# Different Types of Information Warfare

**Aki-Mauri Huhtinen**
*National Defence College, Finland*

## INTRODUCTION

Information warfare (IW) has recently become of increasing importance to the military, the intelligence community, and the business world. The purpose of many actors, like decision makers, military advisers, non-governmental actors, or business people, is to facilitate an understanding of information warfare with reference to both military and civilian life (e.g., Huhtinen & Rantapelkonen, 2002; Kaldor, 2001).

According to James Der Derian (2003), information warfare has become the umbrella concept for understanding cyberwar, hackerwar, netwar, virtual war, and other technological network-centric conflicts. Many of these concepts associate technology and digital equipment and refer to a specific kind of computer technology. But these concepts are also connected to the definition of conventional conflicts and warfare. The question of conflict or warfare is not only physical, but also a psychological issue. For example, the terrorist group would hit the automated teller machine systems (ATM) and steal the money of private people. The damage would be very small technically but the influence of psychological behaviour could have a long effect. The ATM systems work perfectly and safely after the damage has been done but people no longer want to use it because of bad rumours.

Military operation other than war (MOOTW) has a history that goes back at least as far as Sun Tzu, who considered defeating an enemy without violence to be the "acme of skill" in warfare. Asymmetric, non-linear model of war underline the capability of perception and fast influence. The idea of avoiding open linear contact with the enemy and trying to seize the initiative to strike is the revival of the art of war. (Der Derian 2003, p. 453) Information warfare is concept of information society conflicts and threats. Information warfare means the use of information or information technology during a time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Cyberwar is an assault on electronic communication networks.

"The POST-COLD WAR paradigm for U.S. forces in combat and in military operations other than war (MOOTW) is increasingly a nonlinear battlespace where brigades and battalions conduct independent operations in assigned sectors. In postcombat and peace-support operations, nonkinetic/nonlethal means are often the main effort. The new paradigm is changing the way the Army plans, coordinates, executes, and conducts information-operations (IO) and IO-effects assessment at brigade and below." (Tulak, Broome, & Bennett, 2005)

The action of information warfare is defined as information operation (IO). Information operation can be divided into offensive IO (e.g., computer network attack, command and control warfare, special information operations), civil affairs, public affairs (media warfare), and defensive IO (e.g., physical security, computer network defense, and counter propaganda) (Huhtinen & Rantapelkonen, 2002). Information superiority means the simultaneous joint operation with all aspects of information operation. For example, the lack of defensive IO aspect can put at risk offensive IO. Without civil affairs of public affairs capabilities there are risks at achieve success in offensive and defensive IO. Media is one of the most important parts of modern warfare.

## BACKGROUND

Information warfare is not a new phenomenon, but it has been there from the beginning of human society. The effectively of information warfare has drastically increased along the emerge of global information and cyber space. The theory of information warfare is based on the laws of physics, interaction of and within societies, principals, means, and tools that enables one to gain information superiority over opponent. Information warfare is waged both during peace and war. The base of information warfare is created with psychological warfare, deception, and operation security. (Huhtinen & Rantapelkonen, 2002)

Information warfare has two main types. The first one is psychological warfare like media war and perception management, which can also be called the "soft" part of information warfare. The second is net warfare like computer or electronic warfare. The goal of information warfare is information superiority and securing the information system from an enemy or target. Cyberwar as a type of information warfare can define the high-technological warfare in cyberspace and mainly with machine-based warfare. One example is satellite reconnaissance.

The information revolution mainly means digital technology is available to more and more common people. There are two main arguments. The first one is that the information revolution has extended economic and political freedom expanding the world's democratic core. The second one is that computer technology is primarily a supporter of conservatism in government. These two contradictory arguments have brought about significant changes in the conduct of warfare, giving the United States, with its lead in information technology, a great advantage in international relations. So-called "roughly stated" information technology can help those who master it to win large wars at long distances with small forces. Rogue states are likely to turn to asymmetric strategies, for instance, weapons of mass destruction, terrorism, and information operation attacks against the United States and its partners.

For example, in March 2003, we had the opportunity to follow the U.S. attack on Iraq in real time online and on television. "The shock and awe" strategy had been taken into use the one example of information operation. According to its creator Harlan Ullman, it was important that the United States take control of the observations made by the states belonging to the Axis of Evil (Iraq, Afghanistan, North Korea), create a fear of these states' vulnerability, and emphasize the superiority and invulnerability of the United States. A good metaphor is a room into which the Iraqis have been locked in while the United States turns the lights on and off according to its desires. The whole idea was achieved by information superiority goal (e.g., Franks 2004)

## INFORMATION SUPERIORITY AND PERCEPTION MANAGEMENT

The authorities, researchers, and intelligence workers are interesting in outer space, human brains, human imagination, and artificial intelligence (AI) (Baudrillard, 2002). Gilles Deleuze wrote how our reality changes towards the TV studio where we can be the audience, the producer, and the movie star at the same time. The world itself changes movies (Deleuze 1995, p. 72). In the book "*Imagewars. Beyond the Mask of Information Warfare,"* we argued that life is full of paradoxes. They are everywhere: in politics, business, science, and war (Huhtinen & Rantapelkonen, 2002, p. vii). Rantapelkonen interpret the concept of war machine according to the thinking of Paul Virilio and James Der Derian. In his article "The War Machine, Dromology and Iraq War II" Rantapelkonen sees that Der Derian's concept of "military-industrial-media-entertainment (MIME)" network is an extension of the concept of "revolution of military affairs" (RMA). This MIME network runs on videogame imagery, twenty-four hour news cycles, multiple nodes of military, corporate, university, and media power. It is like havens a dream-machine and a horror-machine in one (Rantapelkonen, 2005).

Contending that access to lack of information today is just as crucial as possession of petroleum and ammunition. For example, there are closed circles within information, electric current, and the computer. The pump of petroleum needs electric current and without a computer you cannot direct information you need to pumping petroleum. Without electric current you cannot use computers. The cyberthreat posed by "almost invisible computer assailants" to a nation's power grids, transportation networks, financial systems, and telephone exchanges. Media (e.g., TV and Internet) is the one of the most important parts of information warfare. Superpower states military exercises have involved actions that elevate information warfare from a tactical level to a strategic level. Information warfare involves a new kind of battlefield but with the potential for equally as many casualties. Information warfare does not have the same lethally as classical weapons, but it can be neutralize as lethally (Rampton & Stauberg, 2003).

We assume that in democratic countries the media are not easily controllable and cannot easily be used as an instrument of war. Artz emphasizes that global companies own and control the media that creates spectators and consumers rather than informed citizens. Economical, political, and cultural leadership act neither with unlimited power nor simply through manipulation, but rather with widespread consent arising from the "common sense" of everyday life that has been institutionally organized. (Artz, 2005, p. 9) False beliefs about everyday lives are more dangerous to people than terrorists or criminals. Artz argues that the media–government–popular culture model encourages "Western" countries to understand individual actions as they are institutionally and culturally played out in the daily lives of working people as citizens, students, and soldiers. More dramatically, this model posits that our contemporary culture of spectatorship grounds the legitimacy of government actions and "our way of life." (Artz, 2005, p. 10)

The so-called "militainment" of society has a long tradition in cooperation between media and government. Actors and artists have visited troops since World War I. For example, NATO has a special budget for what is called "morale and welfare activities." The aim is to make the audience familiar with the situation of soldiers training and going to battle, to make the viewers get involved in military thinking and behaviour, and to lose distance from weapons and the force of arms. (Thomas & Virchow, 2005, p. 29-32)