooperation mainly occurs at the PhD level,

through common projects, articles and conferences organisation by multiple universities. However, this can be extended similarly for the master and bachelor levels.

The universities can have in mind also an approach that has been used more frequently in many domains, respectively, inviting professors from another university to hold a presentation for the students on a specific topic closely related to the expertise of the invited professor.

5. Extra-curricular activities

Useful practical approaches can include Capture-the-Flag exercises for students either during the courses in the curricula or as an extra-curricular activity. These types of activities bring practical examples and help students to consolidate concepts learnt during the courses. [7] Of course, an appropriate gamification mechanism should be implemented, taking into account specific characteristics of the university, course content and background of students.

This ties in also with encouragement of students to participate in international or national information security related competitions, with proper coaching for mentoring from professors or from certain professional volunteers from public sector or private sector.

Depending on the post-university professional trajectory of the student, cooperation with relevant national or international cybersecurity associations in the market can be considered in order for students to benefit from certification courses and certification exams. This can bring the student useful knowledge for post-university life/professional life and can bring valuable updated insights into the academic environment.

In terms of gamification, for penetration testing type of activities, for instance, badges, certificates, and diplomas that can be used on social media and on CVs can also be useful. In such cases, these prove the practical technical experience of students in real-life scenarios in which they may find themselves in the future.

Currently, passionate students perform such activities on their own or through a cybersecurity non-governmental organisation/cybersecurity learning platform

performed/webinars certain items from the above. [8] Nevertheless, under the guidance of the professors, more students can have such additional knowledge/experience and the structure/learning path of practical skills included in the curricula can be guided towards the ones useful for the future.

Consequently, the main steps for increasing the level of knowledge in terms of information security can include the above directions. These directions have the purpose of maintaining an updated curricula for educational entities in order to offer students an adequate level of knowledge for their activity after graduation, during their professional life. The cooperation with other fields of activity (e.g. economic, legal, management) is essential in this respect. Further, a holistic and multi-disciplinary approach can increase the impact on the activity after graduation. In addition, the following can contribute to the practical expertise gathered by the students: the cooperation with other educational entities, with private entities, public entities and relevant NGOs (including those providing courses and certification).

References

[1] ENISA, "*Information security Education snapshot for workforce development in the EU*", 2015, [Online]. Available at: https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/cybersecurity-education-snapshot-for-workforce-development-in-the-eu/view. [Accessed on 15 October 2020].

[2] June Wei, "*Knowledge management framework for cyber security learning*", 2010, International Journal of Management in Education, Vol. 4, No. 1 [Online]. Available at: https://www.researchgate.net/publication/249922925_Knowledge_management_framework_for_cyber_security_learning. [Accessed on 15 October 2020].

[3] ISACA, "*Tech Workforce Report*", 2020, [Online]. Available at: https://www.isaca.org/-/media/info/tech-workforce-2020/index.html. [Accessed on 15 October 2020].

[4] ENISA, "*Information security Higher Education Database*", [Online]. Available at: https://www.enisa.europa.eu/topics/cybersecurity-education/education-map. [Accessed on 15 October 2020].

[5] ENISA, "*Information security Skills Development in the EU*", 2020, [Online]. Available at: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union. [Accessed on 15 October 2020].

[6] European Cyber-Security Organisation, "*Gaps in European Cyber Education and Professional Training*" [Online]. Available at: https://ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf. [Accessed on 15 October 2020].

[7] Cyber.org, "*The State of Information security Education in K-12 Schools*" [Online]. Available at: https://cyber.org/news/state-cybersecurity-education-k-12-schools. [Accessed on 15 October 2020].

[8] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou, "*Global Perspectives on Information security Education for 2030: A Case for a Meta-discipline*". in Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE Companion '18), 2-4 July 2018, Larnaca, Cyprus. ACM, US, [Online]. Available at: https://doi.org/10.1145/3293881.3295778. [Accessed on 15 October 2020].

Development of a Customized Master's Program in Cybersecurity for the Field of Electronics, Telecommunications, and Information Technologies

Eduard-Cristian POPOVICI, Octavian FRATU, Simona-Viorica HALUNGA, Laurențiu BOICESCU
Telecommunication Department, ETTI Faculty, POLITEHNICA University of Bucharest, Romania
eduard.popovici@upb.ro, octavian.fratu@upb.ro, simona.halunga@upb.ro, laurentiu.boicescu@upb.ro

1. Introduction

In this article, we want to recount the motivations, methodology, most important steps and plans for the creation of a new master's program in cybersecurity, customized for Electronics, Telecommunications and Information Technologies, in the Faculty of Electronics, Telecommunications and Information Technology (ETTI) from the Polytechnic University of Bucharest (UPB).

2. The context and motivations for creating the new master's program

In the following, we will present the national and local context, as well as the motivations, objectives, and principles that led to the creation of the new master's program in cybersecurity.

2.1. National context

We started the analysis of the national context starting from a very good review of the main master's degree programs in cybersecurity in 2017, made in the subchapter "4.2. *The importance of education and research in the field of cybersecurity*" of the study "*Current challenges in the field of cybersecurity - impact and contribution of Romania in the field*" [1].

From this document, but also the own analysis of the educational offer at master's level with cybersecurity theme, it can be easily seen that currently there is no master's program with specific Electronics and Telecommunications, besides Information Technologies (which are the subject of several such programs).

In this context, in the last 2 years, the CYBERINT National Center within the Romanian Intelligence Service (SRI) and CERT-RO have urged and expressed their support for the creation of new master programs on cybersecurity. In September 2018 Anton Rog, general director at the CYBERINT National Center of SRI, stated at the CyberSecurity Romania Congress in Sibiu, that "*a national program of education and training of cybersecurity specialists, which is already considered by the institution, could double the percentage of GDP produced by the Romanian IT market, which is currently 6% within a decade*" [2].

Fig. 1. *Anton Rog at the CyberSecurity Romania Congress in Sibiu* [2]

Anton Rog mentioned that there are not enough training programs for this field in Romanian universities, so the institution launched a partnership to the university environment: "*As we observed that in Romanian universities there are not enough postgraduate courses or courses master in cybersecurity we decided to take a tour of the 12 main universities in Romania with a technical profile and to propose them to develop*

such short training courses of 2-6 months and with master courses of one year or one year and a half" [2].

2.2. Motivations for the creation and objectives of the new master's program

The need to create a new master's program, entirely dedicated to cybersecurity in the Faculty of ETTI has become clear since 2015. On the one hand, the Faculty has programs that only partially include this topic, given that both Electronics and Telecommunications and Information Technologies are strongly interconnected with cybersecurity issues. On the other hand, at the University's management level, the need for such programs in the Faculties of Electronics and Computers was discussed, and the initial plan was to jointly carry out such a program.

Thus, after such a new program appeared in 2017 in the Faculty of Automatic Control and Computer Science (adapted to the respective Faculty), the management of the Department of Telecommunications, a department in which there is a large majority of teachers specialized in cybersecurity in the Faculty of ETTI, was entrusted to create a team from within the Faculty able to create a new program (customized for the ETTI Faculty).

In this context, the encouragement and support received from the institutions mentioned in the previous subchapter, helped to materialize these plans, as will be described below.

In summary, the main motivations and objectives of the construction of this program were:

- on the one hand, the recommendations made by the specialists from the partner institutions and companies, with who our team collaborated didactically or on research projects (or only made proposals for financing such projects), who referenced a shortage of specialists with master's level training and also their interest in hiring graduates of a new master's program in the field of cybersecurity;
- on the other hand, our desire to create and offer a master's program that takes advantage of the specific expertise of the academic community in the Faculty

of Electronics, Telecommunications and Information Technology (electronic devices and equipment, electronic systems, communication systems, multimedia content processing, fixed and mobile terminals, software applications and systems);

- benefiting from cooperation with colleagues from other Faculties and specialists from partner institutions and companies, who can provide expertise in areas complementary to those we cover, such as cryptology, industrial control systems, critical infrastructures, security and auditing standards;
- at the end, the graduates of the program will have practical skills in the field of security of equipment and information and communication systems, as well as advanced skills in designing and implementing integrated hardware-software security solutions.

The main target group is that of the graduates of the Faculties with ETTI, CTI, Informatics, and other profiles, from the Faculties of ETTI, Automation and Computer Science, FILS, Electrical Engineering, FSA, Transports, and others, within UPB. But we want to offer this program to other target groups, such as graduates of faculties with other types of technical profiles from UPB, respectively graduates with similar profiles from ATM, Bucharest University, the Academy of Economic Studies, etc.

2.3. The principles of the new master's program

As a result of the discussions with the professors specialized in cybersecurity within the Faculty, with a series of institutional partners and private partner companies, a series of principles on which the new program was built emerged, the most important of which are:

- creating a program to cover real labor market needs;
- implementing a specific program of the ETTI Faculty ensuring complementarity with (and differentiation from) other university programs in the field of cybersecurity;
- creating a program with clear and well-argued discipline flows;

- developing collaboration within UPB, involving, when necessary, colleagues from other Faculties (Faculty of Engineering in Foreign Languages - FILS, Automation and Computers, etc.);
- developing collaboration within the ETTI Faculty (between departments) by including professors from all four departments of the Faculty;
- collaboration with profile institutions (SIE, CYBERINT-SRI, ITA-SRI, CERT-RO, STS, etc.) and involvement of invited specialist from these institutions;
- collaboration with specialized companies (Safetech Innovations, Bitdefender, Fortinet, etc.) and the involvement of invited experts from these companies;
- collaboration with partner companies of the ETTI Faculty (Orange Romania, Beia Consulting, Ericsson, etc.) and the involvement of experts invited from them.

2.4. The local context of creating a new master's program

As mentioned, the ETTI Faculty does not have a fully dedicated program, but there is a well-trained faculty in the field of cybersecurity, involved in teaching in several master's programs in the ETTI Faculty and other Faculties (FSA, etc.).

Thus, in the ETTI Faculty, we identified a team that includes 6 university professors, 9 associate professors, and 12 heads of university works. Following the principle mentioned above, they are part of all four other departments of the Faculty.

Starting from the stated objective of developing collaboration within UPB, the new master's program benefits from the participation of professors from both the Faculty of Electronics, Telecommunications and Information Technology (ETTI) and the Faculty of Engineering in Foreign Languages (FILS) as well as from the Faculty of Automatic Control and Computer Science (ACS).

Regarding the development of the collaboration within the ETTI Faculty, the master's program is carried out with the participation of professors from the Telecommunications Department and the other 3 departments of the ETTI Faculty: DCAE, EAII, and TEF.

We also have future visiting professors some Ph.D. employees from the institutions as well as from the aforementioned companies.

3. The main stages of the development of the new master's program in cybersecurity

Next we will present the steps we have taken to create the new master's program.

3.1. Preliminary market study

As previously mentioned, starting with 2017 we made a first market study, finding out that there is potential for a new program to cover the areas of hardware in electronics and telecommunications, along with those of associated software, resulting in a set of areas and subdomains to be covered by the future program, for which we have the necessary faculty. At this stage, we also discussed with a small number of representatives of some partner institutions and companies. It is worth mentioning the discussions we had with the mixed team, made up of specialists from the Cryptology Laboratory of SIE and teachers from the Faculty, who are currently teaching introductory courses in Cryptology, but also the discussions with representatives of the main partners of the Faculty, the Orange Romania company, which has been running the Orange Educational Program in the ETTI Faculty for over 2 decades, a program that includes a consistent section dedicated to cybersecurity in the telecommunications field, as well as discussions with Safetech Innovation, our partner in recent years in a series of research projects on cybersecurity, a company recommended by the profile institutions as a partner for new master's programs.

3.2. Institutional and private partners' support

After this step, we proceeded to deepen the market study, requesting and obtaining (including officially, through letters of support) the institutional support and of the private partners (as representatives of the labor market) to identify their need for those areas and subdomains and to customize the expertise on which we will follow out the curriculum of the new program.

Among the partners, we can mention profile institutions such as the Cryptology Laboratory of SIE (with which, as I mentioned, we already have a traditional collaboration in the field of cryptology), the Institute for Advanced Technologies ITA-SRI, and STS (with which we had collaborations in cybersecurity research projects), CYBERINT-SRI, CERT-RO and NSC (New Strategy Center - the initiator of the PatriotFest competition), with which we want to collaborate through the invited specialists.

The companies that have shown interest in collaborating are Safetech Innovations (with which we have been collaborating for several years in cybersecurity research projects, so it is our main partner in establishing the program strategy), Secureworks, and other companies (such as Fortinet, a partner in the Orange Educational Program), with whom we had discussions to provide us with invited specialists in several disciplines in the program, but also access to infrastructure, to achieve a program well anchored in technological realities and the market. Last but not least, we have the support of partner companies such as Orange Romania, main partners in terms of strategy to follow, Beia Consulting and other companies, which we hope will offer us other invited specialists.

3.3. Selection and harmonization of curriculum proposals

After going through these stages, we continued to select and harmonize the proposals in the curriculum, establishing on this occasion a better-defined team. In this context, we generally consider that each discipline is potentially covered by a team of colleagues, both for the diversity of individual specializations and to have a staff reserve.

At this stage we concluded the previous discussions within the team and with the institutional and private partners, resulting in the following list of knowledge that we would provide within the program. Thus, graduates would be able to:

- draw up a technical project in the field of telecommunications, in particular in the field of security of communications;
- assess security risks;

- understand and develop specifications for secure electronic and communication equipment and systems;
- be aware of security vulnerabilities and risks in telecommunications protocols and networks;
- know the main security protocols;
- be able to implement security plans at the level of critical organizations/infrastructures;
- know how to implement cryptographic applications, systems and protocols;
- know how to work with FPGA devices and on-chip systems;
- know the architecture and characteristics of secure hardware systems (computers, mobile terminals);
- know the architecture and characteristics of secure software systems (databases, software applications);
- know the most important and current security and auditing standards;
- know advanced security solutions based on machine learning, artificial intelligence, and big data;
- know the issue of securing and exploiting multimedia content.

