Editorial

RAISA and IJISC - 5 Years in the Service of Cybersecurity Culture Dissemination

Ioan C. BACIVAROV

President of RAISA - Romanian Association for Information Security Assurance

"Cybersecurity must accommodate and address the needs of people through process and cultural change." [1]

1. *Information security* and *cybercrime* represent an area of global importance because the integration of information technology and communications infrastructure in the Internet is accompanied by risks of intrusion and information compromise.

Nowadays Internet is the world's largest collection of networks that reaches government institutes, commercial enterprises, universities, and research laboratories in all the countries. But along with easy access to information come new risks. The recent statistics demonstrated that the number of the attacks and the frauds on Internet is increasing fast [2].

The most recent *cybersecurity* alert was a global one, and has - once again - drawn attention to the global importance of this issue and the need to take effective actions to counter cyber-attacks.

Indeed, on May 2017, multiple companies and organizations around the world were hit by variations of a crypto-ransomware dubbed WannaCry / WannaCrypt / WanaCrypt0r / WCrypt / WCRY (generally called WannaCry for simplicity). The ransomware also acted as a worm and once it infects a system, it then self-propagates throughout the rest of the network. The ransomware campaign caused chaos due to its massive distribution, affecting more than 150 countries and infecting over 230,000 systems. Interestingly the attack was mounted on Friday 12th May 2017, just before the weekend, making it very difficult for companies and organizations to quickly react and resolve the crisis [3]. This important cybersecurity alert - both in scale and in its consequences - is part of a long series of IT security-related events and, once again, demonstrates the importance of the cybersecurity problem both nationally and globally.

Consequently, the necessity of *strong cybersecurity measures* is self-evident: the proliferation of cyber-attacks is causing increasing damage to companies, governments, and individuals. Hence the importance of the existence of associations and organizations involved in addressing the multiple security issues and, above all, in the development of a "cybersecurity culture". In this context, the establishment of **RAISA** - 5 years ago - appears to be very beneficial.

2. Indeed, 5 years ago, at the initiative of a group of enthusiastic and dedicated professionals to the IT security field from the EUROQUALROM laboratory of the Faculty of Electronics, Telecommunications and Information Technology of the University "Politehnica" of Bucharest and from the *Police Academy* "Alexandru Ioan *Cuza*" Bucharest was founded **the *Romanian Association for Information Security Assurance - RAISA***, a professional, non-governmental, non-partisan political, nonprofit and public benefit association.

The aim of the *Romanian Association for Information Security Assurance* was to promote and support the information security activities in compliance with applicable laws, and to create a community for the exchange of knowledge between specialists, academic and corporate environment in Romania, based on values as: (a) continuous investment in education; (b) openness to new methods to secure information; (c) involvement in combating the cybercrime phenomenon; (d) focus on facts; (e) concern for excellence.

The vision of RAISA was to promote research and education in information security field, to contribute to the creation and dissemination of knowledge and technology in this domain and to create a strong "cybersecurity culture" at national level.

3. *Cybersecurity* involves several different technical and informational solutions that must be adopted and implemented to position an organization for the greatest chance of resiliency in a complex threat landscape. Technology is certainly necessary in addressing cyber-threats, but it cannot work independent of complementary factors such as policy guidelines, information sharing on threats, and user awareness [4].

In the context of the recent global cyber-attacks, 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. Today, it is just as important to secure *human assets - layer 8 -* as it to secure layers 1 through 7 [5].

Consequently, is of crucial importance for all the countries, professional organizations, and companies to consolidate a powerful "*cybersecurity culture*". That's why, one of the most important objectives of RAISA during this five years beginning period was to build a "*cybersecurity culture*" in Romania.

Among the RAISA achievements aimed at implementing a culture of cybersecurity in our country, we can mention the following ones:

- Implementation of several ***RAISA web portals*** specialized in *IT security*, including: ***Information Security*** (*http://www.securitatea-informatiilor.ro/*), ***Cybercrime*** (*http://www.criminalitatea-informatica.ro/*), ***Cybersecurity*** (*http://www.securitatea-cibernetica.ro/*), ***Cyber Networks*** (*http://www.retele-cibernetice.ro/*); these web portals aim to make available to those interested in recent IT security information.

