Секция «Юриспруденция»

Questions of information war and information terrorism in the documents of UNO

Гуляко Юлия Викторовна
Студент
МГУ , международного права, Одесса, Украина
E-mail: li.sierra@bk.ru

In recent years, a concept known as "information warfare"has become popular within certain circles of the U.S. defense establishment.

Information warfare, as a separate technique of waging war, does not exist. There are, instead, several distinct forms of information warfare, each laying claim to the larger concept. Seven forms of information warfare—conflicts that involve the protection, manipulation, degradation, and denial of information—can be distinguished: command-and-control warfare (which strikes against the enemy's head and neck), intelligence-based warfare (which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battle space), electronic warfare (radio-electronic or cryptographic techniques), psychological warfare (in which information is used to change the minds of friends, neutrals, and foes), "hacker"warfare (in which computer systems are attacked), economic information warfare (blocking information or channeling it to pursue economic dominance), and cyber warfare (a grab bag of futuristic scenarios)[1]. All these forms are weakly related.

Although information systems are becoming important, it does not follow that attacks on information systems are therefore more worthwhile. On the contrary, as monolithic computer, communications, and media architectures give way to distributed systems, the returns from many forms of information warfare diminish.

In my work I try to show and to decide problems of information war and information terrorism, also in the documents of UNO.

This essay examines information warfare as the struggle over information processes rather than the efforts made to acquire information. Although the information systems required to manage logistics are substantial, they enter into information warfare only if and when an opponent targets the logistics information system to degrade it; similarly, weather collection systems enter information warfare only if they are subject to attack. By contrast, IBW systems are part of information warfare because they are used to read a target that would avoid being read and that often has ways (e.g., cover, concealment, and deception) to distort readings at the source.

The critical aspects of information warfare are information denial (or distortion) and its counterpart, protection.

What would the analogy for information war be to that kind of terrorism? Targeting individuals by attacking their data files requires certain presuppositions about the environment in which those individuals exist[2]. Targeted victims must have potentially revealing files on themselves stored in public or quasi-public hands (e.g., TRW's credit files) in a society where the normal use of these files is either legal or benign (otherwise, sensitive individuals would take pains to leave few data tracks). Today, files cover health, education, purchases, governmental interactions (e.g., court appearances), and other data. Some are kept manually or are computerized but inaccessible to the outside, yet in time most will reside on networks.

Tomorrow, files could include user-built agents capable of interacting with net-defined services and therefore containing a reliable summary of the user's likes, dislikes, and predilections.

The problem in conducting information terrorism is having to know what to do with the information collected. Many people, for instance, might be embarrassed if the information in their collected data sphere were opened to public view; but that does not necessarily make them good objects for blackmail. Similarly, the hassle created by erroneous entries in a person's files might be significant, but threatening to put them there has only limited coercive appeal (a person so threatened could seek to limit the damage by requesting repeated backups of existing data to archival media along with the demand that all incoming data must be authenticated).

If information terrorism is to succeed, a more plausible response than fear of compromise might be anger at the institutions that permitted files to be mishandled. Before a systematic reign of computer terror could bring about widespread compromise of enough powerful individuals it would probably lead to restrictive (perhaps welcome) rules on the way personal files are handled.

One example dealing with Development of specific legislation dealing with terrorist use of the Internet is Section 4f of the ITU Cybercrime Legislation Toolkit. The International Telecommunication Union (ITU) is the United Nations Organization that has most responsibility for practical aspects of cyber security. The aim of the Toolkit, presented in draft in 2009 and revised in 2010, is to give countries sample language and reference material for the development of national cybercrime legislation, so as to assist, according to the Toolkit's developers, the establishment of harmonized cybercrime laws and procedural rules&#8223;[3]. It aims to be a fundamental resource for legislators, policy experts and industry representatives in order to provide them with a pattern for the development of consistent cybercrime legislation. In addition to traditional approaches, the Toolkit contains several specific terrorist-related offences.

Литература

1. The Information Warfare Site - http://www.iwar.org.uk/;
2. The Information Assurance Technology Analysis Center, Official site - http://iac.dtic.mil/iatac/i
3. CTITF Working Group Report 2009. New York, 2011 - p. 19-23.

Слова благодарности

Хочу выразить благодарность моему научному руководителю Воротнюк Марине Александровне, замечательному и талантливому педагогу. Также я бы хотела поблагодарить Любашенко Вячеслава Игоревича за поддержку и помощь в написании данной статьи.