Following the analyzes performed by our specialized academic community, and with the participation and consultation of specialists of strategic partners (Orange Romania, Safetech Innovations, Cryptology Laboratory of SIE) the program was designed to provide skills in the following areas:

- security of radio communication media, wireless systems, sensor and IoT networks, vehicles, etc.;
- cryptographic applications and systems, including advanced ones (lightweight, block-chain, postquantum, etc.);
- design of security systems with FPGA devices, on-chip systems, embedded cryptography, etc.;
- protection of telecommunications protocols and networks (including virtualization and cloud), working with security protocols;

- security of hardware systems (computers, mobile terminals) and software (databases, software applications);
- security of industrial control systems and critical infrastructures, security and auditing standards;
- machine-learning elements, the issue of security of artificial intelligence and massive data (big data);
- security (watermarking, etc.) and utilization of multimedia content (biometrics).

In the end, the distribution of the contents of the fields of study within the program on the 3 main axes of the Faculty: electronics, telecommunications, and information technologies, resulted as presented in Table 1.

Tab. 1. *Distribution of the contents of the fields of study by domain*

Domain	**No. of courses**	**Allocated hours**
Electronics	4	12
Telecommunications	6	16
Information technologies	5	14
Others (management etc.)	3	6

As can be seen, the disciplines in the subdomains of Electronics and Telecommunications make the largest proportion, which differentiates this master's program from the others existing in Romania.

Also, at this stage, of establishing the curricula, it was decided the name of the new master's program. To be as clear as possible, we looked for a name that would assort as well as possible with both the subjects in the curriculum and the list of competencies provided.

The official name in English, the language in which is taught, is *Security Management of Informational and Communication Equipment and Systems (SMICES)*, which has as equivalent in Romanian the name *Managementul Securităţii Echipamentelor şi Sistemelor Informaţionale şi de Comunicaţie*. This name reflects very well the distribution of the contents of the fields of study in the curriculum on the three main subdomains, but also the management elements that complete the program.

4. Conclusions. The current situation and future plans

In 2019, we first requested and obtained the approval of the Senate of the Polytechnic University of Bucharest (UPB) to take the necessary steps to accredit the new program. Then we obtained the approval of a new qualification, with the same name as the master's program, "*Security Management of Information and Communication Equipment and Systems*" from the National Authority for Qualifications (ANC).

We are currently in the process of updating the detailed proposals, taking into account the current and projected impact of moving to online and digital courses and applications, including adding in the mixed/extended reality components, for which we are in the process of making new partnerships with the research and development community in this field.

After obtaining the ARACIS accreditation based on the updated file, we want to offer in 2021 master training opportunities complementary to those offered by the other cybersecurity master programs, as we set out from the beginning.

Bibliographical references

[1] I. C. Mihai, C. Ciuchi, G. M. Petrică, "Current challenges in the field of cybersecurity - Romania's impact and contribution in the field.", *Strategy and Policy Studies SPOS 2017*, Study no. 4, Bucharest, pp. 67-72, 2017. Available at http://ier.gov.ro/publication-category/studii-strategie-politici/ [Accessed on 10.10.2020].

[2] A. Rog, "A national cybersecurity education program will double the percentage of GDP produced by the IT market in Romania", Agerpres, 2018. [Online]. Available at https://www.agerpres.ro/cybersecurity/2018/09/13/anton-rog-cyberint-sri-un-program-national-de-educatie-in-cybersecurity-va-dubla-procentul-pib-produs-de-piata-it-in-romania--175617 [Accessed on 10.10.2020].

Education Versus Cyber Challenges

Mircea-Constantin ȘCHEAU
University of Craiova
mircea.scheau@edu.ucv.ro

Abstract: With the help of advanced technologies we want to have as much comfort as possible, but the advantages come with a series of rules that we must follow. It is not necessary to become specialists, but it is certainly necessary to keep ourselves informed about the dangers to which we are exposed. Otherwise, the price paid due to ignorance or superficiality may far exceed the darkest expectations. We can be a direct target, a collateral victim, or a valuable tool of malicious access in a certain context speculated or created by a hostile actor. It largely depends on us which position we choose. The impact can also be reflected in the direction of national security.

1. Introduction

The notion of security is perceived differently depending on the culture or the degree of understanding, and therefore social groups relate differently to the concept. For more than three decades, cybersecurity has been primarily technologically assessed, with the human factor, which is just as vulnerable, taking a back seat. Emphasis was placed on infrastructure, communications, processing, programs, hard devices, or firewall systems, and less on "old-fashioned" attacks on administrators or operators. Evolution imposes, among other things, changes in behavior, strategies, priorities, values, permissions, and limitations. Branches of science that deal with the study of attitudes and personality traits, can provide indications of the user's predilection to respect or non-comply with internal policies or ethical rules, specific to a community or an environment of activity. Education is a fundamental component of the human complex. The inherited knowledge is completed with the acquired ones, the principle of Gauss's bell being applied differently in this case.

The regulation of the virtual space must offer solutions to the problems related to anonymity, real-time availability at the request of law enforcement agencies, activation of blocking mechanisms for malicious attacks, etc. Compliance rules are imposed by scientific quality standards.

In the next section, we will try to provide a clearer overview, presenting several types of threats, as a prologue to the chapter in which we will analyze the need to introduce computer security disciplines in the pedagogical curriculum.

2. Parallel confrontations and intersections of interests

It is increasingly difficult to identify the actors behind a cyber attack given that the capabilities engaged are state-supported. The fingerprints of programmers are imitated by teams specialized in actions directed against the critical infrastructures of a state or international organization. The investigation is difficult and there is a danger of accusing and involving entities other than those guilty of causing losses in a third conflict. Stylometry appeals to Artificial Intelligence (AI) resources and comes to the aid of cyber defense teams, but even in these conditions, there is a risk of hijacking or delay in obtaining a result in identifying real aggressors.

2.1. Government entities as targets for cyber espionage

A series of events that prove the escalation of cyber conflicts at all levels marked the beginning of 2020. Vietnamese officials, involved in territorial disputes in the South China Sea, are suspected of being targets of a phishing campaign. The computer systems in the office of the Taiwanese president, who was to be sworn in for a second term, were penetrated, and several sets of documents were compromised.

Analyzes show that some of the operations took place over several years, one of the reports [5] detailing espionage activities attributed to an Advanced Persistent Threat (APT) group [27], which were directed against several government institutions in the Asia-Pacific region, belonging to Australia and the states of Brunei, the Philippines, Indonesia, Myanmar, Thailand, Vietnam, etc. Modus operandi is ingenious and includes the use of a custom Remote Access Trojan (RAT) [2], the

backdoor called Aria-body, the delivery of malicious emails, Rich Text Format (RTF) files [18] infected with Royal Road [25] exploit builder, etc. Several Domain Name Systems (DNS) have been active for long periods and have jumped to the same Autonomous System Number (ASN) in a short time. Pirated government infrastructure has been exploited as Command and Control (C&C) servers [21]. The Aria-body backdoor functionality is very similar to that of the XsFunction backdoor, analyzed extensively in 2015 [14].

Fig. 1. *Countries exposed to attacks* [5]

On the other hand, according to a study [11] by a well-known company, another APT conducted intrusion campaigns aimed at ministerial units for coordination and management of emergencies belonging to a state with which the diplomatic relations of the state sponsoring the aggressions are quite stressed, to obtain information on the crisis caused by the SARS-CoV-2 pandemic. In the first stage, an email was sent with a built-in tracking link, with the role of reporting whether the message was opened and thus confirming the validity of the address. When an autostart metal jack loader is loaded, it executes one of the built-in resources. The malware loads a shellcode into an additional resource Message-Digest algorithm 5 (MD5) [12], performs a system survey to collect data on computer names, usernames (etc.), and adds the information in a

string URL. If the URL call is completed successfully, the malware loads the metal jack payload into memory.

2.2. Cybercrime and financial profit

The financial field is not bypassed either. The fraud recorded in May 2020, assumed and declared, amounts to around the equivalent of 10 million US dollars. The victim was one of the strongest private equity funds [20] in the world, supporting, in particular, the production, agriculture, and renewable energy sectors of developing countries. The attackers intercepted Norwegian officials' correspondence with a microfinance institution in Cambodia. They manipulated the exchange of information and falsified the transfer documents. The amount was redirected to an account in Mexico, the details of the account in which the money was collected being almost identical to those of the recipient, a traditional partner.

The companies were also targeted, with a major British airline [16] stating that the personal data of around nine million customers had been affected. As a result of an "extremely sophisticated" attack, the details of the trip and the e-mail addresses were "stolen", but what worries the most the representatives and the authorities investigating the incident are the 2,208 cards exposed, as during the incident the codes of digital security, CVV or CVC, were also captured. Other airlines in the Middle East have also fallen victim to attacks aimed at data leakage, and although they have been more difficult to attribute to a particular group, the report [1] of the specialist company presenting the case under investigation identifies the APT from behind the threats. Some situations are more complex, but the mode of operation identifies quite clearly the common stages of aggression that include account creation, carefully planned social engineering campaigns, or use of tools to maintain the presence and lateral movement. The technical details are interesting to follow.

2.3. Military cyber espionage

Industrial espionage can be classified as military espionage if information related to a country's defense system is leaked from a strategic manufacturer. Investigators

believe that a team of hackers managed to penetrate a contractor's network [6] due to the vulnerabilities of the software and the hardware produced in the state that allegedly supported the attack. The targeted technical specifications probably included information related to the type of rocket, propulsion, level of heat resistance, etc. Equally interesting is the fact that data on employees, retirees, and candidates for certain positions within the company were accessed, which demonstrates the attackers' particular concern about the organization, functioning, and personnel policy.

Fig. 2. *Attack on a military contractor* [19]

The explicit focus on high-potential military targets [22] becomes rather worrying, especially since nuclear intercontinental ballistic missiles are a priori assumed to benefit from advanced protection systems. The strength of a chain lies in the strength of the weakest link in the chain. In another case, the authors penetrated the contractor's network by compromising a domain administrator's account, "successfully" encrypted the aerospace provider's systems [26], and extracted data considered to be particularly sensitive. Incidents can easily be classified as cyberwarfare, as they can have the effect of making more capabilities unavailable during an ongoing operation, as was the case in one of the first such episodes [17] in 2007.

2.4. Exposure, aggression and response

Concerning the commercial area, certain actions may have quantifiable effects. Others, however, may have secondary trajectories that are difficult to anticipate, especially if they affect the environment. Where a cyber attack on a semiconductor company can be financially justified, an attack on a company operating in the oil industry can jeopardize the capacity of control devices and decisively disrupt the production flow. If several such attacks are concentrated in a short time, targets in the same area are exposed and common code segments or similar approach procedures are identified, the process can be assimilated to concerted aggression [7], directed against that state. The technical fragments may differ from case to case, but the motivation is what fuels the process.

From another perspective, some attacks can be perceived as a response to aggression [9] against the civilian population. Traffic in the naval port area located in the Middle East near the Strait of Hormuz stopped and was seriously disrupted later for several days, some private handling systems were damaged, and dozens of ships loaded with containers were forced to anchor outside the download area. The statements of the officials of the two parties involved in the conflict were contradictory, but the message that was intended to be transmitted [13] was to maintain a minimum level of ethics regarding the non-involvement of civilian infrastructures in sterile conflicts.

2.5. Data transmission in the context of cybercrime

Dual-use civilian and military goods become the subject of dispute in public debates, the export or import of equipment and systems to or from countries with non-democratic regimes or suspected of endangering other democracies are intended to be restricted. Maybe that's why some governments [24] decide to implement new technologies for critical infrastructure, turning to providers in states considered to be allies.

Communication networks provide access to the resources of recipients who can be spied due to vulnerabilities and security breaches exploited by criminal groups,

which use virtual "tunnels" to stay connected to victims' systems. While not all telecommunications service providers can afford to invest large sums in security, certain areas, such as South Asia, are easier to penetrate. According to the report [4] prepared by a specialized company, the range of infection vectors is diversified, and particularly interesting is that publicly available hacking tools are also used. A management utility can be operated to load the executable needed for the operation process, but may also be abused by malicious actors to download harmful tools to the compromised machine.

Increased capacity of data transfer creates the premises for the exchange of information at higher speeds, offering the same type of tools to attackers, who broaden their area of addressability and action through Crime-as-a-Service offers [15]. They provide those interested with complex packages, with verified code sequences adapted to the "customer's" need, with user's manuals and technical support. The selection of "champions" increases the number of "volunteers" who can build distributed or focused attacks on the same target. As I specified at the beginning of the article, it is increasingly difficult to identify the actors behind a cyber attack. An event can be misinterpreted and by default, misjudged in the first instance and that is why, in the field of cybercrime, several alternative scenarios must be considered before implementing a final decision [8]. For example, for DDoS-for-hire or "booter", which is no longer a secret to anyone, the authorities take the right positions, trying to discourage such initiatives [3].

3. Cyber education

Cybersecurity is an expanding and ever-changing field. The cases presented in the previous chapter refer only to some of the areas that need to be handled by specialists capable of preventing aggression, treating the problem, and ensuring resilience. From an organizational perspective, the responsibility for managing cybersecurity risk rests with each of us - manager, leader, or simple employee. From a personal perspective, we just need to adapt to new realities and inform ourselves as best we can to try to avoid current challenges.

Cyber employees, regardless of industry, public or private, are acting as national security protection and must be associated with critical infrastructure [28]. The correlative principle causality - effect reveals in this case, however, that appropriate training is directly dependent on the reduction of the gaps of economic and technological development and an increase of the quality of the educational activity. The National Defense Strategy of Romania for the period 2020 - 2024 refers to hybrid cyber threats, interconnected risks, and, implicitly, the resizing of the perception of cross-border crime. Aggressions can have ideological, economic, expansionist motivation, etc., or they can be the result of behavioral exhibitionism out of control and derived from the need for affirmation or recognition. Disruptive sources use cosmopolitan power channels and involve conventional weapons or weapons of mass destruction [23].

