ECONOMY AND FINANCE • VOL. 12 • ISS. 4 • DEC. 2025 • DOI: 10.33908/EF.2025.4.8

BOOK REVIEWS

Elemér Terták – Levente Kovács
CYBERSECURITY – CYBERSPACE

Budapest, 2025
Hungarian Banking Association

The rapid development of digital technologies has redefined the operation of the economy globally and nationally. For effective cyber defence, up-to-date and high-quality knowledge is essential. Today, the issue of cybersecurity is not simply an IT concern, but a cornerstone of economic and financial stability, social trust and national security. The volume *Cybersecurity – Cyberspace*, co-authored by Elemér Terták and Levente Kovács and published by the Hungarian Banking Association, pursues a scholarly yet accessible presentation of these complex processes.

The two authors have extensive expertise in the operation of the Hungarian and international banking system, financial regulation and the development of innovative financial services. *Levente Kovács* is Secretary General of the Hungarian Banking Association, Professor, Head of Department and core member of the Doctoral School of the Faculty of Economics at the University of Miskolc. He contributes to several scientific journals as member of the editorial board as part of his scholarly activity. Previously, he was Deputy CEO of the Korean KDB Bank, and between 2002 and 2006, he was Managing Director of Development and then Business Director of GIRO Elszámolásforgalmi Zrt. *Elemér Terták* is currently Member of the Board of the Hungarian Economic Association. During his career, he was CEO and Chairman of the Board of Directors of the largest Hungarian bank, OTP Bank Rt. between 1990 and 1992, and later Chairman of the Supervisory Board of K&H Bank and Director of the Directorate–General for the Internal Market and Services of the European Commission.

The aim of the authors is to provide readers with a systematic yet accessible presentation of the technological, economic and criminal dimensions of the operation of cyberspace through the lens of the financial sector while using an interdisciplinary approach.

Several sectors of the economy have seen major innovations in recent years, due mainly to the spread of the Internet and digital technologies, lowering barriers to

entry, decreasing start-up and operative costs in electronic business models and changing consumer habits. A series of paradigm shifts has swept through accommodation services, advertising, music, and finance, and existing business models have often been replaced by new, digital ones.

Cybersecurity and cyber defence are one of the most pressing challenges of our time from the perspective of individuals, society, public institutions, public services and businesses alike. One of the most striking phenomena over recent years is undoubtedly the appearance and growing prevalence of large-scale cybercrime as criminals are abusing technology to the detriment of unsuspecting and careless victims.

Authors Elemér Terták and Levente Kovács clearly had broad practical application in mind when writing *Cybersecurity – Cyberspace*. As professional reviewer of the volume, I had the chance to get a direct insight into a final stage of the working process.

A main observation of the volume is that the legal system's response to ongoing developments is consistently delayed. Therefore, effective law enforcement in cyberspace is significantly lagging behind while cybercriminals, by constantly adapting to technological advances, enrich themselves at the expense of others.

The volume comprises 8 chapters on 206 pages, including 24 tables and 12 figures.

A major strength is the historical overview offered on the evolution of cybercrime. The authors trace the history of criminal activity in cyberspace from the hacking of France's telegraph system in 1834 up to the most complex state-funded cyber attack of the 21st century.

Cybercrime is defined as a 'trillion-dollar industry', characterised by specialisation and task distribution among criminals ranging from lone hackers to state-funded cybergroups. The authors highlight that digitalisation has enabled criminal acts to become impersonal, and as the distance between criminals and their victims lifts the psychological barrier of guilt, the risk and prevalence of crime increases.

A central message of the volume is that cybersecurity is not simply a matter of technical protection but a systematic security challenge affecting many subsystems of society. One focus area of the authors is – quite rightly – the financial sector, which, as an early adopter of digitalisation, is highly prone to its risks. Attacks against banking infrastructures not only cause financial losses but also undermine clients' trust and the stability of the financial system.

A separate chapter is dedicated to international cybersecurity cooperation frameworks, outlining the Budapest convention and its importance. Readers are provided with extensive statistical data and information on cybercrime trends. The

chapter on cyber loss has the dual objective of calling attention to both the scarcity of reliable data and the lack of uniform definitions in cybersecurity.

It is important to clarify that there are two kinds of insurance available against cyber threats. One is for financial risks, insuring businesses against losses incurred in the online space and also against most losses due to malfunctions in software or infrastructure. Liability coverage is the other option.

The volume also includes an encyclopaedic compilation of cyber defence concepts and phenomena, complete with definitions and explanations. At the time of its compilation – and also the publication of this review – the cybersecurity glossary contained 111 core cyber-related concepts and the English equivalents for 33 Hungarian terms, providing a necessary reference for those interested in, or working within, the fields of cyber defence and cybersecurity to navigate this evolving domain[1].

The authors argue that since cybersecurity is a global phenomenon, knowledge of the international terminology is indispensable for coherence in professional communication.

The volume *Cybersecurity – Cyberspace* fills a gap in the Hungarian literature on cybersecurity. Its interdisciplinary approach – considering technological, economic and social implications alike – provides readers with a comprehensive view of the dynamic and precarious world of cyberspace. It is a scholarly yet accessible work on the security dilemmas of the digital age, also offering practical guidance on the management of risks.

It is a recommended read for IT professionals, economists, bankers, academics, researchers and policy decision makers to conceptualise the issue of cybersecurity within the broader context of economic and social modernisation.

The authors conclude from everyday experience that while service providers, bodies of national security and the media can – and do in fact – contribute significantly to strengthening security in cyberspace, it is users who can do even more by engaging in online transactions with care and circumspection, not succumbing to tempting but treacherous advertisements, updating their software regularly and not sharing their sensitive data carelessly with strangers. The principal audience of this work are users, for whom the authors seek to facilitate preparedness in protecting their personal and financial security by disseminating professional knowledge and outlining both cybercriminal practices and viable defences.

1 The glossary was published separately in Issue 3/2025 of Economy and Finance, where the authors also indicated that the glossary is to be continuously expanded and updated in electronic format, expected to be available at www.kiberpajzs.hu.

In addition to professionals and leaders in finance and banking, I recommend this work without any second thought to the broader public, or even as a textbook or handbook, as it is an outstanding summary of essential cybersecurity-related information.

Ádám Kerényi[2]

2 Ádám Kerényi, Research Fellow, ELTE Centre for Social Sciences. E-mail: kerenyi.adam@elte.tk.hu.