**Title of the article – ex. Education in the area of CSDP**

**Alexandre JEROME PhD[[1]](#footnote-1), Alexandra TULVAN[[2]](#footnote-2)**

|  |  |  |
| --- | --- | --- |
| A R T I C L E I N F O |  | A B S T R A C T |
| *Article history:*  Received 15.12.2021  Reviewed 22.01.2021  Confirmed 28.02.2021  Pages/words: 6/3000 |  | The abstract should have 200 to 300 words. The purpose of this article is to highlight the vulnerabilities of the Romanian ID card for the examiners from border crossing points and within forensic laboratories. The Romanian ID card is not only the most widely used identity document of Romanian citizens but also fulfills the role of a travel document that can be used in place of passports in EU countries, in the countries of the European Economic Area, in the countries of European Free Trade Association Exchange, in Albania, Andorra, Bosnia and Herzegovina, Canary Islands, Faeroe Islands, Georgia, Gibraltar, Guernsey, Isle of Man, Jersey, Republic of Macedonia, Moldova, Monaco, Montenegro, San Marino, Serbia and the Vatican. These vulnerabilities are caused by the way in which the ID card is created and the security elements that are easily to counterfeit. Of these vulnerabilities take advantage those who want to illegally cross the border, the Romanian ID card being one of the most counterfeited travel documents in European Union. The information that substantiates this article are the result of our laboratory casework and working groups’ document examination that we attended. |
| *Keywords*  ID card  Security feature  Counterfeit  Laser-jet printing  Document examination |
|  |  |  |

Contents

1.Introduction

2.Main aspects

3.Conclusions

4. References

♦ ♦ ♦ ♦ ♦

**1.Introduction**

The lenght of the article should be between 3000 and 5000 words (6 to 10 pages). The article should have a clear structure (with sections as shown in current example).

The development of professional skills of those who will serve in various areas and who are facing the need for shaping a security information fine-tuned (from governmental and up to the end users) by adopting a management policy outlined by staff quality, rigor and also by seriousness is one of the main objectives which our society must consider. Nonetheless, highlighting the danger emanating from criminal acts committed in informatics is also a societal necessity. Every day, millions of people can turn into victims of crimes such as phishing, smishing, identity theft or similar by simple contact with branches of technology, so it can be easily noticed the compulsoriness of creating by each state of organisms that are designed to identify, analyze , prevent and combat every touch of moral and financial integrity of individuals brought by various methods that constitute the semantic field of cybercrime.

**2. The need for education**

One of the main issues when dealing a new threat is realted to the very idea of knowing its characteristics. As such, when discussing the idea of cybersecurity, one could underline the importance of the education on every layers of the society. The need for education is stringent when referring to cyber environments, as it is a well-known fact that the IT infrastructure is present in every domain and every layer of the society, being a current component of our daily life.

Perhaps the main question to be asked is: how could it support the cybersecurity policies and how could enhance them? Preserving innovation as well as private sector and consumer confidence in the security of the Internet economy is important for promoting economic prosperity and social well-being. Public policies and private-sector practices that promote education and innovation for the purpose of enhancing cybersecurity will help ensure that the Internet remains fertile ground for an expanding range of beneficial commercial and social activity.

The persistence and growth of cybersecurity threats compels us to re-think both how those challenges are affecting businesses and citizens, as well as useful steps that can enhance the security of Internet-based commerce. Small, medium, and large businesses, and consumers, will continue to increase their reliance on the Internet increasing. As that reliance grows, their understanding of cybersecurity must increase as well. A suggestion is that public policies affecting cybersecurity on the Internet, as well as private sector norms, must be continually updated to remain relevant in a fast changing environment.

