Editorial

Professor **Ioan BACIVAROV**, PhD
Faculty of Electronics, Telecommunications and Information Technology
University POLITEHNICA of Bucharest, Romania

International Journal of Information Security and Cybercrime – **IJISC** is a collection of scientific researches in a sensitive domain, which represents a priority at global level.

Information security and cybercrime 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.

Computer security 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. Computer security 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 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.

Cybercrime refers to any crime that involve 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.

The purpose of *International Journal of Information Security and Cybercrime –* **IJISC** is to analyze information, computers and communications security and to identify new valences of cybercrime phenomenon.

The journal has four sections:
1. Advances in Information Security Research;
2. Studies and Analysis of Cybercrime Phenomenon;
3. Cyber-Attacks Evolution and Cybercrime Trends;
4. Books Review and Conferences Analysis

The *International Journal of Information Security and Cybercrime –* **IJISC** is a peer reviewed interdisciplinary journal published biannually. The journal publishes theoretical, methodological, and applied papers, as well as book reviews and conference analyses in the above mentioned areas.

Through the theoretical and practical addressed issues, the target of **IJISC** are the experts from information security or cybercrime field, graduate and postgraduate students, as well as all the people interested to improve or to update their knowledge in this domain.

The Editors of **IJISC** are specialists in information security and cybercrime, their work taking place under the close guidance of a Scientific Council, composed of internationally recognized personalities of the domain from the academic field.

We hope that this new editorial approach will attract experts, academics and researchers working in the important area of information security and cybercrime, so that the topics discussed in **IJISC** will offer theoretical and practical solutions for information security and cybercrime combat.