- Development of several successful ***RAISA research projects*** in the field, including the following ones: "*Scientific Research Promotion in Information Security Field*", "*Studies on implementing safety measures in order to ensure information security*", "*Protection of computer systems against cybercrime phenomenon*", "*Studies on modern methods of publishing information in online*

environment", "Analysis of computer networks. Architectures, equipment and protocols".

- Organization of several **RAISA workshops**, dedicated especially to young researches, engineers, MSc, and PhD students in IT field (especially in cybersecurity); we could mention among the interesting workshops which led to vivid debates the following ones: "*Methods for cyber-attacks investigation*" (December 2013), "*Access to education and information through Internet*" (May 2014), "*Information security in Office applications*" (May 2015), "*Promoting information in online environment*" (May 2016).
- Organization and coordination (by Prof. **Ioan Bacivarov**, PhD and Assoc. Prof. **I.C. Mihai**, PhD) of special sections/sessions on IT Security and Cybercrime at recent **international conferences & symposia** in the field, including the International Conference in Quality and Dependability - **CCF 2014** and **CCF 2016 (**Sessions *Dependability, Risk, Security)* or **eLearning and Software for Education Conference - eLSE 2017** (Workshop *Security Threats for eLearning Systems*).
- Support (organization of debates, specialized software, etc.) for the development of the Master "Quality and Dependability in Electronics and Telecommunications – ICSFET" from the Faculty of Electronics, Telecommunications and Information Technology, University Politehnica of Bucharest.
- Elaboration - by the key members of RAISA - of several books in this important domain; among the books published under the aegis of RAISA during the last years we could mention the following ones: I.C. Mihai, L. Giurea - *Cybercrime* (2nd ed., Sitech, 2014); I.C. Mihai, G. Petrică - *Information security* (2nd ed., Sitech, 2014); I.C. Mihai, G. Petrică, C. Ciuchi, and L. Giurea - *Cybersecurity Challenges and Strategies* (Sitech, 2015); A. Bacivarov, G. Petrică, C. Ciuchi - *Web programming. Applications in HTML, CSS, JavaScript* (MatrixRom, 2016).

4. Undoubtedly, one of the main achievements of the RAISA - the "crown pearl" of the association - is **IJISC** - the scientific journal that RAISA has decided to publish since 2012.

IJISC - the *International Journal of Information Security and Cybercrime [6]* is an international scientific peer-reviewed journal, aiming to bring together the latest high-level research and development in information security and the latest methods to prevent and to combat the cybercrime phenomenon.

The *Editorial Board* of **IJISC** includes specialists in information security and cybercrime from academic police structures and university departments, their activity taking place under the close guidance of an *International Scientific Board*, composed of internationally recognized personalities from the academic field.

In five years of existence, academics and researchers from 12 countries have chosen **IJISC** for the submission of their scientific papers and well-known professors and researchers from 12 countries have joined the *IJISC International Scientific Board*.

IJISC has grown tremendously over the last five years, in terms of both its academic quality and its international visibility. At this moment, **IJISC** is indexed in several *international databases* for scientific journals, including the following ones:

EBSCO*host*; Index Copernicus International; CEEOL (Central and Eastern European Online Library); Google Scholar; CrossRef; OCLC WorldCat; SCIPIO - Scientific Publishing & Information Online a.o. Permanent links to published papers are maintained by using the DOI - Digital Object Identifier system by CrossRef.

The *International Journal of Information Security and Cybercrime - IJISC* will carry its mission into the future, with the aims of enhancing the journal's scientific level and global impact, continuing to provide readers with access to high-quality research, strengthening its digital publication capabilities, and ultimately becoming a top international journal in the field of cybersecurity.

References:
[1]. Gartner press release, June 6, 2016.
[2]. I.C. Bacivarov, Editorial, International Journal of Information Security and Cybercrime - IJISC, vol. 1 (2012), no. 1, pp. 6-7.
[3]. https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst (accessed June 1st, 2017).
[4]. http://www.csoonline.com/article/2977014/security-awareness/cyber-security-culture-is-a-collective-effort.html (accessed June 1st, 2017).
[5]. https://securityintelligence.com/building-a-cybersecurity-culture-around-layer-8 (accessed June 1st, 2017).
[6]. https://www.ijisc.com/.