# The Threat of Terrorist Organizations in Cyberspace

**Gabi Siboni, Daniel Cohen, and Aviv Rotbart**

This article discusses the threat of terrorism in cyberspace and examines the truth of the perceptions of this threat that have formed in recent years. It examines the capabilities that a non-state actor can achieve and whether these can constitute a real threat to the national security of states. For an analysis of the main threats facing a state from a multi-year perspective and in light of anticipated changes in a state's strategic balance, the factors that threaten the state are presented and the roots of the threat are identified. The article thus examines whether terrorism, whose impact is generally tactical, could make (or perhaps has already made) the transition to a cyber weapon capability with strategic impact. Specifically, the question is could terrorists develop cyber weapon capabilities that could inflict widespread damage or damage over time, of the sort that brings states to their knees and causes critical systems to crash.

**Keywords**: cyberspace, cyber terror, cyber weapons, terrorist organizations, non-state actors, cyber crime, enterprise information systems, core operational systems, intelligence guidance capability, technological capabilities

## Introduction

The first motion picture ever screened before an audience was produced by the Lumiere brothers in 1895. It showed a train entering a station, seemingly moving toward the viewers in the hall. The spectators, who were convinced that the train was approaching them, screamed in panic

Dr. Gabi Siboni is a senior research fellow and the head of the INSS Cyber Warfare Program. Daniel Cohen is the coordinator of the Cyber Warfare Program at INSS. Aviv Rotbart is a doctoral student in the Department of Computer Science at Tel Aviv University.

and fled the building. During the first movie ever shown, it seemed to the spectators that what they were seeing was reality.[1]

Cyber terrorism is a field in which reality and science fiction are sometimes intertwined. If we examine one of the key concepts in cyberspace − namely, dealing with terrorist threats − we find that the rationale underlying the concept (which emerged after the formative events at the beginning of the twenty-first century, such as the Y2K bug and the September 11, 2001, terrorist attacks) is that the world appears to be at the peak of a process that belongs to the post-modern and post-technology era, an era with no defensible borders, in which countries are vulnerable to invasion via information, ideas, people, and materials − in short, an open world. In this world the threat of terrorism takes a new form: a terrorist in a remote, faraway basement has the potential ability to cause damage that completely changes the balance of power by penetrating important security or economic systems in each and every country in the world and accessing sensitive information, or even by causing the destruction of vital systems.[2]

Can the reality of September 11, 2001 − when a terrorist organization that had planned an attack for two years, including by taking pilot training courses, eventually used simple box-cutters to carry out a massive terrorist attack − repeat itself in cyberspace? Is a scenario in which a terrorist organization sends a group of terrorists as students to the relevant courses in computer science, arms them with technological means accessible to everyone, and uses them and the capabilities they have acquired to carry out a massive terrorist attack in cyberspace realistic or science fiction? In order to answer this question, we must first consider what capabilities a non-state actor can acquire, and whether these capabilities are liable to constitute a real threat to national security. An analysis of the main threats facing a country over the course of several years, given expected changes in its strategic balance sheet, requires identifying the entities threatening a country as well as the roots of the threat and the reasons for it.

No one disputes that non-state actors, terrorist organizations, and criminals are using cyberspace for their own purposes and deriving benefit from a field in which everyone is at the same starting point − a field that also enables small individual players to have an influence disproportionate to their size. This asymmetry creates various risks that did not attract attention or provoke action among the major powers in the past. The question is whether the activity of these players in cyberspace constitutes

a threat with the potential to cause major and widespread damage, and if so, why such damage has not yet occurred.

This article assesses whether attacks in cyberspace by terrorist organizations, whose effect until now has usually been tactical, will be able to upgrade (or perhaps have already upgraded) their ability to operate cyber weapons with strategic significance – weapons that can inflict large scale or lasting damage of the sort that causes critical systems to collapse and "brings countries to their knees." The purpose of this article is to discuss the threat of cyberspace terrorism and assess the truth of the concepts that have emerged in recent years concerning this threat.

This article focuses on the activities of non-state organizations with political agendas and goals, even if operated or supported by states. A distinction is drawn between these activities and those that are conducted directly by countries, which are beyond the scope of the article, as are the activities of organizations whose aims are mainly of a criminal nature. For the purposes of this article, a terrorist act of a non-state organization in cyberspace will be defined as an act in cyberspace designed to deliberately or indiscriminately harm civilians. For example, disruption of the internet site of a commercial bank by a non-state organization with political goals will be defined as an act of terrorism in cyberspace. Figure 1 illustrates the scope of discussion in this article.

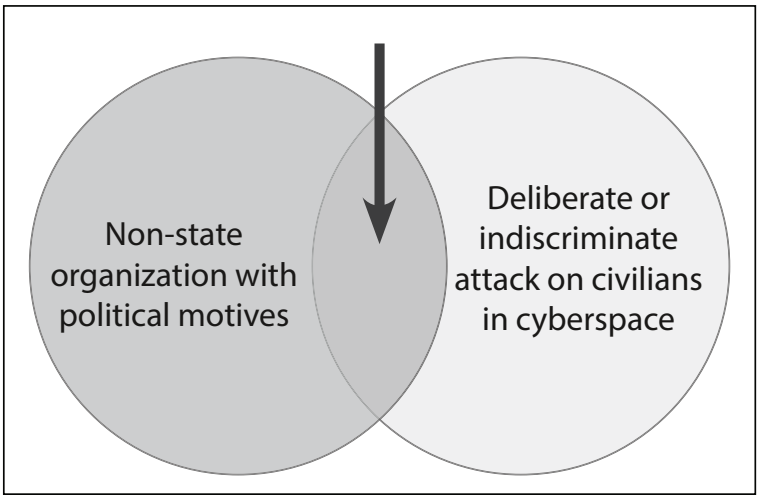


**Figure 1. Terrorist Acts in Cyberspace**

## The Methodology of the Study

A number of benchmarks had to be met in order to assess the activity of terrorist organizations in cyberspace. The first was identification of the motives for using cyberspace as part of the political struggle being waged by the terrorist organizations. Toward this end, two principal motives were identified. The first is the use of cyberspace in support of terrorist activity, mainly the acquisition of money and recruits or money laundering in order to finance the activity. The second is the use of tools in cyberspace to provide the actual strike against the targets that the terrorist organization set for itself, as well as its use for other violent means. In this context we will analyze the cooperation between non-state organizations and the states that operate them and support their terrorist activity.

