ASIGURAREA CALITĂȚII – QUALITY ASSURANCE
Octombrie – Decembrie 2016 Anul XXII Numărul 88

# Cybersecurity – A Major Issue of the 15th International Conference on Quality and Dependability CCF 2016

**Ioan C. BACIVAROV***

**Abstract**

*In the first part of this paper the concepts of **cybersecurity** and **cybercrime** and their importance are analyzed. It is underlined that cybersecurity is one of the biggest issues currently facing governments and businesses in the European Union (EU) and globally. In this context, a special attention is given to analysis of the European Cyber Security Strategy.*
*In the second part of the paper is underlined the fact that cybersecurity was one of the main topics of the 15th International Conference in Quality and Dependability – **CCF 2016**.*
*Based on the papers presented during **CCF 2016** one can conclude that one can speak of a "Romanian school in reliability field", whose achievements and representatives are recognized abroad. Judging after the papers presented by the PhD candidates in the field of cybersecurity during CCF2016, the future of this domain is "in good hands".*

***Keywords**: Cybersecurity, Cybercrime, IT security, Cyber Security Strategy, CCF2016, International Conference in Quality and Dependability*

**1.** *Cybersecurity* is – according to ITU-T X.1205 – the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

*Cybersecurity* is one of the biggest issues currently facing governments and businesses in the European Union (EU) and globally: it is important to mention that the European Union works on several fronts to ensure cybersecurity in Europe [1] [2].

The European Commission and High Representative's *2013 Cyber Security Strategy* was the first comprehensive policy document of the European Union in this area. This Strategy covered the internal market, justice and home affairs and foreign policy angles of cyberspace. The Strategy was accompanied by a legislative proposal to strengthen the security of the EU's information systems.

The Strategy outlined the priorities for the international cyberspace policy of the European Union [3]:

- Freedom and openness: the strategy outlines the vision and principles on applying core EU values and fundamental rights in cyberspace.
- The EU's laws, norms and core values apply as much in cyberspace as in the physical world: responsibility for a more secure cyberspace lies with all players within the global information society, from citizens to governments.
- Developing cyber security capacity building: the EU engages with international partners and organisations, the private sector and civil society to support global capacity building in third countries. This includes improving access to information and to an open internet, and preventing cyber threats.
- Fostering international cooperation in cyberspace: preserving open, free and secure cyberspace is a global challenge, which the EU is addressing together with relevant international partners and organisations, the private sector and civil society.

Another important for step in the process of EU's cybersecurity assurance was the adoption by the European Parliament of a proposal for a *Network and Information Security Directive* (*NIS Directive*) in March 2014 [4].

* Correspondence to Prof. **Ioan C. Bacivarov**, PhD, Scientific Chairman of the *15th International Conference in Quality and Dependability – **CCF 2016**,* e-mail: **bacivaro@euroqual.pub.ro**.

**2**. *Cybersecurity* represent an area of international 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 number of the attacks and the frauds on Internet is increasing fast.

*Cybersecurity* seeks to thwart intruders through hardware and software devices that are independent of the domain of the application or system being protected. Software security methods like authentication, access control, cryptography, antivirus, firewalls and other mechanisms used in computer security are meant to protect an underlying application by Internet attacks. Cybersecurity is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.

Three basic security concepts are important to information on the Internet: confidentiality, integrity, and availability. When information is read or copied by someone not authorized to do so, the result is a loss of confidentiality. If information is modified in n unexpected ways, the result is known as loss of integrity. Information can be erased or become inaccessible, resulting in loss of availability. While computer security has been focused on these three concepts for information, the problems of greatest concern today relate to the systems mission and the continuity of services. The new concept of survivability can be defined as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures or accidents. Survivability has a very sharp mission focus: the system mission has to survive, not any particular component of the system or even the system itself. The mission must go on even if an attack causes significant damage to or even destruction of the system that supports the mission.


**Professors Alessandro Birolini and Ioan Bacivarov were the coordinators of the plenary session "*Risk and IT Security*" during CCF 2016**

**Professors Alessandro Birolini, Angelica Bacivarov and Ioan Bacivarov together with PhD candidates in cybersecurity during CCF 2016**

**3.** *Cybercrime* refers to any crime that involves a computer system or a computer network. A computer can be used in the act of a crime or may be the target to an attacker. It is difficult to characterize the people who cause incidents. An intruder may be an adolescent who is curious about what he can do on the Internet, a student who has created a new software tool, an individual seeking personal gain or a paid person seeking information for the economic advantage of a corporation or a foreign country. An intruder may seek entertainment, intellectual challenge, political attention or financial gain. Intruders identify and publicize misconfigured systems; they use those systems to exchange pirated software, credit card numbers, exploitation programs and the identity of sites that have been compromised, including account names and passwords. By sharing knowledge and software tools, successful intruders increase their number and their impact.

In the context of the vulnerabilities and incident trends, developing a scientific journal for information security and cybercrime research is necessary. A robust defense requires many researches in this field that allows adaptation to the changing environment, well-defined policies and procedures, the use of different security tools to prevent and combat cybercrime.

**4.** The primary objective of the ***15th International Conference on Quality and Dependability*** **CCF 2016** *– a jubilee edition –* was to provide an international forum for the dissemination of recent information and scientific results in the modern domains of quality and dependability.

Cybersecurity was one of the main topics of the *15th International Conference in Quality and Dependability* [5].

In the frame of CCF 2016, 12 papers in the field of cybersecurity were presented.

Most have been included in the plenary session "*Risk and IT Security*", coordinated by Prof. Emeritus Dr. **Alessandro Birolini** from ETH Zurich, Switzerland and by Prof. Dr. **Ioan Bacivarov** – director of EUROQUALROM-ETTI – UPB and President of the Romanian Association for Information Security Assurance (RAISA). Some were included in the poster session "*Dependability*" mediated by Prof. Ioan Bacivarov, too.

In this context it should be mentioned the excellent conference "*Risk management in technical systems*" presented by Professor **Alessandro Birolini**, special guest of **CCF 2016**, considered as a "guru" of the European reliability.

Most presentations in the field of cybersecurity were made by Professor **Ioan Bacivarov** and his collaborators – PhD candidates in cybersecurity.

As a conclusion of the debates, Professor Birolini pointed out that one can speak of a "*Romanian school in reliability field*", whose achievements and representatives are recognized abroad; and judging after the papers presented by the PhD candidates in the field of cybersecurity during CCF2016, the future of this domain is "in good hands".

Extended versions of some representative papers in the field of cybersecurity presented during the **CCF 2016** will be included in this issue (as well as in future ones) of the journal "***Asigurarea Calității – Quality Assurance***" dedicated to the *15th International Conference in Quality and Dependability*.

The international journal "***Asigurarea Calității – Quality Assurance***" will continue to analyze in the future the *cybersecurity* phenomenon in all its complexity.

**REFERENCES**

[1] I. Bacivarov, A Regional Strategy for Cybersecurity, Editorial, *International Journal of Information Security and Cybercrime* , vol. 4 (2015), no. 1, pp. 5-8.
[2] **http://www.computerweekly.com/opinion/What-to-expect-from-European-NIS-Directive**.
[3] *** European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013) 1 final.
[4] **http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis**.
[5] D. Stoichițoiu, I. Bacivarov (Eds) Advances in Quality and Dependability, *Proceedings of the 15th International Conference on Quality and Dependability* **CCF2016,** SRAC, 2016.