43 Review of the Monograph on 'Information – Society – Security'

Zsolt Haig: Információ – társadalom – biztonság

Árpád Varga[*]

Although the definition of the words information, society and security can fill many pages in encyclopaedias, the author has created a unique monograph on the complexity of info-communication technologies. Prof Dr. (Col.) Zsolt Haig has already established himself in scholarship with two decades of publications including several university coursebooks, yet this book fills the gaping niche in Hungarian scientific literature on information technology-controlled attacks.

It is now evident, that our globalised society has to struggle with new waves of security holes. As all modern infrastructures are converted into computer controlled systems, both legal and practical knowledge needs to be transposed into the modern network-based communication context. The author of the book sought to combine these separate areas by depicting the operational background of the potential offences against critical infrastructures and referring to relevant national and global legislative trends. As a military colonel, the author's main purpose was to map the conditions of and strategies for Hungarian cyber security.

In the first few pages the theoretical basis of the monograph is laid out, tracing the sectorial changes that took place in the 20th century. According to Zsolt Haig, besides the three basic sectors of the economy, info-communication inventions – computers, super computers, industrial robots etc. – created their own sector, resulting in the so called "knowledge-society". In this technical age the most valuable products are information, data and science.

This new society then started to go through three different phases, from the establishment of telecommunication networks, through societies' adaptation to them, to the creation of highly defensive information security. Hungary is still trailing behind in implementing the first two phases, these phases must be completed first, before we can guarantee the security of our infrastructure – so the author.

This view is shared by renown sociologists such as Daniel Bell and Alvin Toffler, whose information society theories changed the governing mindset of the 1970's. Today we can

* Research fellow, Institute for Media Studies of the Media Council, Budapest, arpad.varga@mtmi.hu.

also discern other perspectives such as the one proposed by Manuel Castells', who established the so-called "Network Society" theory, which is more like the redefinition of the industrial economies.

Although the theoretical roots of technical development are diverse, the aim is the same: to define the legal and practical boundaries; to detect the vulnerabilities and malfunctions of critical infrastructures. From this perspective the book has the ambition of answering both theoretical and IT related questions regarding Hungary's cyber security parameters.

Among others the author devotes a whole chapter to long term strategies and professional concepts. Hungary started digitalisation back in 1995, and approved more than fifteen documents to modernise the society, introduce e-government, broadband internet connection and the digital literacy. The most interesting paper is the Digital Agenda for Europe which is part of the Europe 2020 Strategy. In Chapter two a Hungarian Action plan attached to the EU directive is introduced comparing the domestic situation with tendencies in the European Union as a whole. According to the data analysis Hungary lags behind other countries, especially from the aspect of e-commerce: Hungary scored 17% in 2013, while in the same year the European average almost reached 40%.

Besides referring to sociological foundations, the book draws attention to the complexity of critical info-communication infrastructures. The thesis emphasises the weaknesses of all countries' infrastructure, since Internet Protocol (IP) based systems globally include computer networks, cell phone communication, and wireless internet connection. According to the author this interdependency gives rise to vulnerabilities on the side of hospitals, governmental organisations, public transportation, financial services etc. Information technology-controlled attacks are perpetrated in order to – temporarily or permanently – paralyze these vital systems and disrupt the civil society's sense of security.

The author also distinguishes between internal and external threats. The first available defence line is to preserve information within the infrastructure, since many attacks are connected to low computer skills or negligence. This means that external attacks can be supported without negligent human conduct.

The aim of all states is to achieve superiority in collecting and analysing information and to be able to predict military action plans and to influence the decision making of governmental and operative participants. In general, the drive of informational operations is the synergy of conventional and modern strategies. Prof. Haig draws attention to the tendency of higher compatibility among electronic appliances, which lower the defence capacity in cyber space – for example, encryption and jamming devices can be disabled through info-communication networks.

Today, when terrorists play their own part in global communication it is important to mention the issue of cyber terrorism. Hungary is not a direct target of such assaults, yet all the democratic countries have to be aware of and be prepared for terrorist attacks. It is

overwhelming to see the consequences of terrorist activity in the physical form, but governments also need to prevent all propaganda activity in order to shut down recruitment on online networks. Although experts state that cyber terrorism is not a relevant threat, such illegal activities have the potential to expand and erupt in a state-wide infrastructure crisis.

The book also provides a unique insight into EU and NATO cyber security policy put in place following the September 11 attacks. The author refers to all relevant treaties and declarations in order to substantiate that the global tendency of modernisation was mainly motivated by unpredictable future offences. Both organisations started to set up their defence plans to prevent such attacks and established branches like the CIWIN[1] or the CCDCOE.[2] As Prof. Haig points out, these incident response systems are the first, but not the most effective solutions to the general problem. He emphasises that all actors need to define the criteria of the various offences and maintain an organizational unit based on confidentiality, integrity and availability. On the other hand the existing units are compelled to deal with forensic issues including the identification of the perpetrator, the modus operandi of the penetration or the selection of necessary and sufficient retaliation. One of the available opportunities the author suggests, is to re-enact previous incidents such as the Estonian cyberattacks of 2007.

As the author summarizes, in a first step, governments and societies must be prepared for cyber threats, but cyber security law and organisations must also be constantly improved and modernized in order to effectively combat illegal activities.

In summary, this book provides the reader with fundamental knowledge on information technology-related theories, infrastructures, systems, vulnerabilities and even the relevant legal environment. Although the author devoted many pages to technical and strategic issues, it is easy to follow his train of thought, rendering the reader familiar with a lesser known part of a professional discourse. This book is an excellent choice for inquisitive sociologists, military engineers and jurists etc., who are dedicated to information technology issues. Furthermore, the book could also help politicians in finding the best solutions when framing nationwide info-communication technology and cyber security policies.

1 Critical Infrastructure Warning Information Network.

2 Cooperative Cyber Defence Centre of Excellence.