The second benchmark of this study required an assessment and in-depth understanding of the capabilities that terrorist organizations can obtain, bearing in mind that not every computer operator, even if a technological genius, can generate an effective and significant terrorist attack. In this context we also examined the assumption that significant attacks in cyberspace will continue to be confined to high-technology countries and will require considerable resources in terms of both intelligence and technology. Next, having established an understanding of the terrorist organizations' array of relevant technological and intelligence capabilities, it was necessary to consider whether such activities by terrorist organizations have actually been identified. Finally, all the findings were analyzed in order to formulate conclusive insights and recommendations as part of the defense needs.

## Analysis of Capabilities

Cyberspace contributes to the enhancement of knowledge and acquisition of capabilities. In addition, technology is useful in creating an anonymous communications network.[3] Similarly, cyberspace serves as a platform for expanding the circle of partners for terrorist activity. In contrast to the recruitment of terrorist operatives in the physical world, in cyberspace it is possible to substantially enlarge the pool of participants in an activity, even if they are often deceived into acting as partners by terrorist organizations using the guise of an attack on the establishment. This phenomenon is illustrated by the attacks by hackers against Israeli targets on April 7, 2013,[4] when some of the attackers received guidance concerning the methods and

targets for the attack from camouflaged Internet sites. The exploitation of young people's anti-establishment sentiments and general feelings against the West or Israel makes it possible to expand the pool of operatives substantially and creates a significant mass that facilitates cyber terror operations. For example, it has been asserted that during Operation Pillar of Defense over one hundred million cyber attacks against Israeli sites were documented,[5] and that during the campaign and the attacks there were quite a few operatives who followed developments through guidance apparently provided by Iran and its satellites.[6]

On the one hand, the array of capabilities and means at the disposal of terrorist organizations in cyberspace is limited because of its strong correlation with technological accessibility, which is usually within the purview of countries with advanced technological capabilities and companies with significant technological capabilities. On the other hand, access to the free market facilitates trade in cybernetic weapons and information of value for an attack. One helpful factor in assembling these capabilities is countries that support terrorism and seek to use proxies in order to conceal their identity as the initiator of an attack against a specific target. In addition, the terrorist organization must train experts and accumulate knowledge about ways of collecting information, attack methods, and means of camouflaging offensive weapons in order to evade defensive systems at the target.

This study reveals that to date terrorist organizations have lacked the independent scientific and technological infrastructure necessary to develop cyber tools with the ability to cause significant damage. They also lack the ability to collect high quality intelligence for operations. The ability of terrorist organizations to conduct malicious activity in cyberspace will therefore be considered in light of these constraints.

As a rule, a distinction should be drawn among three basic attack categories: an attack on the gateway of an organization, mainly its internet sites, through direct attacks, denial of service, or the defacement of websites; an attack on an organization's information systems;[7] and finally, the most sophisticated (and complex) category, attacks on an organization's core operational systems,[8] affecting its core functions – for example, industrial control systems.[9] Cyber terror against a country and its citizens can take place at a number of levels of sophistication, with each level requiring capabilities in terms of both technology and the investment made by the

attacker. The damage that can be caused is in direct proportion to the level of investment.

## An Attack at the Organization's Gateway

As noted, the most basic level of attack is an attack on the organization's gateway, that is, its internet site, which by its nature is exposed to the public. The simplest level of cyber terrorism entails attacks that deny service and disrupt daily life but do not cause substantial, irreversible, or lasting damage. These attacks, called "distributed denials of service" (DDOS), essentially saturate a specific computer or internet service with communication requests, exceeding the limits of its ability to respond and thereby paralyzing the service. Genuine requests go unanswered because the service is overloaded by having to deal with the attacker's requests.

DDOS attacks carried out by a terrorist organization[10] need to be effective and continue for a significant amount of time to ensure that as many people as possible become aware of the attack and are affected by the denial of service. Suitable targets for such an attack are, among others, banks, cellular service providers, cable and satellite television companies, and stock exchange services (trading and news). Popular cellular applications whose disruption can be a nuisance, such as WAZE, access to e-mail service, and appointments calendars, as well as Voice over Internet Protocol (VoIP) call applications, may be added to this list.

Another method of attacking an organization's gateway is through attacks on Domain Name System (DNS) servers – servers used to route internet traffic. Such an attack will direct people seeking access to a specific site or service towards a different site, to which the attackers seek to channel the traffic. A similar, but simpler, attack can be conducted at the level of an individual computer instead of the level of the general DNS server, meaning that communications from a single computer will be channeled to the attacker's site rather than the real site which the user wishes to surf. Damage caused by such attacks can include theft of information; denial of service to customers, resulting in business damage to the attacked service; and damage to the reputation of the service. The attacker can redirect traffic to a page containing propaganda and messages he wants to present to the public.

One popular and relatively simple method of damaging the victim's reputation at the gateway of the organization is to deface its Internet

site. Defacement includes planting malicious messages on the home page, inserting propaganda that the attackers wish to distribute to a large audience, and causing damage to the organization's image (and business) by making it appear unprotected and vulnerable to potential attackers.

## An Attack against the Organization's Information Systems

The intermediate level on the scale of damage in cyberspace includes attacks against the organization's information and computer systems, such as servers, computer systems, databases, communications networks, and data processing machines. The technological sophistication required at this level is greater than that required for an attack against the organization's gateway. This level requires obtaining access to the organization's computers through employees in the organization or by other means. The damage that can be caused in the virtual environment includes damage to important services, such as banks, cellular services, and e-mail.

A clear line separates the attacks described here from the threat of physical cybernetic terrorism: usually these attacks are not expected to result in physical damage, but reliance on virtual services and access to them is liable to generate significant damage nevertheless. One such example is the attack using the Shamoon computer virus,[11] which infected computers of Aramco, the Saudi Arabian oil company, in August 2012. Even though the attack did not affect the company's core operational systems, it succeeded in putting tens of thousands of computers in its organizational network out of action while causing significant damage by erasing information from the organization's computers and slowing down its activity for a prolonged period.[12]

## An Attack on the Organization's Core Operational Systems

The highest level on the scale of attack risk is an attack on the organization's core operational and operating systems. Examples include attacks against critical physical infrastructure, such as water pipes, electricity, gas, fuel, public transportation control systems, or bank payment systems, which deny the provision of essential service for a given time, or in more severe cases, even cause physical damage by attacking the command and control systems of the attacked organization.

