The Strategy for Integrating the Private Sector in National Cyber Defense in Israel

Shmuel Even

In February 2015, the Israeli government approved the establishment of the National Cyber Defense Authority, which will constitute the state's operational arm for the defense of the civilian sphere against cyber threats. One of the state's challenges is to integrate the private sector in this activity, both as the main consumer of defense and as a participant in the defense system. This article proposes a strategy for the state's handling of this problem. In general, it is proposed that the state will defend the national cyberspace up to the organizational entry point, through close involvement with the organizations that generate cyberspace (computer companies, Internet providers). This will reduce the risk of cyberattacks affecting organizations and private homes. It is also recommended that the state should expand its involvement in the individual protection of organizations critical to the functioning of the private sector, establish national priorities, and also increase supervision, guidance, and incentives for those dealing in cyber defense in this sector.

Keywords: cyber defense, national security, Israel, strategy, civilian sector

Background

Israel regards threats in cyberspace with the utmost seriousness. Commenting on this question, Prime Minister Benjamin Netanyahu said in February 2015, "Cyber threats can paralyze nations. This is a strategic threat that can paralyze and hurt no less than other threats in various fields and we must be prepared for it on the national and international levels."[1] This statement was made in the context of the government decision to establish

Dr. Shmuel Even is a Senior Research Fellow at the Institute for National Security Studies.

the National Cyber Defense Authority, "which will have overall national responsibility for cyber defense and which will be gradually established over a three-year period."[2]

This decision, together with the rapid development of cyberspace in the past twenty years in every field of endeavor, raises the question of what the state's responsibility in cyber defense should be, and how the state should fulfill that responsibility. The point of departure for this discussion is that the interpretation of what happens in cyberspace and the government's responsibility for it is analogous to what has been done so far in the three-dimensional physical world and in the electromagnetic field on which cyberspace is based (hereafter, "physical space"), while making adjustments for the uniqueness of cyberspace, as we understand it.[3] As a rule, the state should bear responsibility for the defense of national interests, the needs of the population and the economy, and daily life in the country; the same is true in cyberspace. The problem is that the government currently exercises this responsibility in an extremely limited fashion in the private sector, which constitutes the vast majority of the population and the economy.[4] The private sector itself bears most of the burden for cyber defense, in contrast to other operational spheres on land, in the air, and on the sea, in which the security forces play a dominant role in the defense of the country. In an analogy to physical space, cyberspace resembles a situation in which every individual defends himself with locks and bars, but the state is not prepared to help him defend the roads that lead to his attack.

This article proposes a strategy to integrate the defense of Israel's national cyberspace with its private sector. Part A presents the basic data and a portrayal of the situation. Part B makes recommendations for a strategy to integrate the private sector and the defense of national cyberspace in Israel. Part C recommends that priorities be determined for government intervention in the private sector within the framework of this strategy.

Part A
Basic Data and Portrayal of the Situation

The Risks in Cyberspace for the State and the Private Sector

The greatest risks of the state in cyberspace are attacks against the defense establishment, government, civilian infrastructure, and the business sector by enemy countries, terrorist organizations, and nationalist organizations for the purpose of espionage, disruption, or destruction. The many threats and actual damage have become an acute national problem and are liable to have a profound effect on the state and the economy, including damage to governability, infrastructure, the supply of goods and services, growth, employment, and so forth. Reports of an Iranian cyberattack against Aramco, the Saudi Arabian national oil company, using the Shamoon virus in August 2012, highlighted the fact that Israel's enemies also have powerful cyber weapons.[5]

In the private sector the most common risks are cyberattacks against economic targets in order to engage in business espionage, embezzlement, fraud, and so forth as perpetrated by criminal parties, competitors, hostile employees, and information thieves. Agencies, companies of foreign governments, and agents on their behalf also commonly steal information. Business espionage in cyberspace at the national level deprives the country of its own intellectual property; Israel is exposed to this risk because it has a great deal of knowledge and intellectual property, especially in the high-tech sector, upon which economic growth is based.[6] In both the governmental and private sectors, the malfunctioning of computer systems (for example, when software is being replaced) or infrastructure used by those systems (e.g., power blackouts, communications malfunctions) is a frequent risk. Another risk in both sectors is damage caused by natural disasters, fires, and floods.

The "Cyber Defense" Concept

In 2015, Israel shifted from the concept of "security," as reflected in the "National Information Security Agency" to the concept of "defense," as reflected in the "National Cyber Defense Authority," indicating a changing attitude in this field. The concept of defense reflects massive and effective actions, in contrast to "security," which is a lighter and more passive action. Organizations in the private sector, however, still customarily use the concept of security, such as in the title "information and cybersecurity."