Fig. 3. *Stages in building a cybersecurity climate* [29]

The National Institute of Standards and Technology proposals to build a reference framework for cybersecurity staff training [29] are illustrated in figure 3. The first set of recommendations refers to the use of a common language in communication between trainers, certification bodies, employees, employers, etc. A critical analysis is required to identify the skills necessary for high-risk positions, as well as the usual ones, needed in multiple roles. It is also necessary to carry out an analysis of skills

related to short, medium, and long-term development expectations and capabilities. It is important to allocate roles and tasks in line with the available tools and human capital.

The study by the National Institute of Standards and Technology states that "academic institutions (as a whole) are a critical component of training and education ... in cybersecurity" [29]. The transfer of knowledge must take place naturally, within programs harmonized with the lexicon of the operational sectors. This creates the premises for a two-way relationship between the education system and that of employers. They increase the chances of absorption in the field of work of high school, graduate, or postgraduate students, who can prepare on platforms developed in a public-private partnership.

The same ideas are supported by the European Union Agency for Network and Information Security (ENISA), which advocates for compulsory security courses in computer science and engineering faculties. They may be optional for other specialties, but the general concept that any "student" should understand before learning "how" to code is that one must first of all "learn to code safely". All other development modules, regardless of direction, are required to adhere to this concept [10].

Attempts to shape the human factor without remedying the system or readjusting the system based on traditional social models are doomed to failure because the cyber world allows for sensitive changes in the hierarchy of value systems. Computer tools are accessible to any generation and respond just as promptly to commands. A teenager can always compete with an adult. Passion, analytical ability, and speed of reaction are counterbalances to experience. Coagulation of teams launched in competitions is no longer limited by age, gender, or other conditions considered naturally restrictive. Therefore, the provision of training and skills development programs should also include peer mentoring sections, in order to increase competitiveness and increase integration capacity.

4. Conclusions

From the above, it can be inferred that the front line is quite diffuse, given that the conflicts are deepening more and more and the confrontations in the virtual

universe produce effects in real space. There is a state of uncertainty worldwide. The statements are followed by sanctions that attract reactions. Economic alliances fall apart, old collaborators become enemies and state satellites reposition themselves. We are witnessing an accelerated cyber arms race. Defense systems are adapting to new threats. Security architectures are being reviewed and rebuilt. The civilian and military sectors have to face new emerging challenges, and this is impossible without a proper security culture. The quality index can be ensured only by implementing educational policies addressed to all social categories.

Bibliography

[1] Adrian Liviu Arsene, Bogdan Rusu, *Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia,* Whitepaper, Bitdefender, 21.05.2020, [Online]. Available at https://www.bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf.

[2] Andrew Heinzman, *What is RAT Malware, and Why Is It So Dangerous?*, How-To-Geek, LifeSavvy Media, 22.04.2019, [Online]. Available at https://www.howtogeek.com/410634/what-is-rat-malware-and-why-is-it-so-dangerous/.

[3] Brian Krebs, *Owners of DDoS-for-Hire Service vDOS Get 6 Months Community Service*, Krebs on Security, 20.06.2020, [Online]. Available at https://krebsonsecurity.com/2020/06/owners-of-ddos-for-hire-service-vdos-get-6-months-community-service/.

[4] Broadcom, *Sophisticated Espionage Group Turns Attention to Telecom Providers in South Asia,* Threat Intelligence, Symantec Enterprise Blogs, 19.05.2020, [Online]. Available at https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/greenbug-espionage-telco-south-asia.

[5] Check Point Research, *Naikon APT – Cyber Espionage Reloaded*, Report, Check Point Software Technologies LTD, May 7th, 2020, [Online].

Available at https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/.

[6] Cisomag, *Japan Confirms Defense Data Breach After Cyberattack on Mitsubishi Electric*, Threats, 12.02.2020, [Online]. Available at https://cisomag.eccouncil.org/japan-confirms-defense-data-breach-after-cyber attack-on-mitsubishi-electric/.

[7] Cyberint, *Targeted Ransomware Attacks in Taiwan*, Cyberint Research, 14.05.2020, [Online]. Available at https://blog.cyberint.com/targeted-ransomware-attacks-in-taiwan.

[8] Dan Raywood, *Global DDoS Attack Dismissed as T-Mobile Misconfiguration*, Infosecurity Magazine, 16.06.2020, [Online]. Available at https://www.infosecurity-magazine.com/news/global-ddos-tmobile/?utm_medium=email&_hsmi=89609585&_hsenc=p2ANqtz-8EBpOhN0Bb5raXKtQaPBcNlhLox-0PY34FIdOq3FmL3myBA-vpVtEsQ_N9hVf99kmzum4O_0l08mvmwhKnl0frsDwjZg&utm_content=89609585&utm_source=hs_email.

[9] Deutsche Welle, *Israel thwarted attack on water systems: cyber chief*, Top Stories, 28.05.2020, [Online]. Available at https://www.dw.com/en/israel-thwarted-attack-on-water-systems-cyber-chief/a-53596796.

[10] European Union Agency for Network and Information Security (ENISA), *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, ISBN: 978-92-9204-267-7, DOI: 10.2824/324042, December 2018.

[11] FireEye, *Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage*, Threat Report, 22.04.2020, [Online]. Available at https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html.

[12] James Lyons, *MD5 Hash*, Practical Cryptography, [Online]. Available at http://practicalcryptography.com/hashes/md5-hash/.

[13] Joby Warrick, Ellen Nakashima, *Officials: Israel linked to a disruptive cyberattack on Iranian port facility*, National Security, The Washington Post, 19.05.2020, [Online]. Available at https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

[14] Kurt Baumgartner, Maxim Golovkin, *The MsnMM Campaigns*, *The Earliest Naikon APT Campaigns*, Kaspersky Lab, May 2015, [Online]. Available at https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf.

[15] Larry Johnson, *Crime-as-a-Service Could Be the Next Big Threat to Your Business*, Cybersecurity, Entrepreneur Europe, 06.09.2017, [Online]. Available at https://www.entrepreneur.com/article/298727.

[16] Liam Tung, *EasyJet hack: 9 million customers hit and 2,000 credit cards exposed*, ZDNet, CBS Interactive, 19.05.2020, [Online]. Available at https://www.zdnet.com/article/easyjet-hack-9-million-customers-hit-and-2000-credit-cards-exposed/.

[17] Michael Herzog, *Israel's 2007 Strike on Syrian Nuclear Reactor: Lessons Learned for Iran*, The Washington Institute, 25.04.2018, [Online]. Available at https://www.washingtoninstitute.org/policy-analysis/view/israels-2007-strike-on-syrian-nuclear-reactor-lessons-learned-for-iran.

[18] Microsoft, *Create or Delete a Rich Text Field*, [Online].Available at https://support.microsoft.com/ro-ro/office/crearea-sau-%C8%99tergerea-unui-c%C3%A2mp-rich-text-9f86237d-dbbc-4a85-b12c-9d8dca824630.

[19] Naveen Goud, *Cyber Attack on Mitsubishi Electric and China held as a suspect*, Cybersecurity Insiders, [Online]. Available at https://www.cybersecurity-insiders.com/cyber-attack-on-mitsubishi-electric-and-china-held-as-a-suspect/.

[20] Norfund, *Norfund has been exposed to a serious case of fraud*, Press release, 13.05.2020, https://www.norfund.no/norfund-has-been-exposed-to-a-serious-case-of-fraud/.

[21] Palo Alto Networks, *Command-and-Control Explained*, Threats, Cyberpedia, [Online]. Available at https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained.

[22] Pierluigi Paganini, *Maze ransomware operators stole data from US military contractor Westech*, Security Affairs, 06.06.2020, [Online]. Available at https://securityaffairs.co/wordpress/104387/cyber-crime/maze-ransomware-hacked-westech.html.

[23] Romanian Presidency, *National Strategy for the Defense of the Country for the period 2020 - 2024*, Non-Secret Document addressed to the President of the Chamber of Deputies, Bucharest, June 2, 2020, Nr. DSN 395.

[24] Reuters, *Denmark wants 5G suppliers from closely allied countries, says defence minister*, Technology News, 08.06.2020, [Online]. Available at https://www.reuters.com/article/us-telecoms-5g-denmark/denmark-wants-5g-suppliers-from-closely-allied-countries-says-defence-minister-idUSKBN23F1IT?utm_source=CSIS+All&utm_campaign=dce2ba4551-EMAIL_CAMPAIGN_2018_11_08_05_05_COPY_01&utm_medium=email&utm_term=0_f326fc46b6-dce2ba4551-222630497.

[25] Rintaro Koike, Shota Nakajima, *An Overhead View of the Royal Road*, Report, nao_sec, 29.01.2020, [Online]. Available at https://raw.githubusercontent.com/nao-sec/materials/master/JSAC%2BCPRCon2020/An_Overhead_View_of_the_Royal_Road.pdf.

[26] Sergiu Gatlan, *US aerospace services provider breached by Maze Ransomware*, Bleeping Computer, 05.06.2020, [Online]. Available at https://www.bleepingcomputer.com/news/security/us-aerospace-services-provider-breached-by-maze-ransomware/.

[27] Romanian Intelligence Service, *APT - The perfectly hidden aggressor*, Cyber Focus, Intelligence Magazine, 29.12.2017, [Online]. Available at https://intelligence.sri.ro/apt-agresorul-perfect-tainuit/.

[28] The White House, *Executive Order on America's Cybersecurity Workforce*, Executive Orders, 02.05.2019, [Online]. Available at https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/.

[29] William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte, *National Initiative for Cybersecurity Education (NICE), Cybersecurity Workforce Framework*, National Institute of Standards and Technology Special Publication 800-181, U.S. Department of Commerce, August 2017, https://doi.org/10.6028/NIST.SP.800-181.

Online Child Sexual Abuse During COVID-19 Pandemic. The Importance of Law Enforcement Training in this Area

Iulian-Marius COMAN
Training Officer - SNE, European Agency for Law Enforcement Training
iulian.coman@cepol.europa.eu

Abstract: Impact of COVID-19 on law enforcement might be early to assess before the pandemic is over, but crime patterns have changed in all criminal areas. Huge amount of people are working from home now, far from the comfort of up-to-date security systems. Cybercriminals around the world undoubtedly are taking advantage on this world crisis. Besides home office, also home schooling has been implemented step by step, having children more and more often available in the online environment.

Keywords: *CSAM, pandemic, law enforcement, cybercriminals, security risks, social media.*

Foreword

Our society evolves and we are facing a digital transformation, that in one hand plays a positive key-role in our life cycle, offering innovative and effective solutions for both private and public sector, but in the other hand, accelerates online criminal activity.

The COVID-19 outbreak has been declared a pandemic in 11 March 2020, by the World Health Organization, having countries already struggling with lack of capacity, resources and resolve[1].Many organizations had to face significant challenges

[1] https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

to which they needed to respond fast, starting from the ways of working and continuing with financial and operational challenges.

At the law enforcement level, the pandemic significantly affected the operational overview, having the police and as first responders for medical emergencies and social distancing management, as well as continuing the safety assurance for the population against crime threats.

An INTERPOL assessment of the impact of COVID-19 on cybercrime, related that the major corporations, governments and critical infrastructure, were significant targeted, shifting the crime pattern from individuals and small businesses[2].

Law enforcement still needs to rely on expertise to draw up the developments of the existing and upcoming security threats and building an effective response to this impact. In this time, more than ever, international policing needs to work with the increased connection from both the physical and virtual worlds[3].

In this article, I will draw an overview of the impact that COVID-19 has on cybercrime, specifically targeting online child sexual abuse[4], in which way the law enforcement organizations are prepared to prevent and combat and what will be the future development of training the policing system.

Operational impact

Social media has become an essential aspect, for the public, governments and the private sector, when social distancing and restrictions are in place, shifting the work and education in online environment.

The threat that we are facing I that a major increase has been reported in the online crime area, among which, online sexual exploitation, with the amount of online child sexual abuse material continuing to raise.

Further on, COVID-19 had a negative impact on the operational level of the law enforcement authorities. Investigators faced the impossibility to hold residential meetings, judiciary activity, such as interviews, becoming harder and harder, and some

[2] INTERPOL- COVID-19 Cybercrime Analysis Report- August 2020
[3] EUROPOL – Beyond the pandemic – 30 April 2020
[4] Europol encourages you to use the term ‘child (sexual) abuse material’ and not ‘child pornography’

of the officials where reassigned to COVID-19 social distancing keeping measures. Nevertheless, law enforcement had to adapt in order to face this new crisis.

During a crisis, such as pandemic, law enforcement officials have a crucial role to provide necessary public services and maintain public order[5]. Although each public health emergency is unique with its own challenges, in all incidents, law enforcement responses must be coordinated with public health, medical, and other essential service authorities[6].

A case[7] related by EUROPOL, show a good example of cooperation, even in this pandemic situation. The international police cooperation lead to the arrest of a Darkweb child sex abuser in Spain[8]. The information was sent by Australian police to Europol, showing a suspect abusing an under five years old boy from Spain. By using the operational analysis and cross-checking information, Europol found that the suspect was registered on Darkweb, on websites targeting child sexual abuse and exploitation. The abuser was located in Barcelona via the cybercrime experts from the Spanish Police and they had to be assisted by their cybercrime colleagues, from Madrid, online, due to lockdown in Spain.

Once again, international police cooperation, even in Crisis times, shows a priority of the law enforcement from all over the world, for child protection[9] and the capacity of adapting of the law enforcement institutions.

COVID-19 demonstrates criminal ad hocery. This crisis shows and increased online distribution of CSAM, as stated by IOCTA 2020. EU Members States have reported an increase in detected CSAM activity on P2P networks. One of the reasons of the raising reports may be that, during the COVID-19 lockdowns, children spent more time in the online environment, sharing photos and videos that end up at CSE offenders.