A successful offensive could cause the release of hazardous materials into the air and physical harm to a large population. This is the point at

which a virtual attack is liable to create physical damage and its effects are liable to be destructive. Following the exposure of Stuxnet, awareness increased of the need to protect industrial control systems, but there is still a long way to go before effective defense is actually put into effect. Terrorist groups can exploit this gap, for example by assembling a group of experts in computers and automation of processes for the purpose of creating a virus capable of harming those systems.[13]

Another way of obtaining physical cyber weaponry is likely to emerge from the black market in cyber weapons and its expansion to include physical infrastructure, in addition to the virtual weaponry that it already offers now. It should be noted that as of the date of this writing, such a scenario has not actually occurred. Because it involves complex and costly cybernetic weaponry, however, it is possible that clandestine trading in this area is already underway in the internet underworld.[14] As noted, this is the highest level on the cyber attack scale, and the costs and damage caused by it are correspondingly high, as evidenced by the Stuxnet worm.[15]

Development of attack capabilities, whether by countries or by terrorist organizations, requires an increasingly powerful combination of capabilities for action in cyberspace in three main areas: technological capabilities, intelligence guidance for setting objectives (generating targets), and operational capacity.

## Technological Capabilities

The decentralized character of the Internet makes trade in cyber weaponry easy. Indeed, many hackers and traders are exploiting these advantages and offering cyber tools and cyberspace attack services to anyone who seeks them. A varied and very sophisticated market in cyber products trading for a variety of purposes has thus emerged, with a range of prices varying from a few dollars for a simple one-time denial of service attack to thousands of dollars for the use of unfamiliar vulnerabilities and the capabilities to enable an attacker to maneuver his way into the most protected computer system. Thanks to cyberspace, this market is growing by building on the infrastructure of social networks and forums that allow anonymous communications between traders and buyers.[16] In an interesting phenomenon, seen only recently, these traders are leaving the web underground and stepping out into the light. They can be found on the most popular social network of all: Facebook.[17] A blog by information

security company RSA[18] describes a new situation, in which the traders offer their wares not only as goods, but also as a complete service, including the installation of command and control servers, training in the use of the tools, and even discounts, bargains, and the option of buying only certain modules of the attack tool in order to reduce the price. The growth of this market raises the question whether and how terrorist organizations can use all the knowledge and tools that have accumulated in the cyber crime market.

In order to answer this question, it is necessary to assess the gap between the abundance of tools and capabilities currently offered for sale openly on the Internet and the requirements of terrorist organizations. Today's market for attack tools is aimed at cyber criminal organizations, mainly for purposes of fraud, stealing funds from unwitting bank account holders, and identity theft by collecting particulars from credit cards, bank account numbers, identity cards and addresses, entry passwords to financial websites, and the like. These tools are not necessarily suitable for the needs of terrorist organizations. At the same time, many terrorist organizations might engage in the practices of cyber criminal organizations for the sake of fundraising to finance their main terrorist activity. The principal objective of terrorist organizations – causing substantial damage and instilling fear – can be accomplished in a number of ways and at different levels of difficulty and severity. The tools of the cybernetic underworld can be of great assistance in DDOS attacks and in stealing large quantities of sensitive information from inadequately protected companies (for example, information about credit cards from unprotected databases), which will almost certainly arouse public anxiety. Terrorists still have a long way to go, however, before they can cause damage to control systems, which is much more difficult than stealing credit cards, and towards which cybernetic crime tools are of no help. With respect to the intermediate level described above concerning attacks on an organization's information systems, it appears that the underworld possesses tools capable of assisting cyber terrorism. Some adjustment of these tools is needed, such as turning the theft of information into the erasure of information, but this is not nearly such a long process, and the virus developers will almost certainly agree to carry it out for terrorist organizations, if they are paid enough.

## Intelligence-Guided Capability

One of the key elements in the process of planning a cyber attack is the selection of a target or a group of targets, damage to which will create the effect sought by the terrorist organization. Towards this end, a terrorist entity must assemble a list of entities that constitute potential targets for attack. Technology that provides tools facilitating the achievement of this task is already available free of charge. For example, the Facebook and LinkedIn social networks can be used to find employees in the computer departments of infrastructure companies, food companies, and the like. Taking the Israel Electric Corporation as an example, academic studies[19] show that company divisions can be mapped, employees can be found in the various departments, and those with access to the company's operational systems can be selected, all with no great difficulty.[20] If these employees are aware of the importance of information security, and therefore cannot be directly attacked, their families and friends can be traced through Facebook, and the desired target can be attacked through them. Social networks constitute an important source for espionage and collection of business and personal information about companies and organizations,[21] and terrorist organizations can easily use the information distributed through them for their own benefit.

It is also necessary to map the computer setup of the attacked organization, and to understand which computers are connected to the internet, which operating systems and protective software programs are installed on them, what authorizations each computer has, and through which computers the organization's command system can be controlled. For example, if a terrorist organization wants to control the functioning of a turbine that produces electricity, its task, although much more technical and difficult than mapping the company's organizational structure, is now especially easy, following the publication of a study by a "white hat" hacker, who conducted the first "internet census" in history.[22]

Using a ramified network of robots (software programs implanted in computers that wait for an order from the command and control center to which they are connected), the white hat hacker compiled a list of 1.3 billion IP addresses in use, for some of which he published technical data such as the type of open gates, the requests to which these addresses respond, and more. The published results of the census are freely available to all interested Internet surfers. For a malicious hacker, these data are sometimes

necessary in order to attack and take over the entire computer system of an individual or organization. Thus a company's organizational structure can be mapped, and if its network is not adequately protected, information can also be gleaned about the computers used by the company's employees.

