Cyberspace and Terrorist Organizations

Yoram Schweitzer, Gabi Siboni, and Einav Yogev

In a scene in the 1990 movie *Die Hard 2*, terrorists take control of computer, traffic control, and aerial communications systems, impersonate flight inspectors, and feed in false data, thus leading the pilot and passengers to their death in the midst of a snowstorm with the plane crashing on the runway. Security personnel are helpless, incapable of providing a response; the movie's hero, John McClane (played by Bruce Willis), lacks the means to save the doomed flight and is left standing powerless in the fog on the landing strip, waving two improvised beacons at the approaching aircraft. At first it would seem that the movie is nothing but another Hollywood fantasy, dismissible as a wild exaggeration carried to yet further extremes in the sequel, *Die Hard 4*. However, the events of 9/11 and the changes in the nature of security threats over the last decade indicate that even the most far-fetched scenarios crafted in Hollywood studios are liable to find real-life expression in the public and security sphere in this day and age.

The use of cyberspace as a primary warfare arena between enemies or hostile nations has always been fertile ground for fantasy and lurid scenes on the silver screen. However, cyberspace is rapidly becoming a genuine central arena for future wars and hostile actions undertaken by various types of adversaries. These may include terrorist organizations, although until now they have relied primarily on physical violence to promote their own goals and those of their sponsors. In light of such threats, many nations in the West have in recent years established special authorities to

Yoram Schweitzer is head of the Terrorism and Low Intensity Conflict Program at INSS. Dr. Col. (ret.) Gabi Siboni is head of the Military and Strategic Affairs Program at INSS and head of the Cyber Warfare Program at INSS, which is supported by the Philadelphia-based Joseph and Jeanette Neubauer Foundation. Einav Yogev is a research assistant at the Terrorism and Low Intensity Conflict Program at INSS.

use innovative technological means to prepare for war-like actions against strategic infrastructure targets.

This essay focuses on an analysis of the factors that are likely to make terrorist organizations use cyber tools to perpetrate attacks on critical infrastructures of sovereign institutions and symbols, commercial and industrial infrastructures and systems, and public civilian targets. In addition, it examines the question of whether the threat is actual and imminent, or whether it is a far-fetched possibility that surfaces from time to time in the general discourse on the subject.[1]

The Cyber Threat from Terrorist Groups

Today there are five main groups that use or have the potential for future use of cyber attack tools: 1) states developing offensive and defensive capabilities as a growing part of their force capabilities; 2) criminal elements motivated primarily by illegal commercial interests; 3) commercial companies, primarily in the defensive mode (as the scope of cyber attacks in the commercial context is significantly growing), though some may resort to offensive moves against competitors; 4) terrorist organizations, out of cost-benefit considerations and other inherent advantages, are liable to try to carry out cyber attacks; and 5) anarchists opposed to the existing establishment who are interested in undermining it from within and without, and who endeavor to attack the entire system of computerization, which today is the basis for managing life as we know it, in order to disrupt or even destroy states' current social order and their fabric of life.

Cyber offense has the potential to change society's balance of power because it empowers those engaged in asymmetrical conflicts that operate from a position of inferiority, especially terrorist organizations. Capabilities in this sphere may enable them to attack installations, systemic processes, and sites while causing heavy physical damage and wielding a significant psychological impact on the society and public under attack. They thus acquire capabilities other than those familiar from conventional terrorist attacks, such as suicide bombings, booby traps, hostage situations, hijackings, and kidnappings.