The defense of cyberspace or cybersecurity in organizations (hereafter, "cyber defense") can be defined as an array of operations designed to defend the organization and the state against the leaking of classified information through computer systems, damage to computer activity and equipment, and damage to embedded computer systems (power plants, control towers, and so forth) using computer systems. The computer system itself may not be damaged in an attack. Cyber defense refers to both the defense of cyberspace and its contents, and the defense of cyberspace against attacks passing through that space.

Cyber defense includes logical and physical defense of all types of networks and computer systems, together with their contents: the tools, technologies, data, storage components, and the links between these; the identities of the users; maintaining the ability to function – "business continuity" – in a situation of a cyber event (attack, malfunction, natural disaster); and the ability to return to full functioning as rapidly as possible after a cyber event. Cyber defense is also needed against remote (Internet) or medium-range (connectivity to wireless networks in an organization) cyberattacks, and against attacks from close range (physical connectivity to an organizational network, use of a collaborator within the organization, and the theft of computer equipment).

Information and cybersecurity in an organization combines two fields: logical defense of the computer systems and their content using software; and physical defense of the information, hardware, work environment, printed computer output, authorized access to information systems, authorization to enter the work space, telecommunications closets, and the building. Defense includes checking the reliability of the employees, training, and controlling the access to the computer systems. Defense of cyberspace means from inside and out, and of embedded computer systems. Simultaneously, the traditional physical information security that is not in cyberspace should of course continue.

The definition of the cyber defense concept was designed to create the broadest possible common denominator of the activities and interests of the various players in the government and private sectors. The distinctions listed above are important for the division of responsibility between the state and organizations in the cyber defense sphere. Some of these distinctions are used for internal organizational work between the information security manager, the security officer, and the human resources manager.

The Attribution Problem: Who Did It?

Addressing any problem requires knowledge of its origin. Due to the nature of cyberspace, it is difficult to prove the identity of the party to which an event can be attributed, whether it is a criminal attacker, a hostile country, or a malfunction. The context is also important, as it determines the extent of the state's involvement in dealing with the event and compensating those injured, as can be deduced from the physical world (for example, compensation for victims of terrorism and war damages). In more than a few cases, a comprehensive investigation can determine the cause of the event, the circumstances of the event, the attack signature, the method of operation, the way the operation was conducted, the tools used in the attack, the targets, and so forth. Even if this identification is not solid enough to meet a legal test, it can be enough to determine policy.

Right to Privacy in Cyberspace

The right to privacy in cyberspace, an extensive legal and ethical issue involving relations between government and individuals and between individuals and each other, has attracted a great deal of public attention.[7] For the sake of this discussion, it should be noted that state institutions are legally barred from operating freely in the IT systems of civilians and organizations, particularly in routine situations. This is one of the reasons why it is difficult to employ military cyber capabilities to battle in the local civilian cyberspace (in contrast, for example, to airspace). The agencies authorized to do so, such as the Israel Police and the Israel Security Agency, must do so in a limited fashion, and in accordance with the law. At the same time, the development of technologies, such as the ability to spot anomalies in cyberspace, make it easier to identify abnormal cyber events, even without using the particulars of personal information.

Characteristics of the Private Sector in Cyberspace

The private sector is the largest group in the country, and includes corporations and private business owners, public corporations not under government control, and civilians using cyberspace for their various needs. The private sector generates the state’s income from taxes and foreign currency, and also is the principal supplier of goods, services, employment, social activity, and so on. Without correctly managing the opportunities and risks in cyberspace, many companies will have difficulty in achieving their goals; some will lose their ability to compete, and will vanish from the market. It is therefore important to reduce the private sector’s exposure to the risks of cyber events, such as attacks, espionage, malfunctions; and disasters.

Private sector organizations whose activity relies almost completely on cyberspace are prominent. These include the financial sector, such as banks, insurance companies, investment houses, and credit card companies, and organizations that generate cyberspace, namely companies that provide computer services, communications, Internet services, and information security, as well as knowledge-intensive industries. Cyberspace has rendered the banks a strategic target for attack because the "production floor" and its products have become digital, with the world no longer operating on the basis of paper money. In these organizations, which are based completely on digital information, reconstruction of databases (including the backup systems) following damage is difficult, and sometimes totally impossible.

One example of a cyberattack on a financial system is the cyber break-in and theft of credit card particulars of about 40 percent of the residents of South Korea in January 2014. Thirty senior officials in various financial companies resigned following this event.[8] Another example is a cyberattack that was attributed to Iran and was carried out in late 2012 against dozens of American banks, but without long-lasting damage.[9] At this stage, there has been no known case of a bank collapsing as a result of a cyberattack (other than financial fraud committed by people on the inside using the organizational cyberspace). At the same time, it should be kept in mind that organizations do not have any interest in exposing damage from cyberattacks, due to fear that their reputations will be affected.