Good protection and awareness of information security capabilities can make it very difficult for hackers and terrorists to carry out the abovementioned actions. Organizations with critical operational systems usually use two computer networks: one external, which is connected to the internet, and one internal, which is physically isolated from the internet and is connected to the organization's industrial control systems. The internet census does not include information about isolated internal networks because these are not accessible through the internet. Any attack on these networks requires intelligence, resources, and a major effort, and it is doubtful that any terrorist organizations are capable of carrying out such attacks. Here the terrorist organizations can take advantage of another study conducted by hackers from the University of Berlin,[23] which uses a Google map (enabling researchers to present and share geographic information that they have collected) to display a large number of industrial control systems (ICS) deployed throughout the world that are connected to the internet. The information displayed on the map is taken from an enormous database freely available to everyone through the Shodan website,[24] which makes the life of a terrorist hacker much easier. This service uses information collected by Google for its mapping and location-based advertising services and makes it accessible to the public. It is possible that the hackers who recently broke into the home networks of hundreds of Israelis used services from the Shodan website in order to collect intelligence for the attack, and perhaps also to obtain tools (cyber ammunition) to actually carry it out.[25]

## Operational Capability

After collecting intelligence and creating or acquiring the technological tools for an attack, the next stage for planners of cybernetic terrorism is operational – to carry out an actual attack by means of an attack vector.[26] This concept refers to a chain of actions carried out by the attackers in which each action constitutes one step on the way to the final objective, and which usually includes complete or partial control of a computer system or industrial control system. No stage in an attack vector can be skipped, and

in order to advance to a given step, it must be verified that all the preceding stages have been successfully completed.

The first stage in an attack vector is usually to create access to the target. A very common and successful method for doing this in cyberspace is called spoofing, that is, forgery.[27] There are various ways of using this method, with their common denominator being the forging of the message sender's identity, so that the recipient will trust the content and unhesitatingly open a link within the message. For example, it is very easy to send an e-mail message to an employee at the Israel Electric Corporation (mentioned above), in which the sender forges the address of a work colleague, a relative, or another familiar person. The attacker's objective in this case is to make the receiver of the message trust the content of the message and open its attachments or enter the internet addresses appearing in it.

The forging of e-mail is an attack method that has existed for many years. Defensive measures have accordingly been developed against it, but attackers have also accumulated experience. Incidents can now be cited of completely innocent-looking e-mail messages that were tailored to their recipients, containing information relating to them personally or documents directly pertaining to their field of business. The addresses of the senders in these cases were forged to appear as the address of a work colleague. As soon as the recipients opened the e-mail, they unknowingly infected their computers with a virus.

The forgery method can be useful when the target is a computer connected to the internet and messages can be sent to it. In certain instances, however, this is not the case. Networks with a high level of protection are usually physically isolated from the outside world, and consequently there is no physical link (not even wireless) between them and a network with a lower level of security. In this situation the attacker will have to adopt a different or additional measure in the attack vector – infecting the target network with a virus by using devices that operate in both an unprotected network and in the protected network. One such example is a USB flash drive ("Disk on Key" or "memory stick"), which is used for convenient, mobile storage of files. If successful, the attacker obtains access to the victim's technological equipment (computer, PalmPilot, smartphone), and the first stage in the attack vector – creating access to the target – has been completed. Under certain scenarios, this step is the most important and significant for the attacker. For example, if

the terrorist's goal is to sabotage a network and erase information from it, then the principal challenge is to gain access to the target, that is, access to the company's operational network. The acts of erasure and sabotage are easier, assuming that the virus implanted in the network is operated at a sufficiently high level of authorization. Under more complex scenarios, however, in which the terrorist wishes to cause significant damage and achieve greater intimidation, considerable investment in the stages of the attack vector is necessary, as described below.

Lockheed-Martin, which fell victim to a cyber attack, offers a methodology for analyzing cyberspace attack operations, which it calls "the Cyber Kill Chain."[28] According to this methodology, a complex cyber attack comprises seven milestones, paralleling the actions of planning the operation and creating the attack vector. The first step entails collecting intelligence about the target. The right cyber weapon for the attack must then be selected and launched at the target. The next stage includes the exploitation of a vulnerability in the target computer that will make it possible to implant a malicious file on its system, followed by installing the tool in a way that will enable it to carry out operations within the system. The stage after that is to create communications between the tool and the attacker's command and control servers, so that the tool can be guided and a report obtained from it about events on the victim's computer. The final step in the cyber kill chain is the conducting of active operations from within the victim's computer, such as erasure, spreading of the tool, taking over the physical devices accessible from the computer, and the like. The term "Cyber Kill Chain" was chosen in order to emphasize that in order for the attacker to succeed in carrying out a cyber attack, he must successfully complete every milestone without being detected and without his access to the target being blocked.

A terrorist organization seeking to attack operational systems will have to carry out all the stages in the chain. These are advanced and complex operations, which terrorist organizations usually do not know how to implement by themselves. If the target is protected at a very low level, no great technological capability will be required of the attacker in order to create damage or achieve defacement. In most cases, however, the terrorists will have to acquire products or services from expert hackers. In other words, they will have to use "outsourcing."

Within the offensive cyber products market, terrorists will find accessible capabilities for a non-isolated target. In the same market, they will also find attack products, and presumably they will likewise find products for conducting operations on the target network (similar to the management interface of the SpyEye[29] Trojan Horse). Despite this availability, internet-accessible tools have not yet been identified for facilitating an attack on an organization's operational systems. Access to these tools is possible in principle,[30] but the task requires large-scale personnel resources (spies, physicists, and engineers), monetary investment (for developing an attack tool and testing it on real equipment under laboratory conditions), and a great deal of time in order to detect vulnerabilities and construct a successful attack vector.

## Types of Cyberspace Attacks

It is possible to identify a number of types of cyberspace attacks in accordance with both their level of expected damage and the scope of their intelligence, technological, and operational investment. In most cases, these two measures correspond with each other. The following review paints a picture of the capabilities of a non-state organization in cyberspace.

### *Amateur Attack*

This action is taken using tools that are (in most cases) known to information security companies and are identifiable by standard protection software programs. Defenses against these tools have been developed, and they are therefore likely to prove effective only against unprotected targets. Such tools are usually used only for research or gaming purposes because only in rare cases can they be used to steal valuable information or to sabotage protected computer networks. They have spy and sabotage capabilities, but these are not very sophisticated.

### *Minor Attack*

This is an attack in which not much effort has been invested. Most of its activity consists of searching on the internet for readymade tools or purchasing them from companies that specialize in them. Attacks of this type do not usually succeed in causing damage to entities that are attentive to information security (state, military, and advanced industrial entities), but they can penetrate private computers, steal information, and

sabotage them. In most cases, these attacks are one-time events (theft of an important file, erasing a disc drive), but they can also sometimes be part of an extensive attack, such as the theft of a computer's domain name system (DNS), which makes it possible to monitor its activity on the internet.

