Cyber education approaches for a modern security in a future society

Sorin TOPOR
National Defense University „Carol I"
topor.sorin@unap.ro

Abstract: The digital revolution among all the obvious benefits it brings to human comfort also brings a number of vulnerabilities. These are most often caused by the misunderstanding of new behavioral rules in an information society. Now, these rules are required not to affect the performance of current activities. Determining members of society to their conscious respect is only through education. Reports that indicate alarming growth in the diversity and complexity of cyber threats confirm the rupture between education and the correct functioning values of the entire society.
In our work we propose to launch education themes in the spirit of maintaining a high level of national and community security. In this contest, we appreciate that starting training programs in the areas of cyber security, from the youngest age, is beneficial to the future evolution of the whole society. They should be done for a unitary purpose, with coordinated and carefully verified objectives. To achieve these ideals, new security specialists must be trained and employed, cyber education being a fundamental competence for the future human society.
Keywords: digital revolution, education, cyber education

INTRODUCTION

Cyber-space technologies and threats are evolving continuously, producing deep changes in our lifestyle. These changes are not limited by geographical boundaries, by belonging to military or civilian systems, public or private. But any technology, program or cyber-space system can be a potential target for cyber-attacks. That is why cyber security is and will continue to be a major factor determining the health of an information society. Their complexity and diversity, besides gaining undeniable advantages and uncountable vulnerabilities in the technologies and information systems they base on their day-to-day operations.

People's dependence on information network connections ensures that this type of subject will always be of interest and will lead to wide-ranging discussions to find a way to rise and maintaining at a high level of collective and personal security for users. It has to be understood that these subjects are characteristic of the entire human society and not just the professionals of a professional community. Business and industry may be more concerned with cybercrime and cyber spy issues in order to protect their economic gains. States and international organizations may meet other cyber threats by state and non-state cyber-actors, such as attempts to influence electoral choices, extract information from databases of human resources structures [1], or gain control over the command and control elements of national critical infrastructures, such as power plant, water supply, emergency

communications and other vital services. Besides, there are international exercises that have as main objective the prepare and training of decision-making structures and the defense of national and international infrastructures under ipotetical cyber attacks. An example of this is the Lock Shields exercise, in 2018, which focused on the protection of the key systems that belonged to critical infrastructures.

Therefore, in an interconnected world through computer networks, it is explained why, at UE level, an advanced and continuous education is considered to be a great topic of huge importance [2]. Undoubtedly, the directions of evolution of all economic domains and branches, in an exponential form, could not be achieved without open and quality education. We can assume that they will not only change the form and mode of representation of human society, but will provide economic growth, knowledge, social cohesion, innovation etc., with profound implications for personal development. And because the return to the pre-episode of the "cyber era" is not possible, we appreciate that one of the most obvious directions of evolution is the formation of users to maintain security at the level of devices connected to computer networks.

A BRIEF COMEBACK IN HISTORY

One of the best examples of cyber security education is Estonia. We must remember that since 2007, since the cyber attacks on 58 sites belonging to both institutions and citizens, attacks in response to the relocation of the Soviet bronze soldier monument, Estonia has laid the foundations for specialized programs to citizen education, programs which today are a benchmark in the EU and NATO. Before to the incident, cyber attacks were not considered as threats to a state's security, but rather fraud methods for various financial facilities. For them ware no common rules or agreement for administrative and political decision-makers.

Moreover, at that time it was not established if behind a cyber attack against a NATO member state could activate collective defense, under Article 5, or whether a state could legitimately force respond against such cyber attacks. This event not only taught Estonia but all countries that have a modern cyber-based infrastructure.

Now, it is fully recognized that Estonia has become a global force in the field of cyber security knowledge, being able to ensure the dissemination of information and lessons learned to all states with which it has signed development and cooperation agreements in the field of cyber security.

In fact, from 2016, Estonia hosts in December one of greatest NATO's cyber defense exercises. Under the name of "Cyber Coalition", the event attracts more and more specialists in cyber defense and related fields, law experts, government officials, military, academics staff and industry representatives. It takes place on the network and can be connected from dozens of locations in Estonia and other countries in from Alliance.