[5] Richards, E. P., Rathbun, K. C., Brito, C. S., & Luna, A. (2006). *The role of law enforcement in public health emer gencies: A special considerations for an all-hazards approach*. US Department of Justice: Bureau of Justice Assistance
[6] Richards, E. P., Rathbun, K. C., Brito, C. S., & Luna, A. (2006). *The role of law enforcement in public health emer gencies: A special considerations for an all-hazards approach*. US Department of Justice: Bureau of Justice Assistance. https://www.ncjrs.gov/pdffiles1/bja/214333.pdf
[7] https://www.europol.europa.eu/newsroom/news/international-police-cooperation-leads-to-arrest-of-dark-web-child-sex-abuser-in-spain
[8] IOCTA – Internet Organised crime threat Assessment – Europol 2020
[9] Fernando Ruiz, Head of the European Cybercrime Centre at Europol

Several social media platforms, including Facebook, have reported an important amount of CSAM, the platform stating that the end-to-end encryption, as already used in WhatsApp, will improve user privacy. Although, it can be useful tools, the fear behind this is that law enforcement may face insatiable abuse, the end-to-end encryption allowing no one from the sender and recipient to read or modify messages sent through a platform.

UNICEF estimates that one in three internet users is a child[10] and social media/communications platforms remain the most common methods for meeting children online. In 2019, Facebook was responsible for 94% of the 69 million CSAM reported by US technology companies[11].

In fight against online sexual abuse, Facebook joined Google, Microsoft and other 15 tech companies in formation of Project Protect: A plan to combat online sexual abuse, cooperating with governments, law enforcement, civil society, research center and those directly supporting children and families[12].

Law enforcement training

On 3rd of July 2020, CEPOL has published a report on the impact of COVID-19 on law enforcement training needs. This report aimed to identify the needs in law enforcement training, as a result in the changes in crime patters in COVID-19 outbreak.

One of the EMPACT areas that was analyzed is cybercrime and data was gathered from EU Member States, EU agencies, the European Commission, the European Council, non-EU countries and international organizations[13].

The responders indicated that training needs are necessary during the pandemic, for child sexual exploitation field, in prevention and awareness purposes for young people, cooperation with specialized non-LEA, investigation on dark web and tools and methods of investigation/OSINT[14].

[10] Children in a Digital World – UNICEF Report 2017
[11] https://news.sky.com/story/facebook-responsible-for-94-of-69-million-child-sex-abuse-images-reported-by-us-tech-firms-12101357
[12] https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/
[13] https://www.cepol.europa.eu/media/news/cepol-issues-fast-track-needs-analysis-impact-covid-19-law-enforcement-training
[14] CEPOL – Impact of COVID-19 on law enforcement operations and training needs

CEPOL already took attitude about the training during the pandemic, and COVID related webinars were implemented (e.g. COVID-19 Webinar No2 – Abuse of Zoom and other interactive apps during COVID-19 pandemic as gateway for child sexual exploitation)[15], in order to help LE officials to surpass the current crisis.

At European level, CEPOL provides training in cybercrime, via the Cybercrime Academy, but is this enough in this changing times? Residential activities had to be converted into online courses, due to travel restrictions[16]. We can see the advantage of more officials joining the training activities, but also the social cooperation will be limited, and share of experiences will not be the same.

Conclusions

Jurgen Stock, the INTERPOL Secretary General, stated about the report on impact of COVID-19 on child sexual abuse that: We are seeing just the tip of a growing iceberg in terms of online child exploitation material. And for sure that this threat is just a sample that will continue to grow in the unseen world of online.

We can come at the conclusion that the raise of CSAM threat requires continued close monitoring and prevention measures should be implemented to protect children online[17]. Nevertheless, the cooperation between LE agencies and further on with public sector, will remain a key requirement, as criminals use a shared infrastructure that requires the engagement of multiple levels of collaboration[18]. The pandemic is not over and also the commitment of every law enforcement official.

References

[1] DBBC News, "NSPCC urges Facebook to stop encryption plans", https://www.bbc.com/news/technology-51391301, 2020 and Musil, Steven, "Facebook urged to halt encryption push over child abuse concerns".

[15] https://www.cepol.europa.eu/education-training/what-we-teach/webinars/covid-19-webinar-no2-interactive-apps-cse
[16] https://www.cepol.europa.eu/media/news/further-suspension-onsite-training-activities-hungary-until-end-june-2021
[17] Europol – beyond the pandemic – April 2020
[18] EUROPOL IOCTA 2020

[2] Europol, "Partners & Agreements – Police2Peer: Targeting file sharing of child sexual abuse material", https://www.europol.europa.eu/partners-agreements/police2peer, 2020.

[3] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2018.

[4] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020.

[5] https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020.

[6] INTERPOL- COVID-19 Cybercrime Analysis Report - August 2020.

[7] EUROPOL – Beyond the pandemic – 30 April 2020.

[8] Europol encourages you to use the term 'child (sexual) abuse material' and not 'child pornography'.

[9] Richards, E. P., Rathbun, K. C., Brito, C. S., & Luna, A. (2006). *The role of law enforcement in public health emergencies: A special considerations for an all-hazards approach*. US Department of Justice: Bureau of Justice Assistance.

[10] https://www.europol.europa.eu/newsroom/news/international-police-cooperation-leads-to-arrest-of-dark-web-child-sex-abuser-in-spain.

[11] Children in a Digital World – UNICEF Report 2017.

[12] https://news.sky.com/story/facebook-responsible-for-94-of-69-million-child-sex-abuse-images-reported-by-us-tech-firms-12101357.

[13] https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/.

[14] https://www.cepol.europa.eu/media/news/cepol-issues-fast-track-needs-analysis-impact-covid-19-law-enforcement-training.

[15] CEPOL – Impact of COVID-19 on law enforcement operations and training needs.

[16] https://www.cepol.europa.eu/education-training/what-we-teach/webinars/covid-19-webinar-no2-interactive-apps-cse.

[17] https://www.cepol.europa.eu/media/news/further-suspension-onsite-training-activities-hungary-until-end-june-2021.

Education for a Digital World. Case Study: School Education to Combat Online Misinformation[1]

Handy-Francine JAOMIASA
Doctoral School of the Faculty of Journalism and Communication Sciences,
University of Bucharest, Romania
jean_francine@yahoo.com

The educational act is currently in the process of reorganization as a result of the transition to a digital world. This process, accelerated by the COVID-19 pandemic, has given rise to various social developments, whether positive or negative. A major risk currently observed refers to the impact of the online environment on young people but not only. The influence of a digital environment in which social networks seem to have taken the place of traditional sources of information, verified by specialists (written press with articles written by professional journalists who check the facts, etc.) has led to an avalanche of information difficult to control.

Context elements on the importance of digital education and combating online misinformation

In this context, the importance of digital literacy and education is becoming paramount. To understand their importance, it is essential to try to provide a clear definition of the main concepts as they reflect in the dedicated literature and not only.

Digital education is currently a priority at the European level and the subject of a *Digital Education Action Plan (2018-2020)* by the European Commission [1]. Ignoring the references to the importance of education and training, what we have identified as relevant to the topic is: "Digital technology enriches learning in a variety of ways and offers learning opportunities, which must be accessible to all." [2].

[1] The opinions expressed are those of the author only and should not be considered as representative of the Doctoral School of the Faculty of Journalism and Communication Studies, University of Bucharest official position. This article is an ongoing research and does not in any way engage the responsibility of the Doctoral School of the Faculty of Journalism and Communication Studies, University of Bucharest.

Although access to digital technologies can support the educational process, reduce gaps and increase the autonomy of young people, acknowledging the risks is also important. I will not refer here to the technological or educational gaps, but to the risks caused by misinformation in the online environment. Thus, an identified problem that is now becoming even more pressing is that of fake news.

"Algorithms used by social media sites and news portals can be powerful amplifiers of bias or fake news, while data privacy has become a key concern in the digital society. Young people as well as adults are vulnerable to cyber bullying and harassment, predatory behavior or disturbing online content." [3].

The issue of misinformation is also a topic of interest on the European agenda, being intensely debated especially since 2018. A working definition used at the European level is as follows: "Disinformation is understood as verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security. Disinformation does not include reporting errors, satire and parody, or clearly identified partisan news and commentary." [4].

It is worth mentioning in this regard the Eurobarometer on Fake News and Online Misinformation issued in February 2018 which shows that **respondents are less likely to trust news and information from online sources than from more traditional sources and that they have encountered fake news at least once a week. A large majority of respondents think that the existence of fake news is a problem in their country and for democracy in general** [my emphasis]. Also, the responsibility for stopping the spread of fake news lies with journalists (45%) followed by national authorities (39%), the management of the press and communications (36%), and the citizens themselves (32%) [5].

The situation is currently exacerbated by the COVID-19 pandemic, accompanied by a veritable disinformation infodemic, which affects the Member States and European citizens in different ways. This is highlighted by the multitude of concerns

at the national and European level, all the more so since Internet use is a key condition for the success of combating the pandemic and maintaining social distance.

"It is important to note that the term 'social distancing' focuses on reducing physical contact as a means of interrupting transmission, but while reduction of social contact may be an outcome of that, it is not a specific aim. Indeed, the success of social distancing measures that are implemented over an extended period may depend on ensuring that people maintain social contact – from a distance – with friends, family and colleagues. **Internet-based communications are therefore a key tool for ensuring a successful social distancing strategy** [emphasis added]." [6].

The focus on combating fake news through education thus becomes a priority. We have a series of institutional references on this subject, meant to be at the forefront of the educational agenda at the European and national level:

"We need to strengthen children's and young people's **critical thinking and media literacy**, so they can judge and overcome the ever-present threats of fake news, cyber bullying, radicalisation, cybersecurity threats and fraud" [7].

Legislative concerns have also arisen at **the national level** to regulate and introduce education to combat disinformation in schools. The Romanian Parliament has the *Draft Law for the introduction of the discipline "Education and media culture" in secondary education, PL-x no. 326/2019* which states that "the subjects proposed by this law will include the teaching of communication theories, the formation of a critical and analytical mechanism for receiving news, identifying information manipulation for the benefit of extremist or anti-democratic interests, filtering information that has as the ultimate goal of restricting and threatening fundamental rights, identifying fake news" [8].

How can the fight against misinformation be taught in schools? Case study

This brings us to the way the fight against online disinformation, but also other aspects, such as cybersecurity, in the context of the digitalization of education, can be taught.

A good example is the introduction of *News Literacy Module* in a *Learning Management System – LMS* course [9]. The module aimed to provide students with a series of three key skills, namely:

- understanding the information cycle: to allow students to recognize an information need, give examples of sources available, and contrast scholarly and popular sources;
- locating news sources: to give students the chance to select appropriate search tools for a given information need, develop topic-relevant vocabulary in order to search databases and
- evaluating news articles: to provide students the tools to critically assess a source prior to use [10].

Following the implementation of this pilot program, one of the conclusions was the need for practical exercises, and students had to interact with the sources to then reflect on their safety or unsafety [11].

Another initiative aimed at young people in the United States also benefits from the support of large companies such as Google. It is worth mentioning the MediaWise project initiated and carried out by the Poynter organization, which aims to teach adolescents how to identify suspicious sources, use information checking tools, etc. [12].

Among the objectives of the project addressed to young people are: the creation of a Curriculum available free of charge for secondary and high school education; courses in physical and virtual format; creating a fact-finding network animated by teenagers, respectively using ambassadors (journalists and influencers) to promote these things [13].

A similar program for primary school pupils is carried out in the UK by *The Guardian Foundation*. This program places special emphasis on the use of tests such as True or False?, the use of age-appropriate images by which children play and become detectives meant to identify fake news and learn to ask the much-needed critical questions, etc. [14].

Instead of conclusions

This work did not aim to provide an exhaustive overview of the legislative framework or national initiatives in the field of digital education but wants to create the "yard" for a future analysis dedicated to addressing disinformation and other dangers in the digital world of the future.

The preliminary conclusion of the above ideas is that the importance of critical thinking and the need for digital literacy at any age should not be underestimated. Although it may be "easier" for teachers to develop such modules for students, for example, the efficiency of this process is enhanced by starting at an early stage. It is necessary to create educational programs for both media and cybersecurity from an early age, possibly in primary school, as the age at which children are exposed to the digital world decreases dramatically.

Not educating children about the responsible use of new technologies means limiting their opportunities and putting them at risk. But together, parents and school can reduce these risks and shape the responsible citizens of tomorrow's digital world.

References

[1] The European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Digital Education Action Plan* {SWD(2018)12final}[Online] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0022&qid=1616589531878&from=EN [Accessed on November 12th, 2020].

[2] The European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Digital Education Action Plan* {SWD(2018)12final}, p. 1, [Online] Available at https://eur-lex.europa.eu

/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0022&qid=1616589531878&from=EN [Accessed on November 12th, 2020].

[3] The European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Digital Education Action Plan* {SWD(2018)12final}, p. 3, [Online] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0022&qid=1616589531878&from=EN [Accessed on November 12th, 2020].

[4] The European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling online disinformation: a European Approach* COM/2018/236 final, p. 4, [Online] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236&qid=1616590432172 [Accessed on November 12th, 2020].

[5] Eurobarometer, *Fake News and Disinformation Online*, March 2018, [Online] Available at https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183 [Accessed on November 12th, 2020].

[6] European Centre for Disease Prevention and Control, *Considerations relating to social distancing measures in response to COVID-19 – second update*. Stockholm: ECDC; 2020, [Online] Available at https://www.ecdc.europa.eu/sites/default/files/documents/covid-19-social-distancing-measuresg-guide-second-update.pdf [Accessed on November 12th, 2020].

[7] The European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL,*

THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Digital Education Action Plan {SWD(2018)12final}, p. 9, [Online] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC 0022&qid=1616589531878&from=EN [Accessed on November 12th, 2020].

[8] Parliament of Romania, *PL-x no. 326/2019 Draft Law for the introduction of the discipline "Education and media culture" in pre-university education*, [Online] Available at http://cdep.ro/pls/proiecte/upl_pck2015.proiect?cam=2&idp=17947 [Accessed on November 12th, 2020].

[9] Kendra Auberry, *Increasing students' ability to identify fake news through information literacy education and content management systems*, The Reference Librarian, 59:4, 179-187, 2018 [Online] Available at DOI: 10.1080/02763877.2018.1489935 [Accessed on November 12th, 2020].