The tools used in a minor attack do not include the various software modules; they have a single inexpensive code component that carries out all the actions of the tool. This code component is written in a way that will not allow its capabilities to be easily altered or expanded, and it is target oriented. Through the internet anyone can obtain this type of limited-capability cyber weapon for a few thousand dollars at most.

This category also includes the use of botnet software agents for DDoS attacks. Creating the network is a more complex operation, but once it is created, it can be used for many DDoS operations. It can also be leased to others for denial of service from various websites lacking high-level protection against such an attack.

***Medium-Level Attack***

This is an attack capable of causing significant damage or carrying out advanced spy operations at a lower cost than that of a major attack (see below). Usually this operation does not use new, unique vulnerabilities (because these are very expensive); rather, it uses known or partially known vulnerabilities against which the target is not yet protected. The operation does not include expensive modules for implementation and testing such as those developed for Stuxnet. At the same time, by using modules for an attack on computer systems (erasure, disruption) and spy modules, such an operation can be very effective as part of a short-term attack for destructive purposes (because no effort will be made to conceal the destruction, which would be too expensive) or to spy on a victim whose systems do not have high-level protection.

A medium-level attack is much less costly than a major attack, as the former entails fewer man-years and does not require special, expensive hardware or the purchase of new and expensive vulnerabilities. An inexpensive vulnerability is sufficient for penetration of the victim's computer systems, bearing in mind that these are liable to be detected and blocked in the near future. The mid-level category also includes viruses capable of spreading throughout the computer network (worms) and waiting for an order from their operator. This attack model is particularly

useful in creating a network of software agent robots for DDoS operations. This category also includes a DDoS attack against protected websites, which requires sophistication from the attacker and familiarity with the protection system at the target.

*Major Attack*

This is an attack into which many personnel, computer, and monetary resources have been invested, and which has been thoroughly tested in the laboratory before being put into operation. This operation uses unfamiliar vulnerabilities, giving the attacker a long time to operate it before it is detected and shut down. The operation is usually camouflaged in order to leave few footprints. The software tool contains a number of modules, some of which are likely to be designed to sabotage the victim's special-purpose software or hardware systems (e.g., Stuxnet), and will never operate elsewhere, in order to reduce the possibility of detection.

A major attack operation is likely to entail a wide range of modules corresponding to the target it was designed to attack, such as spy modules – searching for files or information and sending the findings to the operator – and attack and camouflage modules – sabotaging centrifuges while misleading the control system, so that the latter will report that the former are in good repair. Such an attack involves many man-years, advanced computer resources, and sometimes hardware systems and testing equipment designed to simulate the theater in which the hostile code will operate, for example centrifuges with Siemens control systems in the case of Stuxnet.

Table 1 summarizes the differences among the various categories of cyber attack by listing the criteria that make it possible to distinguish clearly between types of cyber weapons according to the level of their capabilities. The parameters are divided into several categories. The first includes the cyber weapon envelope and its ability to reach its target and operate freely there without being blocked. The first two parameters are included in this category. Their importance lies in the comfortable work environment that they enable the attacker to enjoy, in the knowledge that he can penetrate his targets and carry out operations there whenever and however he requires, without fearing that his capability will be blocked or his weapon exposed and removed. The next three parameters constitute the second category, which pertains to the cyber weapon's ability to carry out its main activity

at the target, whether that be the theft of information, its destruction, or electronic or physical damage or disruption. The various weapons in this category are distinguishable by the algorithms that they apply in order to spy on the target, and by their ability to disrupt computer and physical systems. The ability to cause physical damage constitutes the highest level in this category. The final category represents the two parameters relating to the tool's behavior within the target's network, and the extent of its capability and the freedom that it grants to its operators to conduct the operation at the target. High-level capabilities in this category are those that make it possible to adjust the weapon by delivering modules from a distance and to change the definitions of the task, send orders to the tool, and define new intelligence targets for it. Sophisticated tools will also be able to manage a large data-collection operation on the target's network by spreading to other computers and collecting concentrated and coordinated information from them.

**Table 1. Differences among Cyber Attacks**

| | Major Attack | Medium-Level Attack | Minor Attack | Amateur Attack |
|---|---|---|---|---|
| Ability to penetrate systems | Very good | Good | Good | Poor |
| Ability to camouflage activity | Very good | Good | Mediocre | Poor |
| Spy capabilities | Very good | Very good | Good | Mediocre |
| Ability to damage computer systems | Very good | Very good | Good | Poor |
| Ability to damage physical systems connected to the computer setup | Good | Poor | Poor | Poor |
| Ability to spread | Very good | Good | Poor | Poor |
| Ability to communicate with a control server | Very good | Good | Mediocre | Poor |

The table indicates that the criteria significantly distinguishing major attack capabilities (which few countries possess) from other cyber attack capabilities are the ability to spread on the network, to communicate with the control server, and to damage physical systems connected to the computing systems. These operations require the greatest sophistication in conducting cyber attacks. Only a few countries have access to the

knowledge and the ability to produce a weapon of this type. The "minor attack" column in the table reflects the low entry level to the cyberspace battlefield. It appears that even small weapons in the hands of non-state entities are capable of penetrating computer networks well, performing espionage at a very high level, and if they are designed for it, also sabotaging the computer system that they have penetrated. Because their camouflage capability is mediocre, they are unable to reside in the attacked system for as long as heavy or medium weapons, and will therefore have to achieve their objectives within a short time.

## Activities in Cyberspace Attributed to Terrorist Organizations

This section examines terrorist operations in cyberspace in accordance with the above delineation, that is, operations whose purpose is to cause deliberate or indiscriminate harm to civilians through action in cyberspace by non-state organizations with political agendas and goals, even if operated or supported by states.