Together with this, the cyber threat to strategic organizations with physical infrastructure and production facilities prone to attacks using kinetic warfare has also increased. These include power plants; cement, food, pharmaceutical, and chemical factories; transportation and energy organizations, and so on. For example, following the cyberattack using the Shamoon virus, the Saudi Arabian oil company Aramco had to replace its computer systems (30,000 work stations and 2,000 servers).[10] The damage caused was heavy, but the company was able to return to full operation.

The private sector organizations defend themselves at the unit level, and not at the system level. Their organizational cyber defense strategy includes: designing the organizational cyberspace for defense, such as creating a secured inter-organizational network; preventing penetration into the organizational cyberspace from outside (the Internet) and from inside (workstations, connection points, employee loyalty); in the event of penetration, locating and neutralizing the penetrator, and restricting the penetrator's movement using tools in the defense system; managing cyberattacks; implementing a plan for business continuity in crisis events, restoration, and return to full functioning, learning lessons from the event, and strengthening defense.

The private sector has a number of roles in the national defense system. Its first role is as a consumer of cyber defense. Its second role is as a passive participant in the defense system by defending itself, monitoring traffic in its sphere (subject to regulatory provisions and privacy restrictions), and reporting attacks against it. Its third role is participating actively in defense through the industries and services sector in the information and cybersecurity realm.

Factors that Expedite and Delay Cyber Defense in the Private Sector

The general trend in the private sector is towards an increased awareness of cybersecurity; however, this sector is not uniform. The progress of cyber defense in an organization is dictated by delaying and expediting factors. It is important for the government to recognize these factors if it wishes to lessen the effect of the delaying factors and enhance that of the expediting factors.

The factors that expedite cyber defense in the private sector are numerous, and there is a need to protect the company's business activity and profits against the growing cyber risks (the primary interest). Direct exposure to cyber events, media coverage of the subject, and marketing efforts by cybersecurity companies also expedite cyber defense. Regulation, including existing regulatory instructions for information and cybersecurity in the financial sector and "guided concerns," as well as the establishment of functions for information and cybersecurity in organizations, all generate systematic activity and increased awareness. The overlap between the responses to a cyberattack and to traditional risks, such as averting computer malfunctions, preventing fraud and embezzlement, and ensuring data security, makes it possible to respond to several risks for the same cost. The development of risk management in organizations also contributes to the management of information and cybersecurity risks.

Many factors delay cyber defense in the private sector. Cyber defense incurs major financial costs that detract from the organization's profit and/or compete with other items in the organizational budget. Defense systems are sometimes perceived as a burden on the operational business activity: they slow down operational systems, introduce bothersome complex passwords, make it difficult to retrieve information, and are also not very user-friendly. The prevention is passive, and when it is successful, it does not necessarily win recognition even when organizations have software programs that detect and thwart attacks. The threat of damage in cyberspace is just another risk that an organization must manage, like the danger of losing market share, financial risks, risks of failing to comply with regulation, operational risks, and so forth. Regulation is burdensome – in certain cases, an organization is liable to act not out of belief in the regulation, but rather out of fulfilling a duty, and this is sometimes at the expense of more important defense measures. Organizations also express concern about damaging their reputations as a result of reporting cyberattacks.

Government Organizations Dealing with Civilian Cyber Defense

Israel's defense concept is based primarily on the IDF, with other security forces operating alongside it. Like other armies in democratic countries, the IDF is limited in its ability to operate in the cybersphere of the civilian sector. At the same time, analogous to physical space, it can be assumed that the IDF, and also the Mossad, have roles in defending the nation's cyberspace against enemies outside the country in the following ways: deterring enemies and rivals against cyberattacks by maintaining an ability to respond;[11] providing intelligence alerts to the local defense system about external cyberattacks; engaging in counter-operations against attacks originating outside the country; engaging in counter-attacks against the sources of the attack, or as a result of the attack.

The Security Forces

The intelligence organizations operating within the country, such as the Israel Security Agency (ISA), play a key role in the defense system against cyberattacks, including counter-actions and active operations. According to the ISA cyber defense department, "The struggle to defend Israel's critical infrastructure entities against cyberattacks is accompanied by a war of minds . . . the walls are definitely inadequate. Stratagems are also needed, as well as the use of double agents and other creative Internet inventions."[12]

The National Information Security Agency

The National Information Security Agency, which the government decided to establish in December 2002, operates within the framework of the ISA. Its job is defined as "being responsible for professional instruction for the guided agencies under its responsibility in the field of critical computer infrastructure security against threats of terrorism and sabotage in the area of classified information, and against threats of espionage and exposure."[13] The

National Information Security Agency instructs at least thirty-seven civilian entities in the government and private sectors, which are liable to attacks that could cause severe damage to the country. These include, among others, Israel Railways, Mekorot Water Company, the cellular companies, Israel Electric Corporation, Bezeq – the Israeli telecommunications corporation, El Al Israel Airlines, and Zim Integrated Shipping Services. Bezeq, El Al, and Zim are former government companies that were privatized.