[10] Kendra Auberry, *Increasing students' ability to identify fake news through information literacy education and content management systems*, The Reference Librarian, 59:4, 179-187, p. 6, 2018 [Online] Available at DOI: 10.1080/02763877.2018.1489935 [Accessed on November 12th, 2020].

[11] Kendra Auberry, *Increasing students' ability to identify fake news through information literacy education and content management systems*, The Reference Librarian, 59:4, 179-187, p. 8, 2018 [Online] Available at DOI: 10.1080/02763877.2018.1489935 [Accessed on November 12th, 2020].

[12] Kerry Flynn, How Google-backed MediaWise is teaching teens media literacy, *Digiday*, January 7th, 2019, [Online] Available at https://digiday.com/media/google-backed-mediawise-teaching-teens-media-literacy/ [Accessed on November 12th, 2020].

[13] Poynter, *MediaWise for Gen Z*, 2020, [Online] Available at https://www.poynter.org/mediawise-for-gen-z/ [Accessed on November 12th, 2020].

[14] Elli Narewska, Critical literacy in a digital world, *The Guardian*, November 2nd, 2020, [Online] Available at https://www.theguardian.com/newswise/2020/nov/02/critical-literacy-in-a-digital-world [Accessed on November 12th, 2020].

In Search of Lost Cyber Talents

Liviu MORON
Cybersecurity Advisor, European Exchanges Development Agency (ADeSE) - Cybershare, Romania
liviumoron@hotmail.com

1. Cybersecurity skill gap

The cybersecurity skill gap is a well-known problem, there are a lot of studies about this subject.

Even if the problem was identified and some efforts were done to solve it, there is no major improvement in this area and companies are still worried about the Cybersecurity talent shortage.

In this paper we are trying to identify some actions that we have to take in order to fill the cybersecurity skill gap.

2. Identifying new sources for cyber talents

In 2018 the Cyberthreat Defense Report[1] showed that 8 companies out of 10 are impacted by a security talent shortfall.

In 2020 the skill gap in cybersecurity is still present, 70% of ISSA members believe their organization has been impacted by the global cybersecurity skills shortage[2].

There is a need for more talents in this domain, but what actions should we take into account to help companies to find more specialists?

We identified 2 actions that can help to fill this gap:

- supporting the participation of women in the field of cybersecurity.
- educate schools students in cybersecurity.

[1] CyberEdge Group - 2018 Cyberthreat Defense Report, https://cyber-edge.com/wp-content/uploads/2018/03/Cyber Edge-2018-CDR.pdf
[2] Jon Oltsik: The Life and Times of Cybersecurity Professionals 2020, https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf

2.1. Women in Cybersecurity

One direction to follow to bring more talents in this field, could be to support the participation of women in Cybersecurity. The (ISC)² Cybersecurity Workforce Study - Women in Cybersecurity[3] revealed that the percentage of women in cybersecurity is roughly 24%. There is certainly room for improvement and we identified some actors that have already started initiatives to bring more women in cybersecurity.

2.1.1. Women4Cyber

Women4Cyber[4] is an initiative supported by ECSO that "aims to help fill the gender gap of cybersecurity professionals in Europe". The main goal is "to encourage and promote the skilling, up-skilling, and re-skilling of girls and women towards cyber-security education and professions. There are 6 workstreams in the agenda:

1. Create awareness, promote best practices and visible Role Models.
2. Promote tailored training programmes in cybersecurity.
3. Enhance the presence of women on the cybersecurity job market.
4. Increase the presence of women in cybersecurity Research & Innovation (R&I) and in the field of emerging technologies.
5. Support and shape policies at EU and national levels that are in line with Women4Cyber's messages.
6. Establish and coordinate international and national partnerships.

2.1.2. SHe CISO Exec

The SHe CISO Exec[5] initiative focuses on bridging the skill and diversity gap in the cybersecurity industry to create better emotionally intelligent leaders. The objectives are:

1. Empowerment: Create a talent pool of emotionally intelligent cybersecurity community.

[3] (ISC)² Cybersecurity Workforce Study: Women in Cybersecurity, https://www.isc2.org/Research/Women-in-Cyber security
[4] Women4Cyber, https://women4cyber.eu/
[5] SHe CISO Exec, https://www.shecisoexec.org/

2. Mentoring & Networking: Foster a community for knowledge-sharing, collaboration, mentorship and networking.

3. Leadership: Empower and encourage thought leaders in the information security industry.

2.1.3. Cybershare Women in Cyber

This is an initiative of the ADeSE NGO that wants to support women that want to start a career in cyberscurity. It targets the Romanian IT community and the objectives are:

- Promote tailored training programmes in cybersecurity
- Mentoring & Networking

There were 2 community meetings for Women in Cyber in 2019 and 2020 at the Cybershare Conference[6]. On the 30.10.2020 in the second meeting, the community decided to organize a Working Group to decide on the future actions. If you are interested in supporting women that want to start a career in cybersecurity you can contact the working group at adese.eu@gmail.com.

2.2. Cybersecurity for school students

There is no age limit for children to discover Cybersecurity. Sooner they discover it, better understanding of how to avoid cyber-attacks they can have. There are several initatives for teaching cybersecurity to school students.

2.2.1. Cybershare Academy for Schools

Cybershare Academy for Schools is an initative from Romania where Cybersecurity is not studied in schools ADeSE NGO decided to start the Cybershare Academy for Schools initative together with the Romanian National Center Cyberint, CERT RO, Silensec, ISJ Iasi and 4 school parteners. The event offers to school students 1 week of free training on a Cyber Ranges platform, Cybersecurity Workshops and a CTF to test the knowledge that the school students acquired during this week. The first

[6] Cybershare Women in Cyber, https://www.cybershareconference.com/

edition of the event started in 2020 and it is planned as a recurrent event to take place one or more times a year.

2.2.2. CyberFirst

CyberFirst is an initiative from UK and covers a broad range of activities: a comprehensive bursary scheme to financially support undergraduates through university and a degree apprenticeship scheme, a girls' only competition.

3. Conclusions and recommendations

What recommendations are there to fill the cybersecurity skills gap? Encouraging more women to come in Cybersecurity could be one way to fill the skill gap. To achieve this objective, some activities are proposed:

- Organize events where women can share their experience in Cybersecurity.
- Deliver trainings for women.
- Organize mentoring sessions.
- Support women that want to start a business in cybersecurity.
- Organize cybersecurity competitions for women.

The second action that we identified that can help to fill the skill gap is to teach school students cybersecurity. To achieve this objective some activities are proposed:

- Organize events where cyber professionals can talk to school students about their experience in Cybersecurity.
- Deliver trainings for school students.
- Organize mentoring sessions.
- Support school students that want to start a business in cybersecurity.
- Organize competitions for school students.

To fill the cybersecurity skill gap ADeSE NGO have already started activities like Cybershare Academy for Schools and Cybershare Women in Cyber. Companies should support the process of preparing the future cyber talents, in order to be sure that they can easily find talents to hire. Entities that are interested to help in this process of preparing cyber talents are invited to contact us at adese.eu@gmail.com.

The University-Industry CDI Ecosystem - a Key Pillar for Increasing Cyber Competence and Resilience

Olivia COMȘA, Sorin MIRIȚESCU, Marius PÂRVU
Department CDI, Safetech Innovations SA, Romania
olivia.comsa@safetech.ro, sorin.miritescu@safetech.ro, marius.parvu@safetech.ro

Assoc. Prof. Florin POPESCU, PhD
National Defense University, Carol I-UNAP, Romania
Popescu.VFlorin@unap.ro

1. Introduction

The evolution of modern society is unthinkable today without digital development; from easier access to the internet to the digitization of services and industries and the development of complex critical infrastructures, all involve the extensive use of digital services and the internet. In addition to the benefits of rapid access to documents and information, the danger of cyberattacks is also gradually increasing. Cybersecurity is thus at the heart of digital development [1].

And as there are no physical boundaries for the digital world, Romania is also in the position of a local actor of international importance in this process, and **cybersecurity is not only a technological option but a societal need**. Cyber threats are no longer limited to cybercrime but have become a subject of national security. To meet these challenges in the context of the accelerated digitalization of industries and services, it is essential to involve all responsible actors and building a public-private partnership between authorities, research, universities, and the private sector to ensure cybersecurity, increase the resilience of critical infrastructure, promote research, innovation, and technology transfer through the creation of a community and a cybersecurity ecosystem. From the experience of all security companies, also confirmed by the nearly 10-year Safetech experience, **it is the human factor that generates the greatest cybersecurity vulnerabilities**, but also the one that can resolve

them. Unfortunately, the pace of technology evolution is not followed by developments in the education and training system that provide sufficient human resources, niche specializations, and capabilities to enable secure governance of the cyber domain. The announcement of the damage made by various cyberattacks, which not only cause material and/or image damage, but also significant vulnerabilities and security breaches are daily news. **The acute need for specialized staff is felt at all levels**, from small companies to those specialized in such services, to essential service operators, and government institutions. Estimates from responsible agencies and specialized companies indicate a shortage of several million jobs in cybersecurity and growing. The solutions to meet this goal of providing specialized human resources are different from country to country, from institution to institution. All **approaches take into account the involvement of the expertise of all exponents in public and private education and training and the government's decision** to increase professional competence, expertise, and awareness of cybersecurity [2].

This material intends to present the experience of Safetech Innovations SA in ensuring professional competence, strengthening institutional capacity, and developing high-performance solutions and services in partnership with academia and research, as a case study that may be relevant to other companies.

2. Development strategy and institutional capacity building

The EU Cyber Security Strategy sets out plans to address challenges in priority areas such as increasing cyber resilience, drastically reducing cybercrime, developing cyber defense policy and capabilities, developing human, industrial and technological resources for cybersecurity, establishing coherent international cyber policies, and strengthening the response capacity, industrial partnerships and the inclusion of SMEs in cybersecurity programs and projects [3].

Safetech's strategy, keeping the proportions, pursues the same priorities focusing on increasing institutional capacity, adopting innovative technologies, developing high-performance solutions and services through RDI activities carried out in partnership with academia and research, increasing staff performance and competence

through certification, education, and training, establishing long-term partnerships with advanced technology manufacturers, essential service operators, research, E&T in the field of cybersecurity, interoperability and ITC technologies.

The recent listing on the Bucharest Stock Exchange adds to these and it is meant to ensure the capitalization of the company for the implementation of innovative solutions and services projects that will lead to increased competitiveness. Along with the listing at BVB, the priority development of two of the company's major departments, **STI-CERT** and **STI-CDI**, represents the materialization of the institutional development strategy adopted by Safetech.

SAFETECH is one of the first private companies in Romania to set up and own a Cybersecurity Incident Monitoring and Response Center, (type CERT), organized after the model of a Security Operations Center (SOC), and registered under the **STI CERT**. It is represented by a dedicated department within the company, which provides a non-stop system for monitoring, alerting, responding, and managing cyber incidents for public institutions or private companies (24/7). To this is added the **STI-CDI** Research Department, which has developed in the last 5 years numerous research activities and projects in partnership with renowned universities and research centers in the country and abroad.

Since 2015, Safetech has expanded its areas of interest and progressively developed research activities in national and European programs and projects such as PN III, Horizon 2020, ENISA, POC, POCU, SoL, alone or in partnership with prestigious research and university institutions. This has contributed to increasing professional skills, expanding the area of activity, and acquiring extensive capabilities in the field of project management, funding, and administration of research projects. The core team of the company has Brainmap codes and is often required as a partner in innovation, development, and technology transfer projects and good practices [4, 5]. The main certifications of Safetech experts, presented in fig. 1, covers the company's priority areas of action:

Fig. 1. *Professional certificates* (Source: Safetech Innovations SA)

3. Technological development

Today, every company is on a journey in the field of cybersecurity that **requires not only staff with increased skills and knowledge of investigation and monitoring but requires also advanced technologies** to perform rapid analysis followed by the execution of effective actions. Cybersecurity teams need to protect attack areas that are becoming larger and more distributed, mainly due to the growth of remote activities, the development of cloud infrastructures, the proliferation of IoT devices, network services, and other dynamics in social and business environments. Companies understand that to meet these challenges, it is imperative **to incorporate into their security operations program appropriate technologies** that can handle large data sets and the full complexity of cyber threats.