One of the first documented attacks by a terrorist organization against state computer systems was by the Tamil Tigers guerilla fighters in Sri Lanka in 1998. Sri Lankan embassies throughout the world were flooded for weeks by 800 e-mail messages a day bearing the message, "We are the Black Internet Tigers, and we are going to disrupt your communications systems." Some assert that this message affected those who received it by sowing anxiety and fear in the embassies.[31] Several years later, on March 3, 2003, a Japanese cult name Aum Shinrikyo ("Supreme Truth") conducted a complex cyber attack that included the obtaining of sensitive information about nuclear facilities in Russia, Ukraine, Japan, and other countries as part of an attempt to attack the information security systems of these facilities. The information was confiscated, and the attempted attack failed before the organization managed to take action.[32]

An attack through an emissary took place in January 2009 in Israel. In this event, hackers attacked Israel's internet structure in response to Operation Cast Lead in the Gaza Strip. Over five million computers were attacked. It is assumed in Israel that the attack came from countries that were formerly part of the Soviet Union and was ordered and financed by Hizbollah and Hamas.[33] In January 2012, a group of pro-Palestinian hackers calling itself "Nightmare" caused the Tel Aviv Stock Exchange and the El Al Airlines websites to crash briefly and disrupted the website activity

of the First International Bank of Israel. Commenting on this, a Hamas spokesman in the Gaza Strip said, "The penetration of Israeli websites opens a new sphere of opposition and a new electronic warfare against the Israeli occupation."[34]

The civil war in Syria has led to intensive offensive action by an organization known as the Syrian Electronic Army (SEA) – an internet group composed of hackers who support the Assad regime. They attack Syrian opposition groups using techniques of denial of services and information, or break into websites and alter their content. The group has succeeded in conducting various malicious operations, primarily against Syrian opposition websites, but also against Western internet sites. SEA's most recent action was aimed mainly against media, cultural, and news websites on Western networks. The group succeeded in breaking into over 120 sites, including *Financial Times*, *The Telegraph*, *Washington Post*, and *al-Arabiya*.[35] One of the most significant and effective attacks was in April 2013, when the Syrian Electronic Army broke into the Associated Press's Twitter account, and implanted a bogus "tweet" saying that the White House had been bombed and the US president had been injured in the attack. The immediate consequence of this announcement was a sharp drop in the US financial markets and the Dow Jones Industrial Average for several minutes.[36] The SEA is also suspected of an attempt to penetrate command and control systems of water systems. For example, on May 8, 2013, an Iranian news agency published a photograph of the irrigation system at Kibbutz Sa'ar.[37]

During Operation Pillar of Defense in the Gaza Strip in 2012 and over the ensuing months, the Israeli-Palestinian conflict inspired a group of hackers calling itself "OpIsrael" to conduct attacks[38] against Israeli websites in cooperation with Anonymous. Among others, the websites of the Prime Minister's Office, the Ministry of Defense, the Ministry of Education, the Ministry of Environmental Protection, Israel Military Industries, the Israel Central Bureau of Statistics, the Israel Cancer Association, the President of Israel's Office (official site), and dozens of small Israeli websites were affected. The group declared that Israel's violations of Palestinian human rights and of international law were the reason for the attack.

In April 2013, a group of Palestinian hackers named the Izz ad-Din al-Qassam Cyber Fighters, identified with the military section of Hamas, claimed responsibility for an attack on the website of American

Express. The company's website suffered an intensive DDoS attack that continued for two hours and disrupted the use of the company's services by its customers. In contrast to typical DDoS attacks, such as those by Anonymous, which were based on a network of computers that were penetrated and combined into a botnet controlled by the attacker, the Izz ad-Din al-Qassam attack used scripts operated on penetrated network servers, a capability that allows more bandwidth to be used in carrying out the attack.[39] This event is part of an overall trend towards the strengthening of Hamas's cyber capabilities, including through enhancing its system of intelligence collection against the IDF and the threat of a hostile takeover of the cellular devices of military personnel, with the devices being used to expose secrets.[40]

## Independent Cyber Attacks by Terrorist Organizations

Our analysis of attacks by terrorist organizations in cyberspace reveals that the low entry threshold for certain attacks and the access to cybernetic attack tools have not led the terrorist organizations to switch to attacks with large and ongoing damage potential. Until now, the terrorist organizations' cyber attacks have been mainly against the target organization's gateway. The main attack tools have been denial of service attacks and attacks on a scale ranging from amateur to medium level, primarily because the capabilities and means of terrorist organizations in cyberspace are limited. To date they have lacked the independent scientific and technological infrastructure necessary to develop cyber tools capable of causing significant damage. Given that terrorist organizations lack the ability to collect high quality intelligence for operations, the likelihood that they will carry out a significant cyber attack appears low.

In order for a terrorist organization to operate independently and carry out a significant attack in cyberspace, it will need a range of capabilities, including collecting precise information about the target, its computer networks, and its systems; purchasing or developing a suitable cyber tool; finding a lead for penetrating an organization; camouflaging an attack tool while taking over the system; and carrying out an attack in an unexpected time and place and achieving significant results. It appears that independent action by a terrorist organization without the support of a state is not self-evident. The same conclusion, however, cannot be

drawn for organizations supported and even operated by states possessing significant capabilities.

There is also the possibility of attacks by terrorist organizations through outsourcing. A review of criminal organizations reveals that they have made significant forward strides in recent years. The Kaspersky laboratory recently exposed a new group of attackers, apparently commissioned by criminal organizations or by a state for industrial espionage purposes. This is a group of hackers named "Icefog" that concentrates on focused attacks against an organization's supply chain (using a hit-and-run method), mainly in military industries around the world.[41] Another development is the distribution of malicious codes using the crime laboratories of the DarkNet network, which has increased access to existing codes for attack purposes. Criminal organizations are already using the existing codes for attacks on financial systems by duplicating them and turning them into mutation codes.[42]

There is a realistic possibility that in the near future terrorist organizations will buy attack services from mercenary hackers and use mutation codes based on a variation of the existing codes for attacking targets. This possibility cannot be ignored in assembling a threat reference in cyberspace for attacks on the gateway of an organization or even against its information systems. It is therefore very likely that terrorist organizations will make progress in their cybernetic attack capabilities in the coming years, based on their acquisition of more advanced capabilities and the translation of these capabilities into attacks on organizations' information systems (not only on the organization's gateway).

The ability to carry out an attack that includes penetration into the operational systems and causes damage to them is quite complex. The necessity for a high level of intelligence and penetration capabilities, which exist in only a limited number of countries, means that any attack will necessarily be by a state. For this reason no successful attack by a non-state player on the core operational systems of any organization whatsoever has been seen to date. Although no such attack has been identified yet, there is a discernible trend towards improvement of the technological capabilities of mercenaries operating in cyberspace for the purposes of crime and fraud. Presumably, therefore, in exchange for suitable recompense, criminal technological parties will agree to create tools that can carry out attacks on the core operational systems of critical infrastructure and commercial

companies. These parties will also be able to put their wares at the disposal of terrorist organizations.

