ABSTRACT

Thanks to the internet, the distances between the countries are easily overcome and the communication network rapidly expands. This situation also affects the cyber security of the countries to a great extent. Attacks on critical infrastructures, companies, and public institutions can be magnitude that make great harms. These developments in cyber space bring new problems. One of them is cyber terror. Cyber terror does not have a certain and well-known definition. Cyber terror is the realization of terrorist acts in the field of cyber war. In addition, cyber space is a place of display for terrorist acts. The effects of cyber terror attacks have reached a level to scare all countries. There is not enough information about the definition, characteristics, methods used in cyber terror attacks and cyber terror groups. It is important for national administrators and staff to become conscious and to become informed about cyber terror. In this chapter, information will be presented, endeavors on awareness-creation will be made, and a role of guiding the future studies will be taken.
INTRODUCTION

Nowadays, the fields in which internet and computers are not used are gradually decreasing. Many processes are carried out quickly and easily thanks to the internet, which has also become a big part of life. However, as the amount of information used, updated and stored during these processes has increased, their safe storage has become a major problem as well. To illustrate, cyber attacks are carried out against public institutions and organizations, critical infrastructures, commercial companies and states, or against people. Depending on the significance of the information, attacks may also change and become complex.

Information technologies are becoming more important and rapid developments in the field force the systems of private or state institutions to change. This situation makes the large institutions dependent to the internet and internet-based systems as much as it does the individual users. The attackers or attack groups, who are aware of this, conduct the terrorist activities via the internet. Cyber terror is formed by the combination of terror and cyber space. Cyber terror attacks to be carried out at critical infrastructures and places where the important information such as health, education, election, communication and security are kept and processed, can be effective enough to cause chaos throughout the country.

According to Dr Jones, the countries most affected by cyber terror will be the most developed ones (Jones, 2005). Considering countries such as Afghanistan, the rate of dependence on high technology is extremely low. In this case, countries in general will not be affected by the abuse of cyber technologies as much as developed countries. Although, the effects of cyber terror attacks are discussed the definition, framework, scope and effects of cyber terror attacks are not fully clear. For these reasons, it is very difficult to be prevented and stopped. The studies conducted by governmental institutions and concerning this issue are too few. Most of the existing studies relate to verbal expressions and making framework identifications. In a small number of studies, the framework and decision mechanisms are proposed to ensure security. The 9/11 attacks, some attacks of terrorist organizations such as ISIS, Al-Qaeda or PKK can be given as an example of cyber terrorist acts. In particular, the 9/11 attack is considered as an awareness point for cyber terror attacks (Temizel, 2011).