Foreword

People are fascinated by the convenience brought by the Information and Communication Technologies (ICT), adopting them quickly and moving to a state of mind where those technologies are indispensable. But the price of that convenience is an increased cyber-vulnerability, often lurking in the background and becoming visible only when it is too late. For example, it is convenient to store our files in the cloud, as we can access them from anywhere and their backup is seamless; however, this makes them potentially accessible or alterable by an unauthorized person. As another example, it is convenient to be able to reconfigure the elements of the power grid through a remote access; however, this also makes it vulnerable to new types of attacks that can hijack the remote access opportunity and cause parts of the grid to exhibit unwanted and harmful behavior. In short, every new connected entity and Internet service brings new quality and convenience, but at the same time it opens the possibility for a new cyber threat.

This is a timely book that provides a multifaceted treatment of the problems related to cyber threats and their countermeasures in today’s connected society. The book consists of articles written by professionals and researchers with various backgrounds, including military, ICT and legal and thus bringing a diversified view on the subject. The book consists of two parts. The first part treats the cyber threats towards the civil society. The articles in this part analyze the nature of these threats, provide parallels with the traditional crime and warfare, while several articles discuss the attacks and security breaches that are immanent to the cyber world. The second part of the book is dedicated to the means and strategies for achieving resilience towards cyber attacks and warfare. Resilience is elaborated in different context, such as, among others: national cyber-defense, relation to human behavior, dealing with unconventional forms of cyber warfare, law enforcement and protection of the critical infrastructure.

This book brings to the reader the state-of-the-art developments in the area of cyber threats and warfare, as well as the aspects of achieving resilience to those threats. One of the main message that can be sublimed by the diversified views on the subject is that the resilience from the cyber threats is a complex endeavor that pervades the whole society and can be achieved by proper policies and governmental actions that engage various parts of the society. It is therefore a valuable source for any reader that aims to understand the problem of cyber threats and warfare in a context that is broader than her area of expertise.

Petar Popovski
Aalborg University, Denmark
Foreword

Petar Popovski is a Professor in wireless communications at Aalborg University, Denmark. He received Dipl.-Ing. in electrical engineering (1997) and Magister Ing. in communication engineering (2000) from Sts. Cyril and Methodius University, Skopje, Macedonia, and Ph.D. from Aalborg University in 2004. He leads a research group on machine-to-machine communications. He has more than 200 scientific publications and more than 30 patents and patent applications. In 2015 he received the Consolidator Grant from the European Research Council. He is currently an Editor for IEEE Transactions on Communications, a Steering Committee member for IEEE Internet of Things Journal, and a Steering committee member of IEEE SmartGridComm. His research interests are in the broad area of wireless communication and networking, communication and information theory.