## Recommendations for Measures at the National Level

The range of threats in cyberspace is extensive. Basic defenses against these threats need not substantively distinguish among the sources of threats. The notion that a defense can be devised in cyberspace specifically against threats from terrorist groups therefore appears impractical. On the contrary, the defense concept for threats of attacks in cyberspace by terrorist organizations does not, and cannot, differ substantially from an overall defense approach to threats in this realm.

The fundamental concept for defense against cyber threats must be based on a number of basic elements: intelligence, a multi-layer defense approach, an attack approach, public awareness, and civilian defense.

### *Intelligence*

The first basic element in defending against cyber threats is intelligence, including collection of intelligence based on guidance that takes situation assessments into account. In this context, it is important to identify threats and guide the parties collecting the intelligence with respect to information concerning terrorist groups seeking to operate in cyberspace. As noted, in many cases states are behind the activity of terrorist organizations, and intelligence gathered in the state context can also provide information for the terrorist organizations affiliated with or operated by it.

Intelligence constitutes an essential element, second to none, in dealing with threats in cyberspace. The ability to collect and analyze a large amount of information makes it possible today to create high quality intelligence both at the state level and, in more than a few cases, at the level of organizations and businesses that regularly monitor their information and communications networks for the purpose of detecting anomalous behavior that might indicate a future attack, or in order to discern irregular activity on the computer network. In this context, it is appropriate to emphasize that when a country – such as Iran – supports and sometimes even operates terrorist organizations, Western intelligence organizations should monitor not only the target country but also the organizations affiliated with it. In the context of Iran, this means monitoring Hizbollah, Hamas, and the "Syrian Electronic Army."

*A Defensive Approach Containing Several Layers*

This measure entails a perimeter defense as well as protection of critical assets, including the ability to maintain activity even after penetration by malicious code, and preemptive action against active parties, for example by disclosing intelligence information to law enforcement authorities in countries where the activity is taking place, or using legal tools in other countries. Such action could possibly disrupt the ability to operate the malicious code before it is distributed.

*An Offensive Approach to Threats*

This element in dealing with cyber threats includes two levels. The first pertains to the ability to take offensive action within – and sometimes also outside of – cyberspace through a preemptive strike against a terrorist organization's cyber resources (infrastructure, financing, websites, and operatives). The second level concerns the ability to conduct retaliatory actions after the attack, and after satisfactory identification of the parties responsible for the attack. Such a strike need not be confined to cyberspace; it can also include real physical elements. In some cases, a legal arrangement for the offensive activity is necessary in order to make the approach effective. In more than a few cases, a chain of operations can be identified if states (such as Iran) operate non-state organizations (such as Hizbollah and SEA), when all together they operate interested parties or even deceived parties within a network for the sake of bolstering their attack capabilities. The need to operate a broad system of attackers requires guidance in a number of contexts. The first involves determining the targets to be attacked, the second concerns the timing of the attacks, and the third pertains to the tools for carrying out the attacks. All of these require the establishment of websites and special forums to which the information is channeled. This activity creates vulnerabilities by enabling disruptive and deceptive action, thereby sowing confusion while softening the impact of the attack planned by its leaders.

*Explanatory Activity*

It can be assumed that explanatory activity will not be effective within the very hard core of cyber attack operatives. Preventative explanatory activity has two purposes. The first is to increase awareness of the possibility that attackers are liable to be harmed as a result of preemptive activity

in the country in which they reside (for example, their exposure to law enforcement authorities in that country). The second is the exposure of those behind the organization. As noted, in many cases, the attackers have been deceived and are completely unaware that they are being operated by states and terrorist organizations. It is therefore possible that these actions can reduce the scope of the phenomenon to some extent.

### *Organizing Civilian Defense in Cyberspace*

The vulnerabilities of the civilian cyber apparatus in Israel constitute a defensive gap inviting terrorist organizations to take advantage of it. The relatively weak defenses of these systems enable terrorist organizations to take simple action against targets in this sphere. Since civilian cyber systems create structural vulnerabilities, a civilian defense should be established in cyberspace, and the sooner the better. The recommendation of the Institute for National Security Studies to the Israeli government is that the defense of civilian cyberspace should be formulated so that it can provide a better solution to threats should be noted in this context.[43]

Terrorist organizations have not yet crossed the operational and technological threshold that would allow them to operate independently against Israel and other Western countries in the cyber warfare sphere. Developments in the criminal attack market, however, are liable to produce significant attack capabilities. These developments, combined with the support and guidance in intelligence and operations provided by technological powers like Iran, could lead to dangerous activity in the cyber field on the part of terrorist organizations. This threat, therefore, should not be taken lightly. Even though no significant activity by terrorist organizations in the cyber field has been observed yet, the development of the threat in this sphere requires appropriate organization.

## Notes

1 The authors would like to thank Noam K. from the National Cyber Staff and Doron Avraham and Keren Hatkevitz, interns in the Cyber Warfare Program at the INSS, for their assistance in preparing this article. Michal Aviad, *Documentary Film* (Tel Aviv: Heidekel, 2007), p. 5.

2 For example, see Haim Pass and Dan Meridor, eds., *21st Century Battle: Democracies Fight Terrorism, Study Forum* (Jerusalem: Israel Democracy Institute, 2006), p. 25.

3 For example, see Tor – a software program that helps create anonymity on the web. Every layer is encoded, and every station in the route folds its layer

and delivers it to the next station. This principle is called an "onion router," https://www.torproject.org.

4 Oded Yaron, "Hackers Plan Cyber Attack against Israeli Targets in April," *Haaretz*, March 14, 2013, http://www.haaretz.com/news/diplomacy-defense/hackers-plan-cyber-attack-against-israeli-targets-in-april.premium-1.509214.

5 "Steinitz: Military Threat against Israel has also Become a Cyber Terror Threat," *Globes*, July 9, 2013, http://www.globes.co.il/news/article.aspx?did=1000860690.

6 See the statement by Prime Minister Benjamin Netanyahu on this subject: "Netanyahu: Iran and Its Satellites Escalating Cyber Attacks on Israel," *Globes*, June 9, 2013 http://www.globes.co.il/news/article.aspx?did=1000851092.

7 This refers to any system for storing, transporting, or processing organizational information, whether or not it is connected to the internet, and whether or not it constitutes part of the organization's core business.