Cyber offense affords several advantages. First, it removes the necessity of physical presence at the target. It is possible to damage communications networks and control systems of installations and processes from afar and thus avoid physical barriers and human systems. Second, it affords

a wider scope of damage. Cyber attacks occur not only in the physical space but also carry the potential for severe and sustained damage to control and infrastructure systems. Thus, while most conventional terrorist attacks are limited in time and space,[2] a cyber attack magnifies terrorism's psychological impact through fear and intimidation. Third, it is easier to conceal the identity and source of the attack; in cyberspace, identities and boundaries between states are more easily blurred. Terrorists attacking in cyberspace can not only conceal their identity but can also feed false information as to the source of the attack, for example, by attacking a site inside the target state using addresses of a friendly nation. Fourth, cyberspace attacks are cost effective. Using the cyber platform for attacks maximizes the cost-benefit ratio from the perspective of a terrorist organization, endowed with fewer resources and capabilities than the states it targets. Assuming that terrorist organizations would prefer less defended targets rather than well-protected ones, they presumably would be able to gain access and insert malicious code into target sites, or use technologies that are becoming ever more accessible to wider audiences. Fifth, cyber terrorism can be non-lethal. It can cause significant damage without direct fatalities or physical injury, granting terrorists success by means of intimidation and disruption of the routine. This gives the perpetrators the ability to devise a defense and logical explanations for their deeds, which after all did not spill blood but were only an indirect cause of lost lives. The innovativeness represented by such action would also garner terrorist organizations widespread media coverage and enable them to engage in non-lethal threats in which a price would be extorted in exchange for removing the threat of a cyber attack.

It has been claimed that terrorist organizations are not interested in cyberspace because they prefer showcase attacks with much higher visibility rather than the anonymity that supposedly is conferred by attacks in this domain.[3] However this claim does not take into account the basic rationale of terrorism strategy, which holds that terrorist activity should focus on minimizing the power differential in the struggle against a stronger enemy with more powerful means, carry out destructive actions while identifying the weaknesses in the enemy's defense, and achieve a position of superiority at tolerable costs given the relatively poor means at the disposal of the perpetrators. Already today global jihad terrorist organizations are making use of cyberspace, though still in limited and

relatively undeveloped fashion, to realize these advantages. A study examining the cyberspace warfare capabilities of jihadist organizations[4] identified a number of major features that serve to build and improve the organizational and operational infrastructures of terrorist organizations in the following fields:

a. Propaganda: using the web to disseminate ideas, decrees, directives, speeches, and opinion pieces by clergy and terrorist leaders.
b. Recruitment and training: using the web to identify and recruit potential members as well as to transmit instructional and training materials.
c. Fundraising and financing: using the web to fundraise under the guise of charities and aid organizations as well as to steal identities and credit cards.
d. Communications: using the web for operational communications while employing a range of tools, including accessible encryption tools.
e. Identifying targets and intelligence: using information available on the web to identify targets and gather intelligence.

It is thus clear that an essential upgrade of cyberspace tools available to terrorist organizations, from logistical and propaganda tools to actual operational tools, is liable to generate an innovative, dramatic, and relatively cheap type of attack with the power to effect severe damage, even if carried out with a low signature or in total anonymity. Therefore every terrorist organization, especially one seeking fame and wanting to affect the public psyche and morale in the targeted enemy, sees such an attack as an important and worthy challenge. Innovation would also guarantee the perpetrators international fame and transform them into role models. Thus, sub-state entities with more limited technological capabilities than the nations with which they are at war are liable to join the trend of using advanced technology needed for cyber warfare for their own benefit, either by receiving assistance from supportive nations or by acquiring such capabilities themselves in the future, by recruiting and operating individuals with the necessary skills in this field.

As for states supporting terrorism, cyberspace is very attractive for use of proxy organizations because of the anonymity afforded by the domain, the difficulty in proving the identity of the perpetrator, the high level of deniability by states about their involvement, and the satisfaction of causing severe damage to the enemy. Even if suspicions are aroused, it is still hard to prove guilt. Furthermore, the public under attack may

perceive a cyber attack to be less outrageous than a terrorist attack that employs firearms and causes direct death and destruction – even if the damage caused is greater, more destructive of property, and takes more lives than a violent terrorist act.

Despite these advantages of cyber attacks, to date no such attack has been traced to a terrorist organization. Development of significant capabilities in this field requires surmounting a considerable intelligence and technological threshold. At this stage one may assume that terrorist organizations find it hard to identify, harness, and maintain such high technological capabilities and access that would allow them to cross that bar. It is true that this limitation can be partially overcome through the assistance of state supporters of terrorism, but at least for now this is not enough to give terrorist organizations the significant, stable technological platform required for maintaining effective cyber attack capabilities. In addition, terrorist organizations face limitations posed by cyber surveillance and state intelligence and technological capabilities that enable them to identify suspicious conduct on the web, identify attempts at organization, and mount a defense against them and against threats to specific targets.