Public awareness of cybersecurity issues is at the core of our evolving strategy to enhance online safety. As attacks on consumers and corporations become more commonplace and sophisticated, there must be increased preparedness to respond to and mitigate these attacks that can harm the economy, public safety, and our spirit of innovation. While education of the public may offer limited effectiveness in safeguarding against some threats (such as massive data breaches, carding markets, sophisticated point of sale or ATM scams), other common threats (such as malware, fraudulent websites, viruses, phishing or spear phishing emails, and the exploitation of vulnerabilities in servers and network infrastructure) often do take advantage of the lack of education of individuals. While research and development are important to preventing security breaches, informed users and a security-conscious workforce are also important elements of an effective cybersecurity strategy.

As stated before, we are members of a society dependent of technology, internet and their inherent benefits. As the entire world is interconnected, the threats are also networked. Beyond affecting the fundamental rights of a citizen, a cyber threat tends also to tackle national safety of a country, as well as the interest of regional organizations (such as European Union). Developing a powerful and efficient policy in the field of cybersecurity should be a problem to solve for every organization, be there a governmental one or one form private sector. Every country should intervene in developing a national conscience, capable to sustain attacks against cybersecurity capabilities, by developing educational strategies meant to insure a better education for the citizens. Also, stimulating youngsters and attracting them in an active participation in the continuous fight for prevention and fighting events related to cybercrimes should be a must. From this stage, there is only a small step to the development of initiatives/ strategies related to education. There have already been different projects in this field, sustained by either European institutions or private entities or NGO`s (such as DefCamp Conferences, Security for Information Technology and Communications, European Cybersecurity challenge etc.).

**3. The effects of education on the fight against cybercrime**

As noted above, education is being presented as a real support in the fight against crimes committed in cyberspace by developing a strong knowledge base, thus creating a decisive factor. A strong defense against cyber threats is nothing but a huge step forward in winning the battle against crime . Creating organisms on this purpose at European level and also the implementation of projects that have as a theme the concept of computer security (like those above) do nothing but to contribute to fulfilling the proposed objectives of the European cyber security strategy. The training of specialists able to face such a struggle must become a priority for the EU and member countries. Education supports the development of security policy pursued by the European Union(1) through training of persons entrusted with the prerogative of preventing and combating cybercrime , as well as adequate information of users so that they can be able to identify cyber attacks more easily, accomplishing in this way -the most important stage of information security, namely prevention. In this sense, education has proven its significance in the fight against cybercrime by:

• Making a correct and accurate information leading to the formation of a consciousness of our society on the importance of cyber security in the context of globalization and the dangers to which we are subjected every day.

• Empowering people with responsibilities in the information security field, so that they are able to treat threats with the utmost seriousness and not in a superficial way . The issue of cyber security is , as mentioned in the above context , as serious as possible because of the damage that can be produced without a strategy very well developed in this regard can rise to unimaginable levels. Cybercrime causes a great deal of computer security incidents.

• Efficient fight against cybercrime by developing a professional conscience and focusing on the quality of information. Cyber security specialists must be prepared with professionalism and rigor in order to master their abilities in the purpose of mobilization so that they can face this increasing danger.

• Promote campaigns to attract citizens into this active fight against this phenomenon by implementing initiatives such as organizing conferences and national and international competitions on security and cybercrime field, achieving commercials of social interest to bring to the public the importance of cyber security and the immensity of negative effects resulting from the commission of cybercrime, introducing into the school curriculum educational classes in cyber security or even the creation of master's degree programs on this issue to ensure those interested deepening their knowledge on this subject.

**5. Conclusions**

The internet, together with the information communications technology (ICT) that underpins it, is a critical national resource for governments, a vital part of national infrastructures, and a key driver of socio-economic growth and development (2). Over the last forty years, and especially since the year 2000, governments and businesses have embraced the internet, and ICT’s potential to generate income and employment, provide access to business and information, enable e-learning, and facilitate government activities. In some countries the internet contributes up to 8% of gross domestic product (GDP), and member countries of both the European Union (EU) and the G20 have established goals to increase the internet’s contribution to GDP. This cyber environment’s value and potential is nurtured by private and public sector investments in high-speed broadband networks and affordable mobile internet access, and break-through innovations in computing power, smart power grids, cloud computing, industrial automation networks, intelligent transport systems, electronic banking, and mobile e-commerce. The rise of the internet, and the increasing social dependence on it, did not occur overnight. The first ‘internet’ transmission occurred in October 1969 with a simple message between two universities. Now, 294 billion e-mail are sent per day.