8 An organization's core operational system is the hardware on which the organization's core processes are managed and the software used for that purpose (whether it is a security or a civilian business organization). Disruption or destruction of such a system can halt all or part of the organization's activity and could cause physical damage in certain cases.

9 An industrial control system (ICS) is a tool that integrates software and hardware components and is designed to oversee a physical production process. The system contains sensors for monitoring the controlled process and inspectors who control this process. The system is also likely to include a connection to the organization's other computer networks and sometimes also to the internet.

10 This type of attack is also carried out independently by activists and anarchists, or on behalf of and guided by a terrorist organization.

11 "Shamoon Virus Targets Energy Sector Infrastructure," *BBC News Technology*, August 17, 2012, http://www.bbc.co.uk/news/technology-19293797.

12 In this incident, malicious code was inserted into Aramco's computer system, and 30,000 computers were put out of action as a result.

13 Ralph Langner, lecture on the subject of securing industrial control systems, Annual Cyber Conference, Institute for National Security Studies, September 4, 2012, http://youtube/sBsMA6Epw78.

14 "The Disturbing World of the Deep Web, Where Contract Killers and Drug Dealers Ply their Trade on the Internet," *Daily Mail*, October 11, 2013, http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html.

15 Jesse Emspak, "Why We Won't Soon See another Stuxnet Attack," *Tech News Daily*, July 24, 2011, http://www.technewsdaily.com/7012-stuxnet-anniversary-look-ahead.html.

16 Aditya K. Sood and Richard J. Enbody, "Crimeware-as-a-Service – A Survey of Commoditized Crimeware in the Underground Market," *International Journal of Critical Infrastructure Protection* 6, no. 1, (March 2013), http://www.sciencedirect.com/science/article/pii/S1874548213000036.

17 A Facebook page offering cyber weapons for sale can be found at https://www.facebook.com/groups/53807916899/.

18 Limor Kessem, "Zeus FaaS Comes to a Social Network near You," *RSA, Speaking of Security*, April 2013, http://blogs.rsa.com/zeus-faas-comes-to-a-social-network-near-you/.

19 Michael Fire, Rami Puzis, and Yuval Elovici, "Organization Mining Using Online Social Networks," *arXiv*:*1303.3741* .

20 Aviad Elishar, Michael Fire, Dima Kagan, and Yuval Elovici, "Homing Socialbots: Intrusion on a Specific Organization's Employee Using Socialbots," International Workshop on Social Network Analysis in Applications (SNAA), August 2013.

21 Fernando M. Pinguelo, Bradford W. Muller, Norris McLaughlin, and P.A. Marcus, "Is Social Media a Corporate Spy's Best Friend? How Social Media Use May Expose Your Company to Cyber-Vulnerability," *Bloomberg Law*, http://about.bloomberglaw.com/practitioner-contributions/is-social-media-a-corporate-spys-best-friend/.

22 Internet Census 2012, Carna Botnet, http://internetcensus2012.bitbucket.org/paper.html.

23 Map of SCADA systems in the world, http://goo.gl/maps/nqnan.

24 The Shodan website, which contains information useful to hackers: http://www.shodanhq.com/.

25 Gili Cohen, "Hackers Attack Home Networks of Hundreds of Israelis," *Haaretz*, September 11, 2013, http://www.haaretz.co.il/misc/2.444/.premium-1.2117098.

26 Attack vector: http://searchsecurity.techtarget.com/definition/attack-vector.

27 Spoofing attack: http://www.webopedia.com/TERM/S/spoof.html.

28 Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* 1 (2011): p. 80.

29 Doug Macdonald, "A Guide to SpyEye C&C Messages," *Fortinet*, February 15, 2011, http://blog.fortinet.com/a-guide-to-spyeye-cc-messages.

30 Thomas Rid, "Cyber-Sabotage Is Easy," *Foreign Policy*, July 23, 2013. http://www.foreignpolicy.com/articles/2013/07/23/cyber_sabotage_is_easy_i_know_i_did_it?pa.

31 Dorothy E. Denning, *Cyberterrorism*, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S House of Representatives, May 23, 2000, p. 269, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

32 For a chronology of the Aum Shinrikyo actions, see http://cns.miis.edu/reports/pdfs/aum_chrn.pdf.
33 Paul Everard, "NATO and Cyber Terrorism," in *Response to Cyber Terrorism*, (Ankara, Turkey: Center of Excellence Defence against Terrorism, 2008), pp.118-126.
34 Daniel Cohen and Aviv Rotbart, "The Proliferation of Weapons in Cyberspace," *Military and Strategic Affairs* 5, no. 1 (2013): 59-80 .
35 Dylan Love, "10 Reasons to Worry about the Syrian Electronic Army," *Business Insider*, May 22, 2013, http://www.businessinsider.com/syrian-electronic-army-2013-5?op=1#ixzz2h728aL8P.
36 Peter Foster, "'Bogus' AP tweet about explosion at the White House wipes billions off US markets," *The Telegraph*, April 23, 2013. http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.
37 Yanir Yagna and Oded Yaron, "Israeli Expert Said, 'Syrian Electronic Army Attacked Israel' – and Denied It," *Haaretz*, May 25, 2013, http://www.haaretz.co.il/news/politics/1.2029071.
38 Amir Buhbut, "Cyber Attack: Prime Minister's Office, Ministries of Defense, Education Websites Put out of Action," *Walla News*, April 7, 2013, http://news.walla.co.il/?w=/90/2630896.
39 Nimrod Zook, "Cyber Attack: Izz ad-Din al-Qassam Fighters Hit American Express," *Calcalist*, April 2, 2013, http://www.calcalist.co.il/internet/articles/0,7340,L-3599061,00.html.
40 Lee Yaron, "Defense Department Warns: Hamas Cyber Capabilities Stronger," *Bamahane*, November 14, 2013, p. 19.
41 "Kaspersky Lab Exposes 'Icefog': A new Cyber-espionage Campaign Focusing on Supply Chain Attacks," September 26, 2013, http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks.
42 For more on mutation codes, see Cohen and Rotbart, "The Proliferation of Weapons in Cyberspace."
43 Gabi Siboni, "A National Response to Civil Defense in Cyberspace," Viewpoint Paper for Decision-Makers, Institute for National Security Studies, April 2013, http://heb.inss.org.il/index.aspx?id=4354&articleid=5904.