American cyber security policy versus the potential threat to civil rights/ Harel Menashri

Abstract

We are currently in the midst of a wave of an information revolution, categorized by speedy technological development, while computerized systems infiltrate every domain and people become more and more reliant on information and teleprocessing systems. The modern society is utterly dependent on computerized systems, which contain essential and required information for the operation of the country and the private bodies in it, control the civilian infrastructures (communication, energy, transportation, water etc.) and the military defense systems, direct the financial activity and the medical systems in hospitals.

Damage to these essential systems could damage the modern country's security and its ability to sustain a sound way of life. The more developed the country, the more dependent it is on the computerized information systems, and the more severe the outcome of damage to them could be.

The activity in the area of cyber warfare in general and computerized warfare in particular is on the rise in many parts of the world.

Cyber warfare constitutes a solution that is both cheap and causes a large damage effect compared with the alternatives. This issue is doubly important in times of security budget cuts and the price increases of weapon systems.

Terror organizations might take action against information infrastructure systems, while using the internet medium. The wide dispersion of computers make it an ideal tool for performing information terror attacks, which may, in some cases, have a result similar to that of terror attacks performed with conventional weapons. The computer from which the attack originates is hard to identify, there is no need for special labs to create it, the training field resides in every house, and every beginning hacker could serve as a terrorist. In other words, one of the characteristics of cyber

warfare is the fact that not only countries serve as opponents, but private people – hackers, private companies and organizations (institutionalized and others), while using software tools, which use loopholes in personal computers and are available to all.

Cyber warfare threatens the existence of national infrastructures, and warrants countermeasures which like warfare in other terror intelligence domains, takes place in "grey" areas, and sometimes outside the laws of the country in which it is performed and while abusing basic rights and freedoms.

The United States is one of the leaders in cyber warfare and in taking action against informational threats, due to its advanced technological abilities, which make its critical information infrastructures a primary target for cyber warfare – institutional or private (including hackers, terrorists and others) – and the damage to whose targets can be extremely critical, for example, taking over the control tower computer in a busy airport, or derailing a passenger train by taking over the train's control computer from afar, the possibilities are as endless as the reader's imagination.

The American government, acknowledging the availability of these possibilities, allocates many resources to extensive, highly budgeted and systemic actions, targeted at fighting the risks and defending national infrastructures.

The American Intelligence is directing its defense of information infrastructure activities towards foreign citizens, as well as against American citizens, through supervising websites, infiltrating personal computers and networks, listening in on telephone conversations, fax and email correspondences and so on, without the knowledge of these citizens, and without having to abide by the eavesdropping laws, or answer to public scrutiny. In other words, the technological leadership of the American Intelligence enables it to use extremely advanced technologies, which sometimes seem like a manifestation of science fiction, in order to thwart their opponents' actions, while infiltrating personal information systems of citizens and companies from the U.S. and other countries worldwide.

In addition, when confronted with problems created by the eavesdropping laws (for example, being legally unable to eavesdrop on American citizens), the American Intelligence can turn to its allies for assistance.

Part of this activity relies on special laws, directives and regulations ("The Patriot Law" and others). The other part is performed in the "grey area", with the assistance of colleague Intelligence bodies to bypass ethical and legal issues.

This research is based on a literary survey and historical research, and it focuses on examination of the processes and ways of defending essential national infrastructure in the U.S.A. from a computerized attack (cyber warfare means) as well as the possibility of infringing upon the personal freedoms of U.S. citizens (and the citizens of other countries), caused by the American Government, as a result of their activities against terrorists and cyber terrorists. This research presents the decision making process, which led to the founding of government bodies, working in this framework to defend the essential infrastructures, and the causes of the compromises of personal freedoms that result from these actions.

The resources for this research were selected according to these main criteria:

1. Reliability of the source (for example: official publication – governmental or other, well-known professional journal, information received through personal conversation/interview with an official or at a professional conference).
2. Historical descriptions of processes and familiar event descriptions.
3. Practical plausibility of the details described in the information source.

The results of this paper clearly show, that the activities of the American defense agencies, infringe upon the personal rights of the citizens of the United States as well as the citizens of other countries.

This research also shows that it is impossible to sustain a society without compromising its members' privacy to a certain degree in the name of public interest. The defense of society requires access to information using intelligence tools and means, which sometimes requires an abuse of privacy. The "mood" in most of the

western countries and mainly in the U.S. following the World Trade Center terrorist attack and the terrorist attacks in Madrid, Bali and London, has led to the intelligence agencies being given a much freer reign than prior to these attacks, to infiltrate personal domains.

The American experience, accumulated during the past few years regarding defense against cyber warfare and mostly in defining action domains, establishing the cooperation between national agencies (the intelligence community and others) and civilian organizations, developing combat theory and so on, may be of great assistance to Israel. However, those involved in the work should take into account that taking action against cyber threats necessarily creates opportunities and loopholes for abusing primary freedoms of citizens, and they should keep these to the minimum as much as possible, as a "defensive democracy".

System No.
1115130