Moreover, Tallinn hosts the Cooperative Cyber Defense Center of Excellence (CCD COE), an international operational military organization, established in 2008. It is funded and managed on voluntary participating states. Its activity is characterized by scientific research, development, training and education for various technical and non-technical directions in the cyber defense sector. Publications such as the Tallinn Handbook, volumes of the annual CyCon conference papers, other works with reference to exercises such as Shields Locked etc., are not only landmarks for Estonia but also for all the capabilities involved in enhancing NATO's cyber security.

Also noteworthy is that Estonia has succeeded in transforming this cyber security requirement into a way of industry supporting, numerous start-up organizations and Estonian businesses providing consultancy in this field. Among these are the BHC Laboratory, Clarified Security, Bytelife, GuardTime, Cybernetics [3] etc.

Through all these succinct presentations of Estonian performance, we wanted to highlight not only the reality that cyber security is a top field and can determines the existence of the country by ensuring a high level of security in all areas of the economy, and also that these performances require a good education and an adequate

training based on the study of previous events. As you can see, no cyber attack was the same as the previous one. This means a high level of upgrading, flexibility and training of attackers. They may be state or non-state hackers. Cyberterrorism is no longer a topic by which terrorists promote their propaganda through Internet. At present, a terrorist can hit the IT&C critical infrastructure systems and can cause major damage and loss of human life with just a simple keyboard click.

This "fear" is based on hypothesis possible to be made. Therefore, every citizen must be aware that compliance cyber security rules will ensure his existence in the digital era, and that any avoidance of imposed rules, either inadvertently or convenience, will inevitably, sooner or later, lead to cyber death. This is why cyber security education is needed for all members of a informational community.

THE CORRELATION BETWEEN THE EDUCATION REQUIREMENT AND THE MODALITIES FOR ITS APPLICATION

In the EU, education is organized and carried out at the level of each Member State. Starting with the Bologna Process, the educational process has undergone deep mutations allowing the interference of national education systems in higher education. By recognizing qualifications and periods of study, greater openness is gained in the labor market, gaining the full community space[4]. Thus, Erasmus+, Horizon 2020, European Structural and Investment funds (ESI funds), infrastructure and installations investments, other innovative projects etc., all help to create a European education that promotes common values and facilities, by diplomas mutually recognized by all European institutions.

Moreover, the ministers of education gathered in Paris, in May 2018, adopted a the Paris Communiqué and setting priorities for the next few years, more ambitious after 2020. Of these, we draw attention to the recommendation to establish integrated transnational cooperation in the field of higher education, research and innovation. To achieve this, a related education platform is needed in which each institution determines and complies with rules.

In other words, a transnational platform for education implies a new type of education for users. Only such a European citizen who wishes to prepare will be prepared to detect the real information from misunderstanding or manipulation, will be ready to identify the emerging vulnerabilities and decide for what he wants to himself prepare, what is his role and place in the social or professional community etc.

As can be seen, two complementary systems are needed to achieve this objective, both pursuing the same thing, the education of the future European citizen. One of the systems is that related to the content of the educational programs, a requirement determined by the variety of occupations recognized in the European labor market. The second system refers to the security of the educational process, as important as the first system

For example, under the pressure of the huge amount of information that an daily individual undergoes in this globalize information environment, and in order to increase his comfort, he will seek to use the easiest access and easiest ways to perceive. It is obvious that such education tends to be very trivial. Even if he understands that in order to find the quality of work in any field, there are increased demands on his education and training, he will seek to simplify the process of information processing, more and more, based on fast and cheap information resources. Such person will know more about less. We can meet such people anywhere: on the street, in televised reportages, tv shows of obscure media, in schools etc. The top is that they also reach key positions in various institutions where their work can influence the decision-making process.

We can appreciate that this theme is not new. Novelty may consist of how to approach it. We are convinced that a profound analysis of this topic will underpin a security strategy for the educational system, but through our work we don't want to achieve this.

Our work is about the second system, namely security for education, especially cyber security for education. Calling on the model of militarized systems can not do much in the

context of blaming military values from the highest social levels. Moreover, fear of security still represents a social weight, and is often presented as an intrusion into personal life and a restriction of social liberties. Moreover, in the recently international events, some countries adopted the temporary solution to block access to cyber information. This has proved to be a failure and has not solved anything during the various events. Contemporary information technology allows to any person who has access to information to support decision-making on what he finds, ie information from the global information environment on Internet.