Among the technological priorities for which we develop solutions, the need for automation and services in the field of detection and response to cybersecurity threats is increasingly acute. It is not just a matter of automating the data collection that security teams expect from such solutions, but also of **closer integration with the security tools used in security operations centers (SOC) and more efficient orchestration of triggered workflows**. To ensure the necessary technologies, Safetech has resorted to the development of its own solutions and technologies and technological partnerships with world-renowned technology providers. Safetech's

portfolio includes some of the most famous and innovative security technologies on the market, which allow the technical team to implement advanced solutions to ensure cybersecurity and the resilience of the infrastructures we secure and monitor:

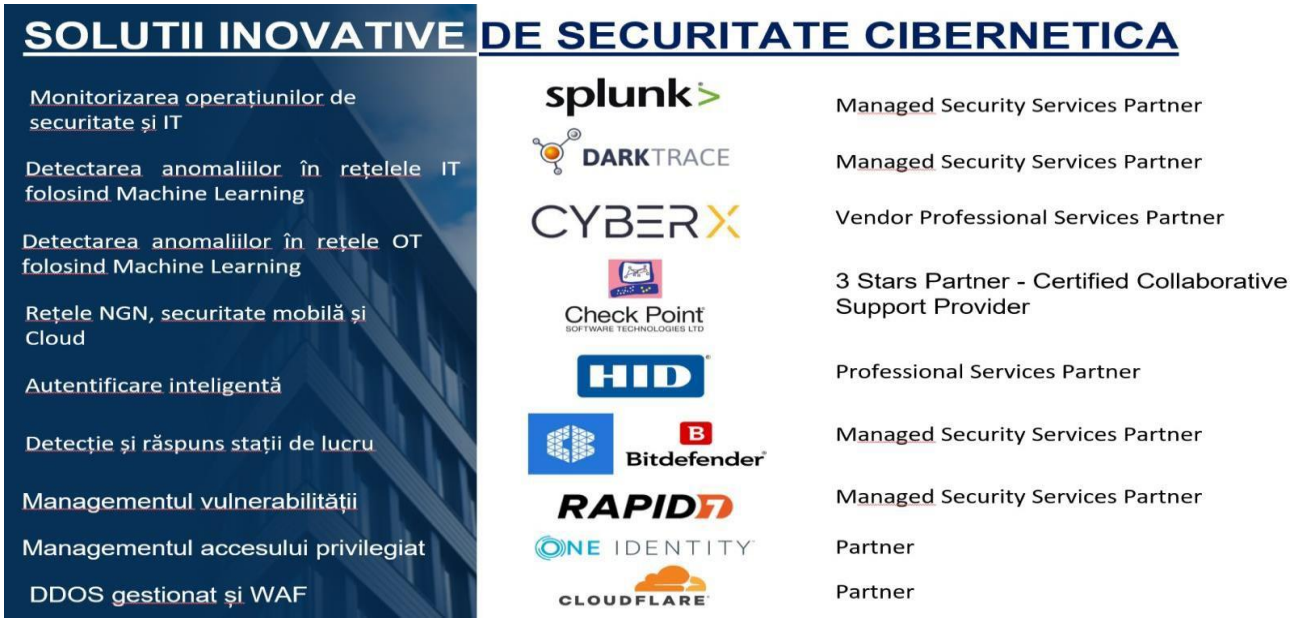


Fig. 2. *Safetech portfolio solutions* (Source: Safetech Innovations SA)

4. Research, Education and Training Partnerships

The technological partnership with developers of top cybersecurity solutions has led to the accumulation of exclusive skills in the company, doubled by obtaining essential certifications for the implementation of high-performance solutions and services. Starting from this technical expertise, with the emergence of the research department we have capitalized on knowledge and practical experience by carrying out numerous proposals for RDI projects in national, European, and international programs in partnership with academia, research, and other private partners. The development of these projects, the collaboration within the high tech clusters, the participation in conferences, seminars, and workshops led to the realization of a permanent partnership and an ecosystem through which both Safetech and partners benefited from complementary knowledge, solutions, and good practices which have increased their individual value. Moreover, senior students from different universities (UPB, UNAP, ASE, UTCB) have done practice/internships at Safetech and in the last 3 years over 10 bachelor's and master's theses have been completed based on topics developed in

collaborative projects. This year, other students are developing bachelor's and dissertation papers in co-tutoring, addressing current topics, with a practical purpose. Many of the undergraduate and master's students were employed in the company after graduation, which was beneficial for both parties. The students from the past years represent the base staff in the technical and research department today, bringing with them both the enthusiasm of the youth, but also the connection with the University from which they come. In this way, we managed not only to increase and provide our own staff but also to maintain a permanent connection with universities and research centers, where we benefit from the theoretical expertise in niche areas that we require when needed. Also, through better knowingness, we understood how important it is for the academic environment to have access to a practice base, for Safetech to have collaborators in cutting-edge fields, and together to address the latest developments in cybersecurity and disruptive technologies. As a corollary, we concluded that it is mandatory to develop cybersecurity labs in partnership. Consequently, we managed to develop cybersecurity laboratories for UNAP, UPB, UCV, virtual labs support for master studies in cybersecurity based on the experience of the first training laboratory [6] CTF (https://ctf.usv.ro/) made with the University of Suceava, ICI, and Assist.

E&T activities have always been included in RDI projects, which we consider necessary both for the project participants and for the beneficiaries of the project results. Projects relevant to the government environment [4, 5] have shown that the partnership with academia and research can contribute to the materialization of major projects that combine complementarity of the expertise of partners, generating added value, an increase in cybersecurity culture, and greater awareness of public opinion.

At the same time, based on the experience gained, Safetech has started to carry out company projects for institutional advancement and the development of its own cybersecurity solutions using European funds. We tried to include under the “SAFE” brand both the technological solutions and the Safetech shares at BVB. The main initiatives and solutions carried out or in progress are presented to illustrate the permanent cooperation with the university environment, research, and other companies.

5. Support for GDPR and NIS implementation

The ongoing concern to have high-performance technologies in the portfolio and the development of its own cybersecurity solutions and services shows how Safetech Innovations SA understands to help prepare the implementation activities of the GDPR and NIS Directive in Romania and to increase the resilience of its customers' infrastructure to cybersecurity incidents. Tight integration of research results with various elements of security infrastructure through flexible interfacing components will allow the continuous addition of new sources and types of data for the development of cyberattack defense strategies, amplifying the agility needed for facing current challenges, mainly to increase the resilience of critical infrastructures.

At the EU level, the main forces driving the ever-growing cybersecurity market are the implementation of the GDPR and NIS as well as the rise of cyber terrorism. The implementation of European requirements has led to an increased awareness of cyber threats and will generate both an increase in demand for cybersecurity products and services and an increase in the need for cybersecurity staff and related fields.

6. "SAFE" by Safetech

We introduce the main products, solutions, and projects developed or initiated by Safetech based on internal qualifications and/or expertise gained in research partnerships in the RDI ecosystem.

1. **CTF - Capture the Flag - "Improving educational processes and activities within the bachelor's and master's degree programs in the field of ICT by creating an information security laboratory" -** partners: USV, SAFETECH, ASSIST, ICI (http://www.posdru-142006.usv.ro/). The long-term positive effect is, at the institutional level, the existence of a material base and human capital formed for the transmission of theoretical and practical knowledge in the field of information security for the next generations of students and masters, as well as the ability to develop a self-

organization information security system and a permanent CTF competition: International Students Contest on Information Security (https://ctf.usv.ro/).

2. **"iSAM" - Integrated information security management system within an organization** (https://www.safetech.ro/simsi/). iSAM is an innovative software platform capable of streamlining activities within a SOC-Security Operations Center (a centralized unit that manages security issues at the organizational and technical level), developed by Safetech in a POC project. Among the benefits provided by iSAM are: Increasing the efficiency of the information security management process; Decreased operating costs; Faster and better-informed decisions; Compliance with various regulations.

3. **"NG-SAFE" - Integrated Platform based on Big Data and AI / ML Technologies, for Advanced Cyber Security Analysis in IT / OT / IoT Infrastructures**. The proposed development by initiating this cybersecurity analysis platform will be able to significantly improve the collection, standardization, aggregation, correlation, and analysis of structured and unstructured data in an organization and the performance of dedicated personnel in the area of detection and response to incidents compared to traditional, time-consuming, work methods, and will contribute to compliance with relevant standards (GDPR / NIS).

4. **"SafePIC" - Center of Excellence for Cybersecurity and Critical Infrastructure Resilience**. This project carried out in partnership with an academic entity (UNAP) and a research entity (IFIN-HH), is the most important initiative underway. Through the implementation of the project, Safetech introduces both a major change in the company's activities, diversification and expansion of Safetech's current capacity to develop innovative solutions and services in the field of IT security, interoperability, and increasing cyber resilience of critical infrastructures and an increase in

TSI-CERT response to cybersecurity attacks and incidents. also, a Cyber Range cyber polygon is being developed at UNAP and a Honeypot laboratory at IFIN-HH.

5. **"SafeCySET" - The Simulation, Certification, and Training Platform** in the field of Cyber Security is a proposal for a Cyber range type IT application, meant to contribute both to increase the capacity and performance of staff to respond to cyber incidents and to increase the resilience of protected networks and infrastructures.

6. **"SafeCyberLab -** The Virtual Cyber Security Laboratory is a prototype developed as a support for master's courses in cybersecurity at UCV, USV, and UNAP. The laboratory integrates innovative solutions such as "*automatic implementation of virtual machine parameters with laboratory activity, based on custom templates adapted at the time of implementation to the user profile/curriculum/topic/activity*" and "*new generations of mixed learning training scenarios, facilitating easier learning by simulating real-life scenarios, mainly ICS-SCADA security*".

7. **SafePIC cyber polygon**

The SafePIC cyber polygon that will operate in the National Defense University, according to fig. 3, is a virtual platform that can be used for the training of specialists or experiments in the field of cybersecurity.

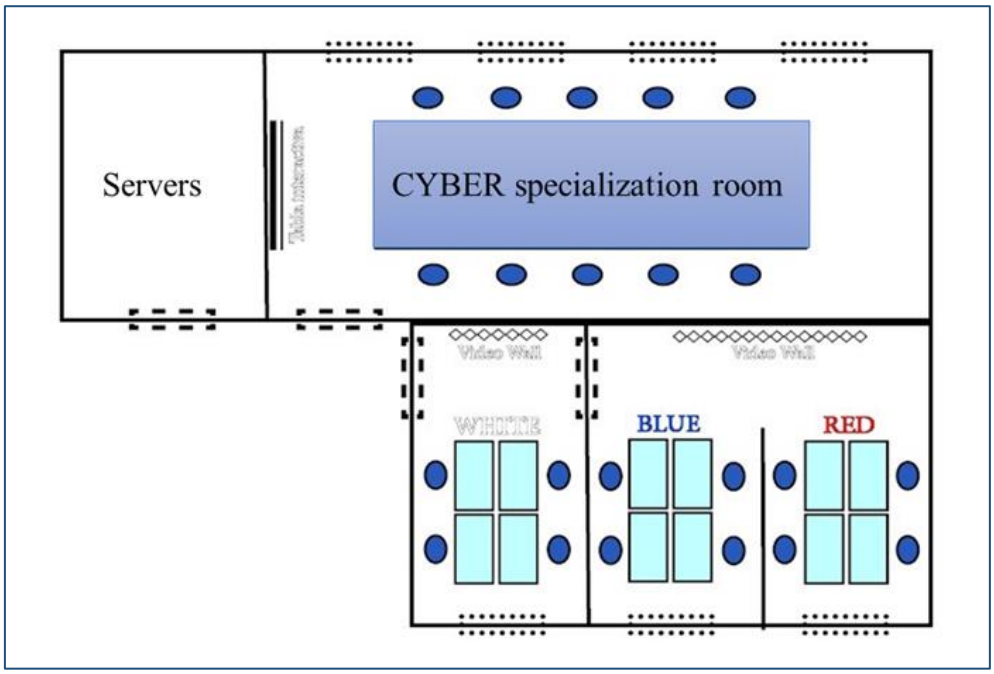


Fig. 3. *Cyber polygon Servers / Cyber specialization lounge*

In this distributed virtual environment that will operate in the National Defense University, based on scenarios, the staff and future master students hosted by the 7 classrooms/specialty lounges, according to fig. 4, will be trained to use cyber defensive or attack tools, tactics, and strategies. This distributed cyber polygon can also be used for the development of new cybersecurity technologies.

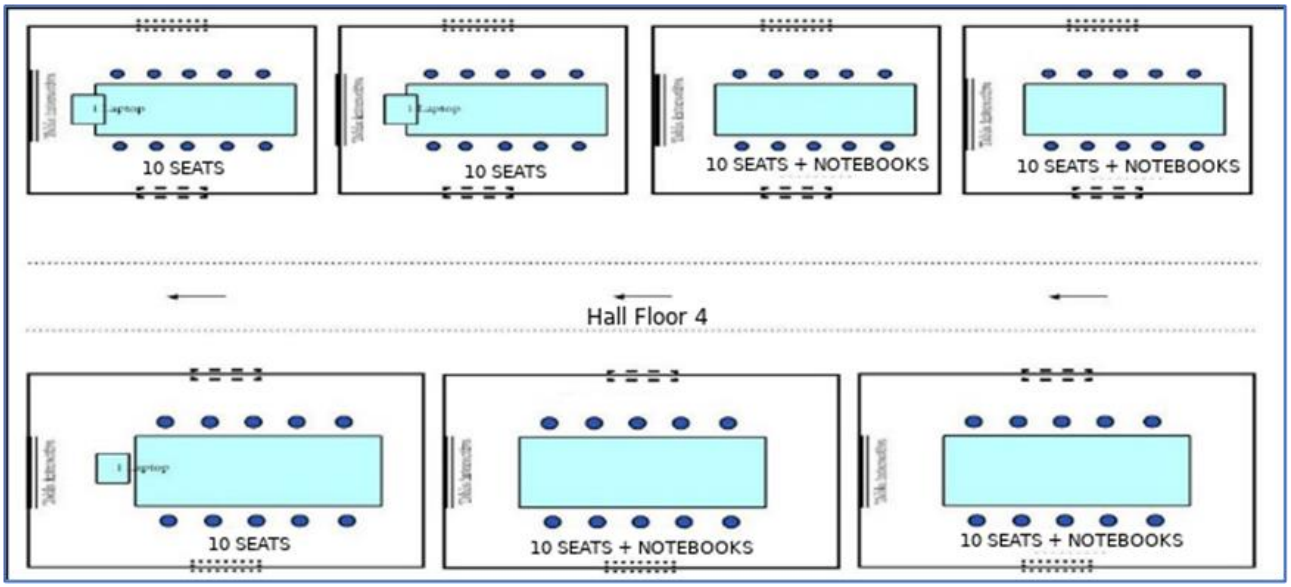


Fig. 4. *Diagram of the 7 specialized lounges in the distributed cyber polygon*

To reduce deployment costs, it is preferred to use virtualization technologies to implement systems or networks. However, this is not always possible, especially when the scenario involves the use of embedded systems or industrial control systems (ICS / SCADA).

To make the most of the existing resources and to benefit from the accumulated expertise, a natural tendency is to interconnect the infrastructures (CYBER Range in fig. 3 with the 7 specialty lounges in fig. 4) to create distributed cyber polygons. The concept of a distributed cyber range, which also involves specialized lounges, is presented schematically in fig. 5.

