Editorial

2020 - New Challenges, New Approaches. A New (Re)Start?

Gabriel PETRICĂ
Faculty of ETTI, University POLITEHNICA of Bucharest, Romania

According to the DIKW pyramid[1], information is the basis of knowledge, and knowledge brings wisdom, but also economic development, financial prosperity, power, and influence. Information is in everything around us; it becomes of vital importance not only for the user himself, but also for the entities to which he belongs (LANs, companies, etc.) and for the devices with which he interacts.

In order to not be used for destructive purposes, against users or the components of the surrounding ecosystem (equipment, policies, documents), the information must have adequate protection, both at software and hardware level. The permanent assurance of the three requirements - confidentiality, integrity and availability - which according to ISO / IEC 27000 are fundamental objectives of information security, are considered the true foundation against current cyber-attacks.

The concept of security has a broad definition and multiple areas of applicability. Security is closely related to information because the security involves keeping data / objects safe, intact. As the amount of information increases and the techniques for accessing it become more varied, new more risks arise, for which control and protection methods must be developed. Cyber security is a dynamic field, with permanent challenges, being considered in the Global Risk Report of the World Economic Forum as the most important aspect in 2020 from technological point of view[2]. But the main factor in ensuring security, both at data, computer and network level, remains the human factor. No matter how advanced a security system is, it can always be combated by the human factor through an optimal combination of creativity and intelligence.

Introduced in 2015 by Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, the term “Fourth Industrial Revolution” (4IR) refers to technologies that combine hardware, software, and biology (cyber-physical systems) based on advances in telecommunications and connectivity. The need to process a large amounts of data has led to an evolution of digital technologies and the emergence of modern mechanisms in areas such as robotics, artificial intelligence, nanotechnology, quantum computing, biotechnology, IoT (Internet of Things), IIoT (Industrial IoT), decentralized

[1] J. Rowley, The wisdom hierarchy: representations of the DIKW hierarchy, Journal of Information Science, 33, 2007, pp.163-180.

[2] World Economic Forum, The Global Risks Report 2020, http://www3.weforum.org.

consensus technologies (blockchain), wireless technologies and 5G networks, 3D printing, fully autonomous vehicles, cloud computing services, big data analysis and processing using artificial intelligence.

The objectives to which the current information society is heading are represented by the storage and data processing in cloud, but also by the accelerated development of the IoT concept. The main security issues related to cloud computing are poor access management, security breaches, data loss, unsecured APIs (Application Program Interface) and DoS (Denial of Service) attacks. As the number of IoT devices connected to the Internet increases (estimated to reach 21.5 billion by 2025[3]), so does the amount and variety of digital assets that are stored, processed and shared by organizations. At the same time, IoT amplifies the potential surface of cyber-attacks, as we find IoT devices in various gadgets, cars, smart homes and cities, or industrial equipment. Classic phishing, scamming or social engineering attacks launched via e-mail or Web will continue to exist, but new hardware / software technologies, which come with high, updated performances, also bring specific vulnerabilities, which developers and specialists will have to address.

4IR-specific technologies, through their development requirements such as increased security, minimizing response latency, large amounts of transmitted / received data and increased bandwidth, will consistently reshape economies and societies. However, these technologies are not only seen from the perspective of technological progress but have the leading role of orienting towards changing the way different related products and services are designed, produced and marketed, as well as the way a number of benefits are obtained from these.

For a prompt and optimal use of these digital opportunities, the European Commission proposed in 2015 an ambitious strategy: to establish a digital, free and secure single market. This will ensure the long-term competitiveness of the European continent, which will have implications for the general well-being and ensure faster economic growth in the digital management sector. On 9 June 2020, the Council adopted conclusions addressing a wide range of issues related to the implementation of the EU's digital strategy. Areas covered by the findings include connectivity, data economy, artificial intelligence, and digital platforms[4]. In order to benefit from the advantages of the digital single market, there is a need to continuously improve the quality and security of IT systems and mobile communications equipment. Investments in these two directions, together with increasing the level of digital skills of users, must be permanently supported, representing the key to ensuring a real progress and achieving high competitiveness.

The first part of 2020 brought a new global challenge - the coronavirus pandemic - and radical changes in approaches at all levels of activity (health, education, tourism, business, etc.) and in human behavior. The complex situation of the moment has already highlighted the impact and role of digital technologies in combating the pandemic. We will see whether 2020 can be considered a reference year in the evolution of the human species, a (re)start to which modern technologies will contribute substantially to the recovery of societies following the crisis caused by COVID-19.

[3] Statista, Internet of Things (IoT) - Statistics & Facts, https://www.statista.com/topics/2637/internet-of-things/

[4] https://www.consilium.europa.eu/ro/policies/digital-single-market/