Weaknesses and Responses

Although to date terrorist organizations have not been able to overcome the difficulties in achieving offensive cyber capabilities, civilian systems and routine civilian life presumably remain their preferred targets, because these are much more difficult to protect than security systems. Strengthening defenses of critical national infrastructures such as electric, water, and communications supply networks would likely encourage terrorists to seek out less protected targets in the civilian and commercial sectors. Even though systems in these sectors are usually not included in the rubric of critical and protected infrastructures, from the terrorist perspective an attack against them could be effective, by breaching ordinary citizens' basic sense of security and enhancing the terrorists' image by instilling fear.

A significant part of constructing a defense against cyber attacks is general and independent of the source of the threat, whether terrorist, state or criminal. This is reflected organizationally – consider Israel's Information Security Authority and ministries specializing in cyber defense in various

nations – and also in certain components of defense from the fields of information systems and general security. In contrast, in fighting terrorist organizations it is also necessary to activate two designated components that require sustained development and improvement.

The first is intelligence. Effective gathering of accurate, high quality intelligence requires using a range of sources, including open sources and material from the terrorists' own computers and networks. To this end it is necessary to develop capabilities of infiltrating these systems covertly and inserting information effectively and continuously. The challenge that must be overcome is the widespread global deployment typical of terrorist organizations that use many chat rooms and transmit messages using unique code words. Intelligence agencies must be able to intercept these transmissions and decode them within the relevant timeframes and at the same time provide cyber defense systems with the tools needed to protect against and even disrupt the planned actions.

The second component is disruption. Unlike defense systems, which do not try to prevent an attack but rather obstruct its success once it has already been launched, the goal of disruption is to thwart the execution of the attack or to hamper its progress. Establishing an effective disruption structure against cyber attacks by terrorist organizations requires intelligence monitoring and control that can identify the organization of an attack before it takes place and operate effectively to foil it. This aspect relies primarily on tactical intelligence gathering capabilities, both from computers and from communications networks used by terrorist organizations.

Disruption attempts can also be directed towards damaging the organizational infrastructures of the organization. An example of this occurred in England when British intelligence hacked the online issue of the British al-Qaeda magazine *Inspire*. In addition, in recent years the various components of the electronic jihad have been targeted for occasional cyber attacks largely attributed to Western governments: the Taliban's website has been hacked time and again, as have exclusive jihadist forums and high profile fundamentalist websites. Meanwhile, American, Saudi Arabian, and Dutch authorities have extracted valuable information about potential Islamic terrorism from jihadist websites serving as honey traps for high quality intelligence.[5]

At the same time, it is necessary to deepen the defenses of civilian systems that represent the greatest weakness and therefore are also preferred terrorist targets. For example, the British government began taking legislative steps that include authorizing the use of invasive techniques such as telephone wiretaps, surveillance of emails in police files connected to crimes of terrorism, torpedoing internet radicalization processes, and specialized training of police units to confront cyber threats.[6] Nonetheless, in most states the defense of civilian systems is still in its infancy. Most states' cyber defense resources are allocated to security systems and to what are considered critical national infrastructures. Deepening the defense of civilian systems requires radical changes on a national scale that must be supported by appropriate regulation.[7]

Conclusion

In December 2001, at a meeting in New York shortly after the 9/11 attacks, the philosopher Jacques Derrida presented his understanding of the changes generated in the world as a result of those events. According to Derrida, the attacks were still part of the "archaic theater of violence," the real, visible world, in which events are still conducted in "clear and great order." However, according to him, cyberspace presents us with a more potent threat to our political and physical world; the dangers inherent in it change the relationship between terrorism, in the psychological and historical sense of a violent attack, and the concept of territory. Now, in the new techno-scientific world, the threat we knew in the past as real has become an invisible, quiet, and swift threat, devoid of bloodshed, which, according to Derrida, is worse than the 9/11 attacks, which at least were directed against a known location at a particular point in time. Now we are facing a challenge that threatens the social and economic fabric of life that connects all of us and upon which all of us depend in every place and at every moment.[8]

