Chapter 3
Information War as a Result of the Information-Technological Revolution

Salome Mikiashvili
Cyber Security Bureau, Georgia

ABSTRACT

In the chapter, different aspects related to the information war and cyber warfare of Russia-Ukraine war and the China-Taiwan relations are analyzed. In general, information warfare (WW) (as opposed to cyber warfare, which attacks computers, software, and control systems) is a concept that includes the use of combat space and the management of information and communication technologies (ICT) to achieve the goal. Information warfare is the manipulation of information trusted by the target, without the knowledge of the target, so that the target makes decisions against its interests but in the interests of the one who wages the information war. As a result, it is not clear when the information war begins and ends and how strong or destructive it is.

INTRODUCTION

Information is everything. When states go to war, information operations including data manipulation and data misuse are one of the keys to achieving their goals. Even in peacetime governments conduct cyberspace operations to support democratic norms and principles while others, surveil and target to destroy for their success and interests. Information warfare has enormous political, technical, operational, and legal implications for the military. Therefore, here we will try to define IW, identify potential military uses and applications, and explain different types of information warfare.

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. Information warfare (IW) has recently become of increasing importance to the military and the intelligence community.

Technology plays a crucial role in information warfare, as it enables actors to spread disinformation, manipulate public opinion, and conduct cyberattacks on a massive scale. One of the most significant

DOI: 10.4018/978-1-6684-8846-1.ch003

developments in recent years has been the emergence of social media platforms, which have become key battlegrounds for information warfare. Social media enables actors to disseminate information rapidly and target specific demographics with tailored messages.

This has been used by actors to spread disinformation, sow division, and manipulate public opinion.

In addition, the development of artificial intelligence and machine learning has given actors the ability to automate disinformation campaigns, making them faster, more efficient, and more difficult to detect. This has created new challenges for defenders, who must continually adapt their tools and techniques to keep pace with attackers.

On the defensive side, technology has also enabled the development of advanced cybersecurity tools and techniques to detect and respond to cyberattacks. These include tools for threat intelligence, network monitoring, and incident response.

Overall, technology has played a central role in shaping the landscape of information warfare, and it will continue to do so in the future. It is important for all actors, including governments, tech companies, and civil society, to work together to address the challenges posed by information warfare in the digital age.

According to Martin Libicki, information warfare occurs in the following forms: 1) warfare in the sphere of command and control; 2) intelligence 3) electronic warfare; 4) psychological warfare; 5) hacker warfare; 6) economic-information warfare; 7) cyber warfare (Libicki, 1995). All of these forms are connected, especially hacker warfare and cyber warfare which are not completely disjunctive.

Command and Control Warfare is a military strategy that applies information warfare on the battlefield to separate the command structure of the opponents from the units they command intelligence deals with the collection and analysis of various types of information including political, economic, technological, trade, etc., and then use this information to benefit one's interests.

Electronic warfare is also defined as a military activity that involves the use of electromagnetic and targeted energy in terms of dominating and managing events in the electromagnetic spectrum and terms of an electronic attack on the enemy and its combat systems.

Psychological warfare involves the use of information against the human mind. Psychological operations have had a serious impact on the war. Bot accounts that have been spreading misinformation about covid-19 were later spreading fake news about the war. There are numerous cases of psychological terror during the Russia-Ukraine war: Threatening messages were sent to soldiers; they were told to flee or otherwise be killed. Facebook accounts of militaries have been hacked, messages were sent using their names saying they surrendered and calling other soldiers to act the same way. but Facebook detected Russian state actors conducting psychological operations and deleted their accounts.

A hacker attack is usually aimed at congestion and changing the content of the attacked website. Because of their functional and physical characteristics, computer systems represent an ideal target for attackers.

In a global context, the" conflict" of the economic and intelligence services is constantly present, around confidential information that would be used against its competitors in the interests of its companies. This "conflict" essentially constitutes economic (or industrial) espionage (Damjanović 2017).

TECHNOLOGIES USED IN THE WAR IN UKRAINE

On February 24, 2022, the Kremlin tried to seize Kyiv in a so-called "Special Military Operation" intended to force regime change in Ukraine. One year has passed since the large-scale invasion of the