Our actual`s society`s paradigm is characterized by an extreme diversity, yet also by a great sensitivity and vulnerability. The society itself resents the need for security (be there social, economic, politic etc.). The newest and most sensitive vulnerability is the one related to cyber security, as new technologies evolve and penetrate most of the compartments of current life. The degree of security can be enhanced thru upgraded technologies, thru multiple investments – yet all of those are inefficient if the human component is not altogether tackled, as it is the basic element to be taken care of.

Cyber security proves to be a serious problem, as the technology is an environment with a high dynamicity. Today`s world is more sensitive and more interconnected than yesterday, and one can say that tomorrow it will be even more sensitive and more networked than today. As such, the implementation of a coherent and efficient policy related to facing the newest threats becomes a must. Our actions can decide what will become of our civilization over centuries to come; as such, efficiency and dedication are needed for tackling such a global problem.

Within this study we have defined the concepts of cyber security and the importance of approaching such subject. Also, we decided to tackle the current stage of education in the field of cyber security development, as well as the role of education in developing a conscience meant to prevent and fight cybercrime. It is a reality the fact that education is an universal necessity, being actually the pillar to sustain a country`s security, as it is capable to create specialists able to fight such type of crimes, as well as it is capable to develop the social conscience able to identify such dangers, avoid and reject them. Human element is an important actor on the stage of cyber security, thus investing in this area must become one of the main objectives of European Union should develop for enhancing its security policies – and the motives for that are obvious, deriving from this study.

Furthermore, an efficient curricula is built on professionalism and quality, and can result in training of an efficient manner the future generations of specialists and stakeholders and implicates the evident growth of efficiency in preventing and fighting cybercrime.

In direct relation with our previous statements and to the content of the study, we have formulated the following recommendations and motions:

-creating excellence training centers for annual educational meetings of cyber security specialists. It would be best perhaps to have such training centers at national level, as well as at continental one, under the umbrella of European institutions.

-implementing policies to allow fast adaptation of the dynamics of informational technology, in order to be able to provide a faster answer to new types of cyber attacks;

-transforming education in the filed of cyber security in a priority for European Union and for the Member States, in order to have the possibility to develop efficient preventive strategies;

-Cybersecurity efforts in the EU also involve the cyber defence dimension. To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyberdefence capability development should concentrate on detection, response and recovery from sophisticated cyber threats;

-Develop industrial and technological resources for cybersecurity;

-Promoting a Single Market for cybersecurity products - A high level of security can only be ensured if all in the value chain (e.g. equipment manufacturers, software developers, information society services providers) make security a priority.

-Promoting common efforts to increase the level of trust in cyber security using a policy based on transparency, responsibility and professionalism;

-Ensuring a better implementation of legal instruments of European Union in the filed o cybercrime and cyber security;

-developing common policies to support international exchange of information and cooperation for preventing, detecting and fighting cybercrime phenomenon thru the creation of an unique strategy and vision.

being highly tempting among forgers through the implied reduced complexity of counterfeiting.

**References & endnotes**

1. T.Newman, Research in cyberdomain, Springer, Paris, 2020, p.14-19.
2. G.Malloy, Practical opinions, University Press, NY, 2017, p.320.
3. X.Name, Name of the publication, Publishing house, year, pages.

1. Assoc.Proff., University Academy, 1A District Alley, District 1, New York, USA, name@gmail.com. [↑](#footnote-ref-1)
2. Head of the Research Center – Address etc., name @domain.com [↑](#footnote-ref-2)