The rapid technological developments and innovations of recent years in the domain of cyberspace have indeed created a battlefield that simultaneously brings together many varied populations, local and international, representing a desirable target and fertile ground of activity by sub-state entities. Since thus far there has been no known cyber attack perpetrated by a terrorist organization, the threat does not seem acute. The challenge facing those who would try to use cyberspace for malicious

purposes is three-pronged: attaining high level intelligence, the ability to crack computerized systems protected with advanced technology (or accessibility to such ability), and very high levels of calculation and computerization skills.

However, the advantages afforded by attaining cyberspace capabilities as described in this essay are liable to serve as an incentive for terrorists to develop, acquire, or harness such capabilities in the future. Gaining control of the advanced technological and intelligence capabilities required in cyberspace is likely to give these elements who seek to seriously damage their enemies by causing massive destruction and sowing terror and intimidation in the public at large the ability to disrupt the normal routine of civilian life, undermine civilian trust in their governments, and of course gain valuable prestige and media stature.

Therefore, Western nations must work diligently to meet this threat and improve the effective intelligence and defensive capabilities of civilian systems, while at the same time construct accurate intelligence gathering capabilities and the ability to disrupt cyberspace organization and attack by terrorists. Neglecting the civilian cyberspace domain, which is an attractive target for terrorists, is liable to prove disastrous in the future and place security personnel, when the time comes, in the same position as that fictional Hollywood hero of *Die Hard 2* trying to save airplanes from crashing using nothing other than improvised beacons.

Notes

1 The use of the term cyber terrorism in this essay refers to the use of cyber tools liable to be used by terrorist organizations to attack economic infrastructures and civilian systems in targeted nations.

2 There are of course important exceptions: the 9/11 attacks in the United States had a global effect on flight security systems.

3 Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts, Trends, and Implications for Israel*, Memorandum No. 109 (Tel Aviv: Institute for National Security Studies, 2011, p. 42).

4 *Examining the Cyber Capabilities of Islamic Terrorist Groups*, Institute for Security Technology Studies at Dartmouth College, Technical Analysis Group, March 2004.

5 Adam Rawnsley, "Stop the Presses! Spooks Hacked al-Qaida Online Mag," *Wired*, June 3, 2011, http://www.wired.com/dangerroom/2011/06/stop-the-presses-spooks-hacked-al-qaida-online-mag/June 4, 2011.

6 "Warning of Rise in Cyber-terrorism," *The Independent*, July 12, 2011, http://www.independent.co.uk/news/uk/crime/warning-of-rise-in-cyberterrorism-2312434.html.

7 Gabi Siboni, "Protecting Critical Assets and Infrastructures from Cyber Attacks," *Military and Strategic Affairs* 3, no. 1 (2011): 93-101, http://www.inss.org.il/upload/(FILE)1308129638.pdf.

8 Jacques Derrida, in Giovanna Borradori, *Philosophy in a Time of Terror: Dialogues with Jürgen Habermas and Derrida* (Hebrew translation, United Kibbutz Press, 2004), pp. 173-74; also available (in English) at http://www.press.uchicago.edu/Misc/Chicago/066649.html: "One will be able to do even worse tomorrow, invisibly, in silence, more quickly and without any bloodshed, by attacking the computer and informational networks on which the entire life (social, economic, military, and so on) of a 'great nation,' of the greatest power on earth, depends. One day it might be said: 'September 11' – those were the ('good') old days of the last war. Things were still of the order of the gigantic: visible and enormous! What size, what height! There has been worse since. Nanotechnologies of all sorts are so much more powerful and invisible, uncontrollable, capable of creeping in everywhere. They are the micrological rivals of microbes and bacteria. Yet our unconscious is already aware of this; it already knows it, and that's what's scary."