Terror and internet: case study / Alla Ofenberg

Abstract:

Numerous Technological Innovations in the information age have changed the Sociological order. Information became a main factor at this period of time and a dominant one. The cold war between east and west contributed to the development of communication networks which were used as a defense system against enemy's attack. This process contributed to the development of the Internet which makes the formation of different combination regardless of geographical position feasible. Every day there are being added new addresses to the internet. The internet gives people full freedom of expression.

Terror and Internet – although these two notions are completely different from one another, they were combined together in the concept of "information warfare". Information warfare constitutes an activity which is intended to make one object superior over another object by damaging the knowledge systems of the enemy by using the tool of processing information. Information warfare strategies can be a mean of protection and also a warfare tool. Terrorist seeks for ways which will assist him in his goal to disrupt the daily live of the nation by hitting exposed spots. An example of these spots is the communication networks and also social events which guarantees an extensive media coverage. A vast usage of computing and of communication networks created also an infrastructure to crimes that can be added under the title: "terrorist attack"; terrorist attack of this kind have gained a new name: cyberterrorism. Actions of cyberterrorism can be performed by individuals (that is, suicide killings) and by terror organizatians. Usually a terror organization has its own web site, which represents the organization in a positive light. By using the internet these organizations can attain support and sympathy and even to recruit new members and followers. The terrorist attacks arena is getting wider and one of the main factors of it is the internet. Operating terror via the internet is inexpensive: all is needed is a computer, a modem and a highly motivated hacker; these three factors can damage an entire system. The

attack of communication systems is most highly dangerous, because it can harm important strategic systems.

This research was conducted as a qualitative research which examined whether there is a connection between the appearance of cyberterrorism and a crisis which is happening simultaneously (e.g. political, nationalistic and regional crisis). During the last several years the cyberspace has became a battle field or even more accurate, another warfare front. Almost in every political crisis which is taking place around the globe; such as the crisis between Israel and the Palestinians, between India and Pakistan, the crisis in the basky district and in Kosovo. This research shows that there definitely exists a connection between the emergence of cyberterrorism and political, regional and nationalistic crisis, which occurs simultaneously. In these cases terrorist warfare is another front in the struggle. Further more this research shows that cyberterrorism can emerge as a completely independent phenomenon.

System no. 000568878

303.625 אופ.טר תשס"ג