Chapter 1
New Dimensions of Information Warfare

Since the dawn of humanity, the progress machine tirelessly introduced tools and resources that facilitated our everyday tasks. Over the years, new technologies have continually changed society with novel discoveries and inventions that proved capable of greatly improving human life. Historically, many of the processes that radically changed human lifestyle occurred gradually. However, in the past few decades, modern technology has enabled a fast and radical change of our society, modifying our habits, production means, and in some cases the very essence of work, through the widespread adoption of a plethora of new devices comprising smartphones, voice assistants, chatbots, and smartwatches that made our lives faster, easier, and funnier. Technology is also introducing new habits and addictions, changing every aspect of our society such as personal interactions, education, communication, financial services, physical goods production, logistics, and entertainment. This is happening in parallel with a wild race to the digitization of information.

Nowadays, an increasingly large share of our daily activities are performed with the help of digital devices, offering us a huge number of different Web-based services through which we manage every aspect of our lives. These services help us to learn, have fun, fulfill our work-related tasks, pay bills and manage our bank accounts, communicate with distant friends and meet with new ones, handle personal agenda, and buy items and services. On the one hand, such technologies guarantee access to a boundless range of services and information, to anyone and at any time. On the other hand, they allow service providers to access an equally boundless quantity of personal information, which are often harvested (and employed) without user awareness, let alone its consent. For instance, think of the rise of Online Social Networks: it has led to a new information ecosystem that prefers speed and immediacy to accuracy, trustworthiness, and reliability. As Meglena Kuneva brilliantly foresaw in a famous keynote speech at the European Commission in 2009—"Personal data is the new oil of the Internet and the new currency of the digital world"—we live in an era where wealth is directly linked

R. Di Pietro et al., *New Dimensions of Information Warfare*, Advances in
Information Security 84, https://doi.org/10.1007/978-3-030-60618-3_1

to the available information [1]. Within this context, Online Social Networks represent the new gold mines. Gold mines in which every technologically savvy actor can freely dig its nuggets. Digital breadcrumbs left by our daily activities thus represent a tempting opportunity for different actors—such as governments, advertising companies, state-backed organizations, hackers—opening up scenarios that would have been simply unimaginable, just a few years ago.

Online information is not only valuable per se, but it can also be used to influence other aspects of our modern societies. In fact, the ever-increasing convergence between the cyber and physical worlds is making more and more difficult to disentangle the critical systems that make up our societies. As a consequence, a single carefully crafted and perfectly timed piece of (dis)information can now potentially make or break elections, governments, economies, and infrastructures, thus granting a tremendous leverage in the hands of those who know how to weaponize and manipulate these critical systems. As a ubiquitous and striking example of this kind, think of FinTech, a growing field where finance and technology are now completely intertwined. Within this context, the interplay between Automatic Trading systems and the online chatter that feeds them for driving market decisions exposes such systems to a plethora of manipulative activities. Information reliance is also critical to business entities and industries, a problem exacerbated by the increasing adoption of outsourced ICT infrastructure (think of the cloud), with resulting increased security risks. The increased automation of information-driven modern industrial plants also exposes them to unprecedented risks. When the businesses or infrastructures at risk are those that are of critical importance for a nation—such as those responsible for telecommunications, logistics, or directly supporting military capabilities—the risks practically extend to whole countries.

The frantic technological advancement previously outlined radically changed information warfare scenarios, posing new threats, ranging from personal to national security that every actor should take into consideration [2]. Classic books on information warfare usually deal with the subject by categorizing the treated arguments based on the "warfare capabilities and directions" of the most powerful nations (e.g., the United States, Russia, China, and others) or based on the pillars of information warfare: Psychological Operations (PSYOPS), military deception, electronic warfare, physical destruction, and Operational security (OPSEC). Unlike these traditional approaches, in this book, we will discuss new threats opened up by the latest technological advancements that have never been addressed before—at least, in the dimensions we categorize them. In particular, we partition the discussion on the new dimensions of information warfare into three macro areas: Society, Economy, and Infrastructures. For each area domain, the relevant threats are contextualized with real case scenarios and explained in detail; we also provide, for each domain, insights in terms of possible future attacks and countermeasures; and, finally, for every scenario, we also highlight the related open issues.

In conclusion, we show that the genie is out of the lamp and that the ones that will tame it would likely have a strategic advantage—our aim with this book having been to provide some food for thought to enable reaching the latter objective.

1.1 Organization

1.1.1 Book Structure

The topics covered in this book are discussed following a vertical, top-down approach where we first introduce the background and the general layout of a topic, before delving into the detailed description of its characteristics. With the exception of this chapter—discussing the landscape of the new dimensions in information warfare (NDIW)—this book is organized into three parts. These parts provide the coarsest viewpoint on information warfare. In particular, they represent the pillars of a nation and the possible macro-targets for the cyberwarfare, namely, Society (Part I), Economy (Part II), and Infrastructures (Part III). Parts are organized in chapters that list and discuss different information warfare scenarios. At the finest grain, each scenario describes current and future security threats, surveys existing scientific literature on the topic, documents notable attacks, provides a list of known countermeasures, and concludes by analyzing open issues as well as proposing directions for future research, experimentation, and intervention.

1.1.2 Infoboxes

Throughout the book, two different types of *infoboxes* are used in order to highlight specific pieces of additional information that readers might be interested in. Definitions of important concepts and keywords are contained in *definition* infoboxes, as shown below.

Definitions

Information Warfare The manipulation of information trusted by a target without the target's awareness, so that the target will make decisions against their interest but in the interest of the one conducting information warfare. It involves the collection of tactical information, assurance that one's own information is valid, spreading of propaganda or disinformation to mislead the enemy and the public, undermining the quality of the opposing force's information and denial of information to opposing forces.

In addition, whenever useful resources are available, they are listed and briefly described in *resources* infoboxes. Useful resources include public, curated datasets and knowledge bases; Web portals that contain extensive detailed information on a topic; pieces of software such as packages and libraries that can be used for carrying out specific analyses; as well as full-fledged applications.

Resources
Springer's page on *Security and Cryptology* includes links to several titles that discuss topics strictly related to information warfare.[1]

[1] https://www.springer.com/gp/computer-science/security-cryptology.