Therefore, we argue that if "security" is presented as a requirement to maintain comfort, perhaps the civic perception will be other. The creation of inclusive and connected higher education systems may be a solution for the contemporary social problems faced by European democracy. This is only if national policies and strategies for higher education are inclusive and in all environments and that higher education institutions will not offer exclusive educational programs linked to their own communities alone. In addition, teachers and students need to reform their methods and forms of communication for increased efficiency in global educational resource management. This requires interventions by the government, schools and higher education associations.

It may be noted that at this time there is a serious lack of basic literacy and numeracy skills, digital skills, experience of independently learning, lack of orientation based on native qualities etc., but that does not mean that nothing has to be done. We appreciate that systematic cooperation between education institutions, schools, education service providers and industry representatives is necessary not only for the proper training of young people but also for students orientation to develop their talents, not just on the basis of previous training. This requires a secure educational environment.

Based on Estonian experience, preparing all national institutions to limit the effects of a cyber crisis is through intrusion detection and protection systems, by facilitating collaboration between public and private institutions and, last but not least, by making all users aware in all areas of activity of the cyber security requirement. That is why we support the opinion of Klaid Mägi, the head of the incident response department (CERT-EE), who said that: „*Most important, there is a common understanding that cyber security can only be ensured through cooperation and that a joint contribution is required at all levels - state, private sector and individuals*". [5]

On the other hand, the contemporary attacks of cyber criminals are an increased risk to the security of any national system. It is proven that their interest is stimulated by the use of digital services in online financial fraud or extortion. Through the spread of ransomware in IT&C systems integrated into hospital facilities, road, rail, air and maritime traffic management, power supply, or other vital elements, organized crime can endanger people's life and health. In the future, where is anticipated a greater digital communication, through the implementation of the concept of "Internet of Thinks," the protection of modern and comfortable living requires investment not only in the security of essential services and e-government but also in the creation and support of new educational programs that systematically raise awareness and competence in information security science.

It is obvious that such solutions will control not only the phenomenon of cyber crime but also the politically motivated attacks or cyber terrorism. Thus, we can truly appreciate the fact that the importance of cyber security for electronic services is much more underline than any other factor for both the private and the public sectors.

CONCLUSIONS AND PROPOSALS

As you can see, the subject chosen for analysis is extremely vast and complex. That is why we want to conclude, without claiming that we have exhausted it, with the observation that only an adequate education forms a security culture that can provide discouragement for a potential entity that will want to speculate or even develop the inherent vulnerabilities in a information society.

We consider that a possible public debate

on this subject should be organized on five headings to unify the basic concepts of security and to identify the common environments through multidisciplinary security approach as follows:

• Identify the multitude of security objectives;
• Establishing the procedural nature of security;
• Identification of the objective and subjective dimensions of security;
• Establishment of ways to security instrumentalize for other purposes;
• Underline the importance of methodological pluralism to a convincing and thorough analysis of security.

As we can see, all five directions are within any educational system. We are convinced that only an interdisciplinary approach of security, in general, and cyber security, in particular, will allow for the establishment of interdisciplinary assessment systems under various application designs which will provide not only increased resilience to cyber societies but also a form of discouraging those interested in influencing social events by depriving information or manipulating.

For this, training of cyber security specialists can be a contemporary and real requirement of the relevant market for develops of protection and defense systems against new types of threats. But this technical approach will not able to oppose a complex cyber crisis situation where victims will be ordinary citizens. That's why we consider the only solution for a long time is educating all users to become aware of the cyber security requirements.

Based on the various studies that aboard the evolution of cyberspace and education, we propose to follow some development as:

1. Earlier it is the better

Undoubtedly, early preschool education lays the foundation for later success in life in terms of education, professional and social integration. This is also done on the basis of cyber-space-facilities such as games, communication programs, digital facilities of object etc., all online. Therefore, they need to understand what is permitted and what can endanger their life, thus strengthening the advantages of early education. In this regard, we recall the effects of the "blue whale" game, which among minors led to "experiments" of various extreme activities, some children losing their lives.

2. Understanding that graduating from high school or faculty does not mean the end of learning

Most young people enrolled in primary and secondary education when they reach adulthood will be attracted to occupations that did not exist before. That is why lifelong learning is not only a valid concept for the present, but a commitment to a society that evolves and is obviously also characterized by the aging process of the population. Therefore, changing the profession, changing the workplace and even the field of activity are not workforce caprices, but a way to adapt to the market needs. If several generations ago, a younger who chose an occupation could retire from that job, having only one life-long job, in the future, the one on the retirement threshold will know more professions and holding more jobs throughout his career.