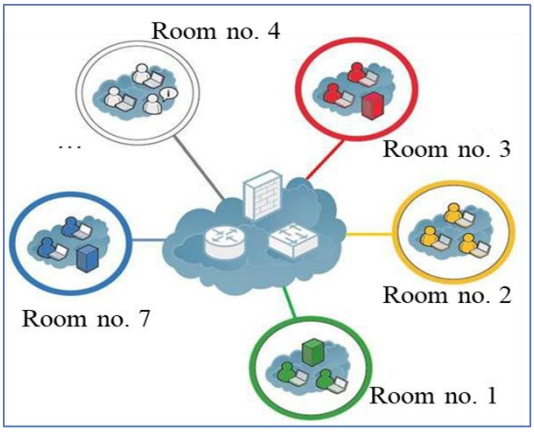


Fig. 5. *Schematic presentation of the distributed cyber polygon Lounge 1 – 7*

The advantages of interconnecting the cyber range platform with the 7 specialty lounges are obvious:

- ✓ Resource sharing - in addition to processing and storage resources, you can share scenarios, educational content (online courses), or specialized equipment (traffic generators, SCADA systems, etc.);
- ✓ Joint organization of exercises - depending on skills, each lounge can play different roles (red team, blue team, white team, etc.);
- ✓ The assessment of developed products and software applications and the security testing of products will be done in a controlled environment that accurately simulates the real environment.

The logical architecture of the cyber range platform proposed to be implemented is shown in fig. 6.

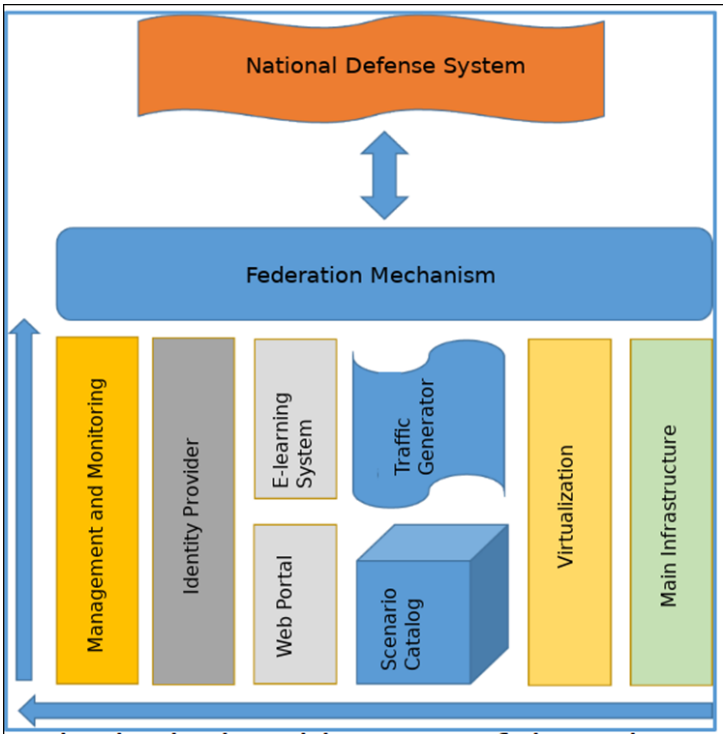


Fig. 6. *The logical architecture of the cyber range platform*

The main components of this infrastructure are:

- ✓ Basic infrastructure - servers, SAN, network equipment (SW, routers), FW, IDS / IPS, specialized equipment (ICS / SCADA);
- ✓ Virtualization/isolation level - creating and running virtual machines and networks;
- ✓ Scenario catalog - description of the platform configuration for different exercises (network defense, penetration testing, digital forensics, etc.);
- ✓ Traffic generator - simulation of standard network activity or attacks of various types (exploits, malware, DoS / DDoS);
- ✓ Frontend (Web Portal) - The web interface employed by users for access;
- ✓ E-Learning System (LMS) - administration system and delivery of learning modules;
- ✓ Management and monitoring tools - administration interfaces for controlling the resources used during an exercise.

The proposed architecture provides the necessary flexibility to organize complex exercises and experiments in the field of cybersecurity. The solution also allows one partner to specialize in a specific field (for example SCADA, mobile devices, IoT), and

the other partners to access the resources developed by that partner. Also, the scenarios and exercises developed by one partner will be able to be ported and used by the other partners to train their own students.

8. Conclusions

The development strategy based on RDI partnerships and the preparation of human resources proved to be a winner for Safetech. This formula may be relevant for other entities with similar activities, in particular in the ICS - SCADA area [7]. Beyond this formula, it is very clear that in the next period the security services market will be growing dramatically and that an increasing number of specialists with relevant training will be needed to ensure the implementation of cybersecurity solutions and services. It is an obvious trend and a necessity to create centers of excellence in education and research in the field of cybersecurity that bring together higher education institutions and industry representatives. The integration of the research - education - industry will generate opportunities for students and educators to develop their knowledge and skills in innovative projects and will support high-quality teaching and learning. This integration should be done on a sustainable basis, not just project by project, but should be based on long-term cooperation and a responsible approach to knowledge and technology transfer. The ECSO analysis of the need for specialized resources in the future and how to balance the gap between supply and demand also reveals the obligation of all responsible actors to find common solutions to solve this major problem of future development. In summary, the study concludes: "*To meet the growing demand for qualified cybersecurity professionals, educational opportunities must be expanded at all levels by increasing the number of qualified educators, creating synergies between educational formulas and on-the-job training opportunities, involvement and training of skilled unemployed and workers who are not satisfied with their current profession, creating the foundations of lifelong learning in cybersecurity. Gender diversity and the inclusion of women in education and training must also be ensured in order to inform and encourage girls and women to pursue careers in cybersecurity. To achieve this, lucrative cooperation between academia and industry*

is needed, using and combining available resources to ultimately strengthen the field of cybersecurity" [8].

We believe that the human resources strategy followed by Safetech has not only confirmed the conclusions of ECSO, but added another dimension, multidisciplinary training to complete the profile and competence of staff as required by this complex area of cybersecurity.

Bibliography

[1] ECA: Challenges for an effective EU cyber security policy, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_RO.pdf.

[2] ENISA, "Cybersecurity Skills Development in the EU", March, 2020, https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union.

[3] EC, EU Security Union Strategy, COM/2020/605 final, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52020DC0605.

[4] ToR-SIM-Integrated software platform for malware analysis of mobile terminals, https://tor-sim.pub.ro/.

[5] SIIMA-"Integrated IT system for activity management", https://www.ici.ro/pn3-siima/.

[6] USV-" Improving educational processes and activities within the bachelor's and master's programs in the field of ICT by creating a security laboratory", http://www.posdru-142006.usv.ro/.

[7] M. Rauta, V. Gansac, O. Comsa, "A brief Introduction to Cybersecurity Landscape in Industrial Control Systems; Practitioners view", Rocyran, Bucharest, 2020.

[8] ECSO POSITION PAPER, Gaps in European Cyber Education and Professional Training, European Cyber Security Organisation (ECSO), 2018.

Cyber4Kids.ro - How Industry Can Support Cybersecurity Education of Children

Ionuț FLOREA
certSIGN, Romania
ionut.florea@certsign.ro

1. Introduction

Cybersecurity education has two aspects: the education of professionals, those responsible for ensuring the security of information systems, and the education of users, those who use technology to work, learn, or to have fun. For professionals there are specialized courses in the public and private education system, especially in the academic environment; international certifications have been created, such as CEH, CISSP, or CISM, and companies that develop cybersecurity products have developed training and certification programs for those who use them. However, according to Cybersecurity Ventures [1], there is a global shortage of 3.5 million professionals.

Unlike professionals, users do not always have access to training in cybersecurity. Security awareness programs are provided mainly by companies to reduce the risks of a cyber attack [2]. Those who are using the technology for recreational purposes do not receive such training.

An important category of technology users is children. They use it to learn, to communicate, and to have fun. Due to the SARS-COV-2 pandemic and the accelerated implementation of remote learning programs, the interaction between them is mostly electronic nowadays. Although their usage of Internet and on-line resources has increased, formal training on the associated risks is not keeping pace. Also, parents and teachers are not always prepared to guide them on proper online behavior.

Cybersecurity companies can contribute to the education of children. They have the necessary knowledge about risks and protection measures, and they need to pass these things on to children and their educators. The Cyber4Kids campaign

(cyber4kids.ro) is a project which helps parents, and, along with them, their children, to be aware of the risks to which children are exposed on-line and what are the minimum protection measures. It is designed as a series of animated films presenting them in plain language what cybersecurity means. Each episode is accompanied by a guide with tips to stay safe on-line: one page for parents and one for children.

2. Children's education on cybersecurity

Information technology is part of the daily lives of so-called "digital natives", the people born between 1980 and 1994 [3], and is even more present in the lives of today's children, but the curriculum does not keep up with the new technologies they have access to [4]. In the context of using information technology and the Internet, children react and adapt to the digital environment. In the absence of a pre-established framework, the adaptation is made individually or according to a group typology, which depends on each one's entourage.

The risks to which children are exposed online have been analyzed. Some of the issues identified in [5], regarding children in Romania, are:

- Internet access has increased more than 4 times since 2010, reaching 84% in 2018;
- approximately 25% of the children between the ages of 9 and 16 had their devices (phone, tablet, computer) infected with viruses or spyware;
- 43% of the boys and 33% of the girls have been contacted online, for the first time, by a person they had not met before.

In Romania, the curriculum for early education, which addresses children aged 0 to 6, was updated in 2019 and states: "Digital skills are not directly covered by the curriculum for early education, but it is recommended that insofar as the available resources allow, to be approached through the way of carrying out the activities." [6]. The curriculum for primary education was approved in 2013, for the preparatory class, class I and class II [7], and in 2014, for classes III and IV [8].

In 2019, "The Guidelines for the design and updating of the national curriculum" were approved [9]. The following were considered:

- Global trends and challenges, which include the advance of technology and the impact on the labor market and digitalization. The school has a responsibility to provide learning contexts that take these trends into account.
- Defining digital skill as a key competence, in line with the eight key competencies defined at the EU level [10]. This skill includes the cybersecurity component.
- The use of information technology and digital content as modern educational resources, identifying the need for educational resources to be adapted for use in electronic form, including access using a mobile phone.

The Strategy for Digitalization of Education, SMART-Edu, underway since 2020, includes among the ten directions of action "*encouraging and promoting initiatives on online security, data protection, cyber hygiene, IT ethics*" [11].

Through [9], [10], and [11], the development of digital and cybersecurity skills for children is brought to the forefront at the national level in Romania.

In parallel with government programs, alternative educational resources for cyber education are available. They can be created faster and benefit from the practical experience of specialists from the companies.

3. Carrying out a cyber education campaign

certSIGN is a Romanian company that offers products and services in several information technology fields, including cybersecurity. It operates a SOC (Security Operations Center), has a CSIRT team (Computer Security Incident Response Team), and a training center, certSIGN Academy. Its products and services are addressed to companies and government entities. Given their knowledge of cyber threats, certSIGN experts were invited to talk about online protection measures at the schools where their children study, as part of the "School taught differently" („*Şcoala altfel*") program. The audience consisted of students in primary school who used computers and mobile phones mainly for recreational purposes. Since the presentations were received with interest by the students, they were repeated. However, the audience was reduced, at the level of students of several classes.

In 2020, considering the high interest in cyber education shown by students, certSIGN's Marketing and Cybersecurity departments have defined the Cyber4Kids project, to present to primary school children and parents the dangers associated with Internet use and protection measures.

To carry out Cyber4Kids, the following have been considered:

1. Identifying the most relevant cyber security topics for children;
2. Creating the messages and transmitting them in a form that is easy to understand;
3. Promoting the campaign.

3.1. Topics on cybersecurity for children

The topics covered by Cyber4Kids are common in the field of cybersecurity, but they had to be filtered to be relevant to children and to respond to the most common issues they face online.

To select the topics security reports were followed, such as ENISA Threat Landscape [12] and those issued by cybersecurity solution manufacturers, as well as the most common types of attacks identified in real life environments by certSIGN's CSIRT team.

Eight topics of interest were selected:

1. Mobile games;
2. Personal information;
3. Who fools you online;
4. Dangerous links;
5. Internet does not forget;
6. Cyberbullying;
7. Connecting to WiFi;
8. Choosing and protecting passwords.

3.2. Creating the messages

To achieve the desired impact, the topics must be presented in a way that is easy for children and parents to understand. Each topic was documented together with the CSIRT team and then the message was created by the marketing team to ensure that it is suitable for the audience.

The topics were covered by two types of materials:

- Animations, published on certSIGN's YouTube channel [13]. Short films of 3-4 minutes were created, each of them presenting a security risk and recommendations to stay safe. A gamification component was introduced, as the children were presented as Super Cyber Heroes, and each episode introduced a magic object to help Super Cyber Hero in his online adventure.
- Guides for children and parents, published on the campaign website, www.cyber4kids.ro. For children, the guides present tips from animated films. For parents additional information and advices are provided, for example, to discuss with children the topic of online safety, to test the applications and games used by the little ones, to know and constantly monitor their online activity, including through the use of technical solutions of parental control type.

The materials have gone beyond cybersecurity and have also been used as a medium to encourage children to play outdoors, offline, to tell friends the advice they have learned, or to discuss and share experiences with parents.

3.3. Promoting the campaign Cyber4Kids

The campaign was initially promoted through certSIGN's social media channels and press releases. It was immediately successful, being taken over by the central and local press. Cyber4Kids was presented on the radio, on Radio Romania Actualitati, which invited certSIGN to present the campaign in several shows, and on Radio Guerrilla, which organized a contest during the morning show.

Cyber4Kids was registered as an activity in Cyber Security Month, organized at the European level by ENISA [14] and received the support of CERT-RO, which

promoted the campaign's posts on its own channels. CERT-RO and certSIGN also sent letters to the School Inspectorates, the Ministry of Education, and teachers' and parents' associations. Some of the recipients of the messages asked for permission to reuse the materials or for support to organize training campaigns for children on cybersecurity.

Also, the campaign was widely presented at the CERTCON10 event, organized by CERT-RO, in the panel Education, Awareness & Psychology in Cybersecurity, and at CyberThreats & CyberSecurity Day, an event organized by the Romanian Banking Institute and certSIGN. The audience consisted of specialists in the field of cybersecurity. At the second event, during the presentation, an online questionnaire was conducted, one of the questions being whether the participants offered safety advice to family and friends. Over 90% of them said they had done so.

