some original, interesting ideas, worthily to be considered and that might contribute to these evolutions in a constructive manner.

Artur Lakatos

***Homeland Security. Threats, Countermeasures, and Privacy Issues* (ed. by Giorgio Franceschetti, Marina Grossi), Boston-London, Artechhouse Publishers, 2011, 254 p.**

This book is practically a collection of studies, based on the works of International Workshop on Homeland Security, held in Italy to the end of September 2009. In the same time, the book is not intended to represents only the simple proceedings of the workshop, but by a unified, updated structure, a complete synthesis of the issue of what homeland security means nowadays.

The book is structured on 13 chapters, each of them having in its composition several subchapters, which are dealing with a concept or a particular case-study on their turn. The first chapter, "The New Vision of the Homeland Security Scenario", represents practically the introduction in the wider problematic, by presenting a brief history of homeland security challenges, illustrated by several case-studies like the Tokyo chemical attack, London bombings by Al-Qaeda, or the Beslan hostage crisis until seemingly banal, but basically very serious threats like Vandal cut of cables or computer worms. The whole chapter is focused upon the idea of scenario, or, according to the use of the authors, the Homeland Security (HS) Scenario. Chapter two, "Homeland Security and National defense in the Twenty-First Century", deals with some even deeper aspects of HS Scenario, applied to post-Cold War realities. Threat- and risk- counterfeiting scenarios are designed to general characteristics of these relations, defined by the authors as "New World", which is based on a thesis according to which after the fall of the Berlin Wall the global political landscape evolved into a new equilibrium, characterized especially by regional balances of powers, a new system in which some are stronger than others, but no one is invulnerable. At the end of the chapter, a case-study of possible implementation of the so-called network-Enabled Capability (NEC) in Italy is presented.

Chapter three, "Homeland Security and Challenges in Information Systems" has the features of a synthesis, by presenting an overview of currently existing information- and communication technologies, with all of their strong and weak points, complexities and vulnerabilities. The two case studies are represented by advantages and vulnerability of internet banking, and by brief presentation of the Parsifal project of the European Union. The next chapter, "Analysis of Emerging Phenomena in Large Complex Systems" represents a managerial-philosophical approach, which has the definition of system as base of the analysis. It deals with theory, applications, and examples of various organizations, heavily illustrated with mathematical calculations and tables and other figures common to statistics.

According to the authors, "the chapter attempts to clarify the emergent aspects of this new Science of complexity, in relation to the large systems operating in the domains of HS and homeland Defense (HD)".

The chapter entitled "Model-Based Design of trustworthy Health Information Systems" represents an incursion into management of sanitary systems, having a particular accent on patient-centered clinical information management and on information flowing inside of the systems specific to healthcare industry. "Urban defense Using Mobile Sensor Platforms: Surveillance, protection and Privacy" deals with the issue of security in urban areas, giving a special importance to the role of video cameras, static or mobile. "Detection and Identification of Dangerous Materials for Airport Security", written by three Italian practicing experts, introduces the reader into the world of airport security measures, which are more complex and more difficult to refer to as it seems to be at first sight, both from the point of view of personnel activity and of technology. "Privacy Versus Security: A Fight that May Turn into an Alliance" deals with the recently debated issue of personal privacy, whose relevance in the HS scenario is increasing, and it is often a concept opposed – in theoretical and practical debates – to the concept of security: for performing a working security, nowadays often privacy has to be violated by authorities. The chapter concludes that privacy is a basic value of our society and shares the same need of protection as security and safety, along the same lines of implementation, and also offers a new model, the so-called archetypal approach, which is aimed to be a new standard of public-private relationship for the sake of social security. The ninth chapter, edited by Stephen B. Wicker, "Privacy-Aware Design for the Monitoring, Control and Protection of Critical Infrastructure", deals with the potential of sensing systems in protecting critical infrastructures, even on the level of a typical household. Chapter 10, "Military Defense, Civil Defense, and Civil Protection Integration in a Multiscenario Crisis Event", signed by Robert Mugavero, approaches the field of international relations, by describing the experience – in which the author was personally involved in – of organizing and managing the security of the G8 Summit 2009, which took place in the city of L'Aquila, Italy. The last chapter, "Repel Borders!" has as subject the Piracy scenario, and the systems of measures to combat it, using as case study the recently designed POMPEIUS antipiracy system. There are no general conclusions at the end: every single chapter, designed to be as an independent unit from the others, has on its own conclusions to the end of it.

By reading this book, one could be impressed by its multidisciplinarity and by the manner in which it attempts to offer a complex image of what the term 'security' means nowadays.

Artur Lakatos