3. Digital competences are literacy for the future digital society

At present, there are disciplines that are the foundation of education for any profession. However, in order to practice a profession, it is not necessary to know all the disciplines of a science but those that are considered fundamental and specialized. Based on these disciplines through dedicated programs, specific practical skills can be developed and deepened. We estimate that, as mathematics and physics are the foundation for engineering sciences, digital competences will become indispensable for the professions of the future. At this time, over 90% of professions involve the use of an independent or integrated IT&C device in an ensemble. We could say that young adults are advantaged by the reality that they grew up with a computer in their hands. But technology will not stay in place and new skills, perhaps unimaginable at present, will be needed to meet the demands of the future labor market.

4. Adapt people to technology control

Nowadays, in most businesses, it is noticeable that people are often in a position to compete with a technology robot or an software during the work program. Because of this, there are situations where people's efficiency is much lower than that of the robot. This does not mean that, in social terms, the production process must be abandoned and employees' education must be reorientated to develop native skills such as creativity, intuition, negotiation, critical thinking, communication, teamwork etc., and computer science to support these skills, unparalleled by any robot.

5. Moving from curricula's intredisciplines to interactive multidisciplines education

Tendencies of adopting distance learning programs are currently known. The Internet allows this. But distributed or online education programs are a tribute to an academic institution or teachers [6]. We are all convinced that contemporary technology can be used to acquire new learning ways. Problems arise in how to access and control the learning of those enrolled in a program. There are very few who try a multidisciplinary approach to a lesson. It is clear that such a lesson requires much higher costs and resources. But the benefits are multiple. For example, a lesson on vine growth can be a multifaceted analysis, not just a biological study, but an analysis with implications of geographic, economic, sociological etc., so that young people learn interactively by activating their acquired knowledge in other disciplines.

6. Planning the transition from school to employment

Currently, it can be seen that young graduates hardly find a job. That is why they are oriented to jobs where life security is not greatly affected by social fluctuations, the evolution of society or local economic development. Moreover, learning motivation is no longer stimulated by the „note". More and more employers submit a candidate to an exhausting practical test or require experience in field of job. Therefore, in order to make education more effective, each educational institution should be supported by the beneficiaries. It is advisable to involve these beneficiaries in the management of educational programs and to determine which disciplines should be known, not to criticize the incompetence of the graduate series.

7. Stimulate critical thinking and entrepreneurial skills

Most contemporary social events demonstrate that young people can not make the difference between fake news and real news. This is why in learning programs should be included critical thinking topics. This would help the youngers to live in the right direction. But the greatest gain would be of society of which the young people belong, thinking rationally ensuring the security and development of any democracy. Critical evaluation of information and knowledge of interest from diverse dedicated or open sources (mass media), is one of the most important skills that a young person should have in the future in order to find his profession which best channel their native skills. These combined with a range of entrepreneurial skills will enable it to be linked at macroeconomic level with other institutions, thus contributing to maintaining a high level of national and international security.

References

[1] Mihai-Ştefan DINU, New *Data Protection Regulations and Their Impact on Universities*, in eLearning & Software for Education, Vol. 4, Bucharest, 2018, pp. 26-33.

[2] https://ec.europa.eu/education/education-in-the-eu/about-education-and-training-in-the-eu_en

[3] *The NATO Alliance and the "cyber sword" Estonia*, http://weaponews.com/opinions/7702-the-nato-alliance-and-the-cyber-sword-estonia.html visited on 14.01.2019

[4] *Procesul Bologna şi spaţiul european al învăţământului superior*, https://ec.europa.eu/education/policies/higher-education/bologna-process-and-european-higher-education-area_ro visited on 10.01.2019

[5] https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/ visited on 20.01.2019

{6} Elena Şuşnea, *Improving Decision Making Process in Universities: A Conceptual Model of Intelligent Decision Support System*, In: 5th International Conference EDU-WORLD 2012 - Education Facing Contemporary World Issues, In Procedia - Social and Behavioral Sciences • April 2013

{7} Nouzha Harrati; Imed Bouchrika; Zohra Mahfouf, *e-Learning: On the uptake of modern technologies for online education*, In: 6th International Conference on Information Communication and Management (ICICM), IEEE, Hatfield, UK,2016.