The campaign also drew the attention of other companies: E.ON invited certSIGN to participate in an online event addressing the dangers of cyberbullying [15].

4. Conclusions

Governmental cyber education programs need to be doubled by private initiatives. Private companies and specialists in the field have knowledge in terms of security risks. At the personal level, they are willing to share information and, in some cases, such as certSIGN or E.ON, an organizational framework can be created to support the communication and promotion of information to a large group of people.

Private initiatives can be implemented faster and if the content is relevant, they can be communicated and even promoted through the channels of public institutions.

References

[1] Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021, https://cybersecurityventures.com/jobs/#:~:text=The%20New%20York%20Times%20reports,one%20million%20positions%20in%202014 [Accessed on November 7th, 2020].

[2] B. Gardner, V. Thomas, *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats*, Elsevier, 2014.

[3] S. Bennett, K. Maton, L. Kervin, *The 'digital natives' debate: A critical review of the evidence*, British Journal of Educational Technology, Vol. 39 No. 5, 2008, pp. 775-786.

[4] Page to Screen: Taking Literacy into the Electronic Era, edited by Ilana Snyder, 1998, Chapter 10.

[5] D. Smahel, et. al, *EU Kids Online 2020 Survey results from 19 countries*, London School of Economics and Political Science (LSE), 2020.

[6] Order of the Minister of National Education no. 4694 / 02.08.2019 regarding the approval of the Curriculum for early education.

[7] Order of the Minister of National Education no. 3418/2013 regarding the approval of school curricula for primary education, preparatory class, class I, and class II.

[8] Order of the Minister of National Education no. 5003 of 2 December 2014 regarding the approval of school curricula for primary education, grades III and IV.

[9] Order of the Minister of Education and Research no. 5765 of 15 October 2020 regarding the educational policy document "Guidelines for the design and updating of the national curriculum".

[10] COUNCIL RECOMMENDATION of 22 May 2018 on key competences for lifelong learning (2018/C 189/01).

[11] Digitization of education in Romania - 2021-2027, https://www.smart.edu.ro/ [Accessed on November 16th, 2020].

[12] ENISA Threat Landscape through the years, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape [Accessed on December 2nd, 2020].

[13] certSIGN Romania, https://www.youtube.com/c/certsign [Accessed on December 2nd, 2020].

[14] The European Cybersecurity Month (ECSM), https://cybersecuritymonth.eu/countries/romania/cyber4kids [Accessed on November 16th, 2020].

[15] certSIGN & e.ON webinar on cyberbullying, https://www.facebook.com/E.ONRomania/photos/a.568531686534126/3411953072191959/?type=3&theater [Accessed on December 3rd, 2020].

About Authors

List of authors (in alphabetical order by last name):

Lisa-Maria Achimescu is an expert in security and international law issues, with two doctorates, one in intelligence and national security and another in law. With research expertise in the aforementioned fields, she has successfully collaborated with both the Romanian Academy and higher education institutions as a researcher and expert. She currently carries out her research within the "Carol I" National Defence University.

Ioan Bacivarov, PhD, is full University Professor and Director of EUROQUALROM (ETTI - P.U.B.). He developed during the last 45 years several programs in quality and dependability. He is president of RAISA and of ASRO/CT 144 "Dependability". He is Editor-in-Chief / Editor / Co-Founder of several international journals, including Quality Assurance, IJISC, Quality - Access to Success and Chair of CCF international conferences.

Lecturer **Laurențiu Boicescu**, PhD, graduated Politehnica University of Bucharest in 2009 as a communication network engineer and software developer versed in over than a dozen markup and programming languages for mobile and web applications, as well as M2M communication. He is a specialist in IoT, databases, cybersecurity, and quantum cryptography, involved in several national and international projects.

Răzvan Bologa is a full Professor within the Computer Science Department in the Bucharest University of Economic Studies. He is the head of the innovation and research commission inside the university where he has managed several important projects as well as a master program. He is actively involved with innovative start-ups. His research interests include: Industry 4.0, cybersecurity, AI and online learning.

Simona Caraiman is Associate Professor and researcher at the Faculty of Automatic Control & Computer Engineering. She coordinates the "Distributed Systems and Web Technologies" master's track. Her teaching and research experience has been primarily focused in the fields of computer vision & machine learning. She also holds a postdoctoral degree in quantum computing & quantum information processing.

Daria Catalui is a cyber security training and awareness professional with significant working experience in EU's cyber security agency- ENISA, the European Commission and the Romanian Presidency of the Council of the EU. She is currently leading the global education account of a major financial services company, also conducting research with focus on gamification through CyberEDU project.

Costel Ciuchi, PhD, is Senior Expert in the Information Technology & Digitalization Directorate, General Secretariat of the Government with responsibilities in developing government apps and infrastructure, security of IT services (INFOSEC) and coordinating GOV.RO Domain Registry. Associate Professor at University Politehnica of Bucharest, he conducts research activities in cybersecurity and security risks area.

Dan Cîmpean accumulated over 20 years of experience in cyber security, risk management in Brussels, Bucharest and internationally. He led professional teams that supported European institutions, national competent authorities, and large industry actors in defining and implementing their cyber security policies and strategies. Since May 2020 he was appointed as General Director of CERT-RO.

Iulian Coman is a Seconded National Expert at the European Union Agency for Law Enforcement Training (CEPOL), police officer in the Ministry of Internal Affairs, Romania, with expertise in analysis, law enforcement training and international relations. He is a PhD candidate in public order and national security domain with "Alexandru Ioan Cuza" Police Academy Bucharest.

Olivia Comșa is the coordinator of Research and Development Department at Safetech Innovations. She has a strong background in security research and relevant expertize in cyber security policies, strategies, programmes and projects at national and international level. Increasing cybersecurity culture and international cooperation in cybersecurity framework development are her main priorities.

Dirk Dubois graduates the Belgian Military Academy with a master degree in social and military science. In the first part of his career, he occupies several operational posts and positions as a staff officer. From 2007 to 2012, he was a training manager at the European Security and Defence College, before joining the Directorate-general for education of the Belgian MoD. Since 2015, he has been appointed as Head of ESDC.

Ionuț Florea graduated Politehnica University from Bucharest and holds an MSc from the Military Technical Academy "Ferdinand I". He is active for over 20 years in cybersecurity, having assignments in consultancy, audit, and technical implementation as well as in analyzing the impact of legal framework over the cybersecurity domain. He is involved in research projects and in standardization activities within ETSI.

Octavian Fratu (IEEE Member from 2000) received the PhD degree in Electronics and Telecommunications from the University "Politehnica" of Bucharest, Romania in 1997. He achieved postdoctoral stage as senior researcher in 3rd generation mobile communication systems, based on a research contract between CNET-France, ENS de Cachan - France and Université Marne-la-Vallée - France.

Larisa Găbudeanu is a data protection and information security professional. She is a PhD candidate with the Babeș-Bolyai University. With a vast experience as a lawyer in an international law firm, counselling international clients and coordinating projects related to IT law, cyber-crime and data protection matters, she also has good knowledge of information security in a regional banking group.

Tiberiu-Marian Georgescu is a Teaching Assistant within the Department of Computer Science in the Bucharest University of Economic Studies. He completed his PhD program in Economic Informatics in 2019 having the main topic Cybersecurity in the context of Big Data. His main fields of interest are cybersecurity, machine learning and natural language processing.

Simona V. Halunga is a full professor at in University Politehnica of Bucharest, Telecommunications Department. Her domains of interest are communication systems, with an emphasis on wireless systems modeling and evaluation, satellite communications, digital signal processing for telecommunication, data modulation and encoding, security in wireless systems and mobile networks.

Prof. Dr. **Udo Helmbrecht** studied Physics, Mathematics and Computer Science and obtained a Doctorate in Theoretical Physics in 1984. From 2009 to 2019, Helmbrecht was the Executive Director of the European Cybersecurity Agency ENISA. Currently Helmbrecht runs a Quantum–Communication project at the Universität der Bundeswehr Munich, Germany.

Math. **Angela Ioniță**, PhD, is Senior Scientific Researcher I, graduated in mathematics - informatics, has been involved in numerous national and European projects as coordinator and / or expert, is the author and co-author of several research and technical reports, scientific papers, books and has more than 35 years of experience in research and development in the field of informatics.

Handy-Francine Jaomiasa is a specialist in communication and public relations with practical experience in the field of audio-visual and social media. Currently, among the areas of interest and expertise: the impact of new media on political communication, the use of social media, the impact of disinformation on society, etc. Concerned about the words fitly spoken.

Ioan-Cosmin Mihai is a researcher, professor, trainer, and conference speaker, with an experience of more than 16 years in cybercrime and cybersecurity. He is a cybercrime training officer at the European Union Agency for Law Enforcement Training (CEPOL), associate professor at "Al. I. Cuza" Police Academy and visiting professor at the University Polytechnic of Bucharest and "Carol I" National Defense University.

Sorin Mirițescu heads the Security Architecture and Software Development department, joining Safetech Innovations in 2019. Over the last 20 years he has held various technical and managerial positions, being involved in complex projects in the fields of software development, information security and IT&C infrastructures. Sorin graduated with a degree in CS from Bucharest University, Faculty of Mathematics.

Cătălin Mironeanu is a cybersecurity researcher, trainer and conference speaker. He lectures at the "Gheorghe Asachi" Technical University of Iasi, Faculty of Automatic Control & Computer Engineering. He is a trainer for "Fortinet's NSE Institute" Security Academy and a member of the Open Infrastructure Research Center of the Faculty of Automatic Control and Computer Engineering.

Liviu Moron is a cybersecurity consultant for Cybershare. He holds multiple cybersecurity certifications (GPEN, GXPN, GMON, GAWN) and he is interested in new methods to deliver cybersecurity educational programs. He worked for public and private companies (European Commission, URW, Viparis, etc.) and he is involved in Cybershare Conference, Cybershare Academy for Schools and CyberSchool CTF.

Bogdan Mureșan is a project coordinator and expert within the European Studies Unit, European Institute of Romania. He is an associate editor for the Romanian Journal of European Affairs. His academic studies include the fields of international relations and European Affairs, history and political science. His area of interest also touches upon the domain of strategic communication and countering disinformation.

Dr. **Tal Pavel** is the founder and director of the Institute for Cyber Policy Studies. An academic lecturer, researcher, and speaker specialize in cyber threats, and policy, the Head of Cybersecurity Studies in the Information Systems Program, at The Academic College of Tel Aviv Yaffo. Dr. Pavel holds a Ph.D. in Middle Eastern Studies from Bar-Ilan University, Israel.

Marius Pârvu is an experimented engineer in cyber security, specialized in securing mobile devices and devices having Linux operating system. He also has programming skills in several popular languages, skills related to cloud technologies, virtualization, having many technical security certifications. He has studies in computer science that include a master's degree at the Academy of Economic Studies in Bucharest.

Assoc. Prof. PhD. Eng. **Florin Popescu** at National Defense University Carol I, holds a PhD at Polytechnic University of Bucharest and he has brought over time elements of originality which have been disseminated to prestigious international publishers working closely with expert researchers and professionals from leading institutions, including Massachusetts Institute of Technology, Harvard and Stanford University.

Assoc. Prof. **Eduard-Cristian Popovici**, PhD, graduate of POLITEHNICA University of Bucharest in 1992 (BSc, MSc), is a specialist in mobile and client-server technologies for communication systems, IoT and cybersecurity. He was involved in several national and international projects as software architect and software developer. He co-authored 5 books and more than 50 papers.

Dr. **Nathalie Rébé** holds a Doctorate in Business Administration (DBA) from Paris School of Business, and a Doctorate in Juridical Science (JSD) on Financial Crimes from Thomas Jefferson School of Law (USA). With a Post Graduate Diploma in Cyber Law from the University of Montpellier, Dr. Rébé’s research and publications have been focused on New Technologies, Security, Privacy, and Regulatory matters.

Răzvan Rughiniș is Professor in the Department of Computer Science of University Politehnica of Bucharest, co-founder and coordinator of the Innovation Labs tech accelerator. He has extensive research, teaching and doctoral coordination experience in the field of cybersecurity, human-computer interaction, and IoT. He has published over 50 scientific research papers in the field of cybersecurity, in the last decade.

Dr. **Gregor Schaffrath** graduated in Computer Science at Saarland University. His academic work at the University of Zurich and the TU Berlin covered topics in cyber security and network management. He worked together with the European Commission on concepts for the design of a Health Research and Innovation Cloud and is currently SNE to the European Security and Defence College (ESDC).

Dr. h.c. **Detlef Schröder** has been the Executive Director of CEPOL since 2018. Prior to joining CEPOL, he was a Senior lecturer at the German Police University, with over 100 publications in journals and six book publications. Earlier, he had a career within the Police of the Federal State of North Rhine-Westphalia up to senior police management positions. Dr.h.c. Schröder has two Master Degrees and a BA.

Mihai Sebe holds a PhD in Political Science from the University of Bucharest. He currently coordinates the European Studies Unit at the European Institute of Romania. Among his topics of interest are: European affairs; the history of the European idea; the impact of new technologies on politics and society, etc. Passionate about the shape of things to come.

Mircea-Constantin Șcheau is PhD in Public Order and National Security with a theme of interest for the economic and security domains "Cybercrime regarding financial transfers". Author and coauthor of three books, more than thirty scientific articles in the fields of management, economy, law enforcement, defense, critical infrastructures, information technology and lector for many international conferences.

Dr. **Marios Thoma** holds a PhD degree in Cyberspace Defense and specifically in the modelling and early detection of cyber-attacks. He is a military officer currently seconded as training manager in the European Security and Defence College (ESDC) leading since 2018 the Cyber Team of the College. Previously he served in the military of Cyprus at various posts in the domain of communications, security and cyber.

Eliza Vaș has been working for the European Institute of Romania since 2014, as an expert in European Affairs. She is the Policy &Strategy Director of the Young Initiative Association. She has studies in the field of international relations and political sciences, and she is currently a PhD candidate with the Babeș-Bolyai University. Her research themes include democracy, digitalisation, youth policies and circular economy.

Romanian Association
for Information Security Assurance

Romania, 2020