

Preface

The world is facing new challenges in all aspects of business involving the geopolitical and military environment. Religious radicalization, arm races, refugees' movements, global cyberattacks and terrorist attacks are some of these challenges. To be able to operate in such a volatile environment, various government agencies and organizations, including the department of defense, homeland security and intelligent services, as well as surveillance and security businesses, attempt to gain a tactical advantage to mitigate challenges or to make smart decisions, by collecting and processing all sources of important information relevant to their mission. On the one hand, smart phones, smart watches and in general smart devices, including surveillance sensors and on the other online social network platforms, have become the main vehicles to collect surveillance in action information.

Governments, especially after 9/11, started running intensive surveillance programs intending to identify potential terrorist threats. At the same time, companies use data collected through various devices or sensors in order to understand customer behavior, and tune it to improve security and protect their interests. Traditional sources of information are also used by various parties to acquire strategic knowledge against their competitors. As a result, there is an increased need for novel methods of surveillance that can be adapted to the new and dynamic military and civilian environment of the modern world.

In this context, the book attempts to address the aforementioned needs by presenting novel research by different experts around the world in the areas of military, civil, and cyber surveillance. The book is organized into three parts (themes) that present the current trends and novel techniques in the areas of (i) surveillance of human features, (ii) surveillance for security and defense and (iii) cyber surveillance.

In the first part of our book, *Surveillance of Human Features*, the contributors review surveillance systems that use biometric technologies. They propose various novel approaches that cover different topics such as gait recognition, facial soft biometrics, face-based physiology, face recognition using frontal and profile images, cross-spectral iris recognition or examine the facial characteristics in the visible

or in different bands and wavelengths of the infrared (IR) spectrum for the purpose of improving recognition performance.

The second part of our book, *Surveillance for Security and Defense*, summarizes mainly surveillance techniques used by the army and secret services. It also discusses the ethical issues raised by the use of surveillance systems in the name of counterterrorism and security. More specifically, the different generations of satellite surveillance systems are presented and the requirements for real-time satellite surveillance for military use are described. The new standards of surveillance using Unmanned Air Vehicles (UAVs) and drones are explored. Then, novel surveillance techniques are proposed in order to detect stealth aircrafts and drones. Due to the increase of cross-border terrorist threats, the book contributors highlight novel techniques for maritime border surveillance, bio-warfare and bioterrorism detection. Next, the way that intelligence services operate and use surveillance in the new era of social media is explored and, finally, the right and conditions under which the governments need to use surveillance technologies is discussed.

The last part of the book is *Cyber Surveillance*. It focuses on a series of computational techniques that can be used for cyber surveillance. First, a review of data hiding techniques that are used to hinder electronic surveillance is provided. Then, novel methods to collect and analyze information by social media sites (such as Twitter or other organizational communication systems) are presented. The focus is to discuss approaches capable to detect inside and outside threats by different individuals such as spammers, cybercriminals, suspicious users or extremists in general. Finally, the third part of our book concludes by examining how high performance environments can be exploited by malicious users and what surveillance methods need to be put in place to protect this valuable infrastructure.

We hope this book can become a reference work for military and law enforcement personnel using surveillance-related technologies, as well as researchers (academic or not), Masters and Ph.D. students who want to focus in the area of surveillance technologies and want to be updated with the current developments in the area of military, civilian, and cyber surveillance. Finally, we would like to thank all the contributors of the book for the high-quality work they have submitted to us and their support in the coordination of this publication.

Dekelia Air Base, Attica, Greece
Morgantown, WV, USA

Panagiotis Karampelas
Thirimachos Bourlai

Surveillance in Action

Technologies for Civilian, Military and Cyber Surveillance

Karampelas, P.; Bourlai, T. (Eds.)

2018, XIV, 412 p. 149 illus., 128 illus. in color.,

Hardcover

ISBN: 978-3-319-68532-8