Introduction

While industry and society started imagining, creating and dreaming of new lifestyles for humanity with the evolution of information technologies, strategists were imagining new conflict scenarios for the 21st Century; how could we take advantage of information and information technologies to take the lead over our competitors or enemies?

The Gulf War in 1991 seemed to provide an early conclusive answer. Controlling information and its technologies is the key to victory against modern conflicts. The expression "information warfare" was recognized throughout the world as a new and major concept, becoming the object of concern for many decision makers and strategists, whether they were military or civilian.

During the 1990s, other concepts took root in these debates on the control, risks and challenges of information and new technologies, such as, for example, information operations, cyber warfare, computer network attack, network-centric war or cyber terrorism. Since then, international literature has abounded with books, articles, reports, studies, analyses and official, unofficial, serious, and even sometimes far-fetched expert comments, describing these concepts and theories ad infinitum. Today, in the military field, we sometimes prefer the expression "information operation", though we increasingly mention cyber warfare, infowar or cyber attacks; however, the basic concept remains the broader "information warfare", which includes a range of operations carried out within the information world.

Information technologies, presented as the primary vector of international growth in the 21st Century, seem also to be our worst enemy, the Achilles heel of our societies dependent on information systems because, through them and with them, our adversaries and enemies can attack us.

And attacks are widespread in cyberspace. They may vary in type (spamming, phishing, intercepting, intrusions, data leaks, site defacements and DoS[1] attacks) but they are all an attack. As for the attackers, they have long had the image of a hacker, sometimes a minor, wrongly portrayed as a prodigy of computer genius (as if one needed genius to type on a computer to attack systems), able to penetrate the computer systems of a bank or government agency alone, and even suspected of being able to launch a major and destructive attack against the networks of a nation. But attackers are not all teenagers desperate for a new game. There can be multiple profiles and motivations; attacks do not only take the form of hacker attacks.

More generally, the concern that cyber attacks can disrupt the economy of a corporation or a nation, or even affect global stability, has become the nightmare of countries dependent on information technologies. The world has become conscious that it has entered the information technology insecurity age, controlled by security vendors.

And, since it is no longer possible to do without information and information technologies, we might as well, while we're at it, do well by them and, if possible, be harmful to our enemies. How can we use information and information systems to increase our defence capabilities? How can we dominate the enemy? How can we defeat them?

Information warfare must respond to these expectations. It must provide nations that do not have the resources to reach the level of more powerful nations on a military, technological, economic and digital basis, the means to rival them. But for all that, information warfare is not the weapon of the poor, the rock that must be thrown at the giant's eye to blind him, because information warfare supposes that we have relatively significant technological means, financial means and, especially, strategies.

The expression "information warfare" has not found a single, consensual definition. The reason is undoubtedly in the terms that it is made up of. The term "warfare" is still the subject of many a debate and its definition is different whether we are a sociologist, anthropologist, economist, historian, political scientist or member of the military. As for "information", it is approached in a different way whether we are a mathematician, computer specialist, sociologist, journalist, member of the military or economist.

This book, which introduces the concept of "information warfare", is not meant to completely solve these questions of definition. Its objective is to analyze what information warfare can be, its multiple aspects and components (because

[1] Denial of Service.

information warfare cannot be reduced only to attacks against computer networks), to identify its players, challenges and possible strategies, as well as looking at the input of some of the larger nations, where the world's economic, political and military balances are decided at the beginning of the 21st Century.