New Dimensions of Information Warfare

Part 0: Introduction

Roberto Di Pietro
Hamad Bin Khalifa University - CSE
rdipietro@hbku.edu.qa

Simone Raponi
Hamad Bin Khalifa University - CSE
sraponi@hbku.edu.qa

Maurantonio Caprolu
Hamad Bin Khalifa University - CSE
mcaprolu@hbku.edu.qa

Stefano Cresci
National Research Council - IIT
stefano.cresci@iit.cnr.it

January 19, 2021

Foreword

It would be difficult to imagine our daily life, our production systems and, in general, our society without the technology solutions we are immersed in and surrounded by. However, technology, and in particular information technology, is a double-edged sword.

The capillary diffusion and reach of social networks enable us to communicate our ideas to the world, but they could easily be used to spread fake news; the adoption of digitized industrial control systems is rewarded with a boost on cost reduction, efficiency and performance, but those very same controls can also make the controlled systems much more fragile; the advent of novel digital financial instruments and tools, from high-frequency trading to cryptocurrencies, do multiply the possibility to trade and to access financial instruments, but they also pose a threat, for the policy makers, to the control of the financial leverage; technologies that have been developed for entertainment, such as drones, have expanded to a number of no-one-envisioned-before applications and jobs, but they also enabled the possibility of physical attacks through the very same media.

Technology has drastically reduced the distance between ideas and implementation, projects and outcomes. This is just a logical consequence for what technology is: a magnifier of our capabilities. Nowadays, a 240 characters piece of news, conveyed to hundreds of millions, could sink the NYSE or skyrocket the price of a share. An induced malicious glitch in a water-desalinization or oil extraction pressure-controller could induce the outage of critical infrastructure and spur, according to the allegedly attribution, geo-political tensions in vast regions of the world. Similarly, the use of a social network by billions of young people can slowly induce, by subtle AI algorithms, new life models and different values to new generations—potentially creating domestic turmoil of an unprecedented magnitude.

As a result, the technology transformed the society so in depth and so quickly that almost all the essential functions and services of a Nation have been digitalized, this is why even the decision on the very same adoption of an apparently neutral technology, such as the 5G, or which data can be exploited by a social network company, could lie with the Department of State

as a national security matter rather than with a technical, bureaucratic desk. This means every nation needs to set appropriate cyber defenses in terms of sociological, legal, organizational and technical issues to cope with the complexity and threats induced by the cited technology waves that could harm the very pillars of our democracies, putting at stake even the values of our new generations. While initially lagging behind these threats, States and Supranational Organizations have started to respond. For instance, at the EU level the Network and Information Security (NIS) directive and the "Cybersecurity act" are being implemented. In the US, each government organization is involved on a daily basis to implement its own piece of a multidimensional Cybersecurity Strategy regularly revised by the White House to take both latest technology development and its social-economic implications into account. In Italy the Parliament has recently passed a law: "National Security Perimeter for Cyber", whose mission is twofold: (i) to create a more resilient Country by reinforcing security measures for essential functions and services of the State through a complex techno-legal organization; and, (i) to foster a strategic plan to achieve an intended degree of digital sovereignty.

As a consequence of the previous arguments, it is true more than ever that "Information (and the technology used to manage it) is power". It is no surprise, therefore, that Information Warfare—roughly, the manipulation of information trusted by a target without the target's awareness—is a topic that cannot be anymore restricted to the battlefield. The one who is able to control or influence information within a given ecosystem (ranging from your ring of friends, to industry, finance, and politics, to cite a few), can exercise a form of control over that ecosystem.

The above scenarios and considerations do pave the way to a number of fundamental questions, such as: What are the novel boundaries of Information Warfare? What technologies are today critical to that respect? To which extent the very fabric of our society, economics, and critical infrastructures can be affected by Information Warfare?

All the above introduced questions do require are urgent attention and, especially, a framework that sets the tone of the discussion, highlights the assets at stakes, and suggests the objectives to be achieved. That is why I found this book a gripping read. It introduces a novel vision on Information Warfare, addressing relevant dimensions of Information Warfare so far overlooked, put them in context, highlights the main strategical and tactical assets, and provides the tools for an educated discussion on the topic. The cited key features, combined with the clear exposition, the pleasant style, the comprehensive references, and the links to real-world cases, do make this book a reference for technologists, decision makers, practitioners, academicians, and insiders. But what is more, this book also provides food for thought for all the ones that are aware that information technology and its

nemesis, Information Warfare, are playing a vital role in the evolution and shaping of our Society. A Society that is in dire need to elaborate a strategic reflection on the novel dimensions and threats posed by Information Warfare.

Rome (Italy) August 27, 2020

Prof. Roberto Baldoni[1]
Deputy Director General
Department of Information for Security
Presidency of Ministry Council of Italy

[1]Roberto Baldoni is currently on leave from the Sapienza University of Rome, where he is a full professor of computer science. As DIS Deputy DG, Baldoni chairs the Italian Cybersecurity Management Board (Nucleo Sicurezza Cibernetica - NSC), an inter-ministerial organization established at DIS via executive decree (DPCM 2/2017). NSC implements and oversees the prevention and management of nationwide cyber crises coordinating National CSIRT, Postal Police (Ministry of the Interior), the Inter-Force Cyber Command (Ministry of Defense) and the intelligence agencies. NSC is also responsible for national cybersecurity policy positions in international forums and for fostering cybersecurity cooperation between government, research, and industry. Roberto Baldoni led the working group designing the Decree Law 105/2019 "National security perimeter for cyber" and in 2020 he is acting, on behalf of the Inter-ministerial Committee for Security of the Italian Republic (CISR), as roll-out coordinator for the Legislative Decree 105/2019.

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, 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 to the available information. 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 an 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. 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., USA, 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: So-

ciety, Economy, and Infrastructures. For each area-domain, the relevant threats are contextualized with real case scenarios and explained in details; 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.

Organization

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 3 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 cyber warfare, namely: Society, Economy, and Infrastructures. 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.

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 & Cryptology* includes links to several titles that discuss topics strictly related to information warfare[a].

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