Cyber-Terrorism

July 25, 2017 | **Written By:** Schafferman Karin Tamar

Cyber-terrorism, terror committed via a computer, is a complex threat which countries all over the world are struggling to outsmart. In this article originally published in Hebrew in Parliament, the Israel Democracy Institute's online journal, Karin Tamar Schafferman explains that fighting cyber-terrorism is "battling an enemy without borders", a truly challenging phenomenon. She warns that the consequences of cyber-terrorism could in fact be more severe than acts of conventional terrorism.

One of the greatest threats to modern society in the 21st century is the threat of cyber-terrorism - acts of terrorism committed via the computer. As developed countries increasingly turn to computer networks to control their infrastructure, they also become increasingly exposed to the dangers of someone hacking into their systems. The range of cyber-terrorist acts can be extremely diverse - from hacking into the database of a medical center and deleting patients' information, to disrupting water and electricity supplies of an entire country, to causing accidents by disrupting the transportation system. Experts in the field of cyber-terrorism believe it is no longer a question of whether this kind of attack will or will not take place, but rather a question of when and where cyber-terrorism will finally strike.

One of the essential differences between terrorism that strikes in a physical space and terrorism that strikes in cyberspace is logistical - it is exceedingly difficult to plan, coordinate, and execute a conventional terrorist attack, whereas cyberspace terrorism requires only the appropriate knowledge and a personal computer. Hackers can break into computer systems long-distance, without the need of any logistical support.

Terrorist groups have long noticed the opportunities cyberspace presents, and the internet's accessibility, anonymity and global character have made cyber-terrorism very attractive and difficult to battle. Today, most of the terrorist organizations' activity on the web focuses on propaganda, psychological warfare, the recruitment of funds and human resources, enemy surveillance and espionage, and coordinating activities. These actions are not yet considered terrorist acts, but they can contribute greatly to those advancing such acts.

Beyond hacking into systems and collecting information, which doesn't cause much damage on a national or international scale, there is also the possibility of more pernicious cyber-attacks. Although this stage has not

yet been reached, the future threat of cyber-attacks is very plausible. Possible targets of such an attack are communications systems, banks, electricity, water, transportation, government services, emergency rescue services, and the systems responsible for storing and distributing natural gas and oil. Possible scenarios are hacking into the banking system, which could lead to a complete shutdown of a country's economy or a disruption of communications between airplanes and control towers, which could lead to serious loss of life and property.

Less intimidating scenarios are the disruption of television and radio signals, traffic lights, student databases, etc. In fact, cyber-terrorism can potentially disrupt any part of our day-to-day lives, anytime and anywhere.

One may ask if there are people or organizations with the ability and motivation to carry out such attacks. Some claim that most terrorists are not yet capable of cyber-attacks, but that it is only a matter of time before they are. A report entitled Cyber-terror: Prospects and Implications, published in 1999 by The Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School (NPS) in Monterey, California, claimed that it will be a long time before cyber-attacks can take place, since the obstacles to be overcome are very high. According to the report, any group that would want to execute a particularly violent cyber-attack would need between six to ten years of preparation - quite an unnerving finding, considering the report was published nearly a decade ago. Indeed, since 1999, and especially since 9/11/2001, some research has shown that fundamentalist Islamic terrorist organizations, mainly Al-Qaeda, are establishing cyber-terrorism academies, with the goal of developing terrorists' ability to attack the West through cyberspace.

Countries that are threatened by cyber-terrorism are working fervently to protect their computer networks and systems, but do not tend to cooperate with one another, because they wish to preserve any advantage they may have in the field of information security. Most joint international efforts focus on cyber-crime, rather than cyber-terrorism. As for UN conventions, history has taught us that a convention dealing specifically with cyber-terrorism will probably not be drafted, until there is a major cyber-attack.

Battling an enemy without borders, who can attack anywhere, is a difficult task indeed. The next generation of terrorists will grow up in a digital world, with the tools to allow them to instantly infiltrate computer systems and networks, without leaving the comfort of their own home. The fact that so much of our daily life is based entirely on computer systems makes cyber-terrorism a strategic threat, the consequences of which could be just as severe as conventional terrorism, if not more so.

Sources

Prof. Gabi Wiemann and Dr. Yariv Zfati, Online Terrorism [Hebrew]
Founding an organization for researching and developing tools for fighting terrorism, for the sake of homeland security in the face of the threats of terrorism [Hebrew], National Security Council and the Samuel Naeman Institute for Advanced Studies in Science and Technology.
'Hacker', Wikipedia [Hebrew]
'Cracker', Wikipedia [Hebrew]
Fighting Terrorism in the field of Information [Hebrew], Students of the multi-disciplinary law and technology workshop, School of Law, Haifa University
Collin, Barry C., 'Future of Cyber-terrorism: Where the Physical and Virtual Worlds Converge', The 11th Annual International Symposium on