The National Cyber Bureau

The National Cyber Bureau was founded in January 2012 in the Prime Minister's Office. Its main task is to be "a bureau for the prime minister, the government and its committees that recommends national policy in the cyber realm and promotes its implementation, subject to all law and decisions by the cabinet." The Bureau in effect bears overall responsibility for the cyber realm, including cyber defense. In this framework, the Bureau is responsible for carrying out situational assessments of civilian cyber defense; formulating policy; constituting a regulatory agency in cyber defense fields; and composing and publishing alerts, information, and instructions to the public on this subject.[14]

The National Cyber Defense Authority

As noted, the cabinet approved the establishment of the National Cyber Defense Authority on February 15, 2015. According to the cabinet press release, "The authority will oversee cyber defense actions so as to provide a comprehensive response against cyber-attacks including dealing with threats and events in real time. The authority will also operate an assistance center – a Cyber Event Readiness Team – for dealing with cyber threats to strengthen the resilience of organizations and sectors in the economy . . . The authority and the bureau will constitute a single national cyber directorate in the Prime Minister's Office, led by head of the National Cyber Bureau Dr. Eviatar Matania."[15] On the same occasion, the cabinet approved a number of policy measures to be carried out by the National Cyber Defense Authority in the future, including a plan to organize the cyber defense services market, including relevant professionals, products, and services; regulation of the evaluation of cyber defense within economic organizations, to be based on existing regulators; and a plan to assist economic organizations and provide incentive mechanisms designed to bolster their readiness for cyberattacks.

The Unit for Government Cyber Defense

On February 15, 2015, it was also decided to establish a unit for government cyber defense to offer professional guidance and directives for the government as a whole. The unit will also establish a government security operations center to operate in the event of cyber threats.[16]

The Bank of Israel and the Ministry of Finance

The Bank of Israel and the Ministry of Finance issue regulations to the financial sector, including in the cyber realm. The banks are regulated by the supervisor of banks. The insurance companies and other financial concerns are regulated by the Ministry of Finance.[17] In 2012, the Bank of Israel set up a unit responsible for the banks' operational risks, headed by technology and information security risks.[18] In early 2014, the Bank of Israel approved the founding of a joint center for cyber defense in the banks, to be coordinated under Shva (Automated Banking Services), a company controlled by the banks. At the same time, the Bank of Israel issued a draft circular to the banks on the subject of cyber risk management, requiring the banks to explain in detail how they were dealing with cyber threats, including formulating a strategy; establishment of a cyber defense system; restriction of access to information systems; development of a cyberwar room; reporting of cyberattacks to the Bank of Israel; and so forth.[19]

Israel Law, Information, and Technology Authority

The Ministry of Justice established the Israel Law, Information, and Technology Authority (ILITA) in September 2006. ILITA's goals are to strengthen the protection of personal information, regulate and supervise the use of the electronic signatures, and enhance enforcement of the laws against invasions of privacy. ILITA also serves as a knowledge center for legislation, and for projects with technological aspects, such as E-Government.[20]

The Israel Police

In November 2012, the police commissioner declared the establishment of a new cyber warfare unit. The declaration came on the heels of growing attempts by hostile parties to conduct online attacks on computer infrastructure in Israel and the spread of cybercrime.[21]

The Common Interests in Cyber Defense of the Government and the Private Sector

In general, the government and the private sector have a common interest in reducing cyber risks and dealing successfully with various types of cyber events. At the same time, each of the parties emphasizes different aspects of cyber defense. The government bears general responsibility for state security. Although it wishes to maximize defense, it is subject to a given budget, which dictates priorities, with a preference for national security above personal security. This includes the effect of a cyber event on the public interest, as government intervention will be greater when a larger number of people is affected by the cyber event.

Organizations in the private sector have an interest in reducing cyber risks to a level acceptable to their management and shareholders, taking into account the cost-benefit ratio while also complying with the regulatory requirements (existing in the financial sector, for example). Private companies in compliance with the law bear limited liability, if any, for damage that a country might suffer as a result of a cyber event, especially when it is an enemy attack. The private sector is concerned first and foremost with criminal actions, such as business espionage, outside crime, embezzlement and fraud by employees and suppliers, and cyber malfunctions that affect companies' functioning. Major fraud or a serious malfunction in a company is a greater risk than that of a cyberattack by the country's enemies, which is a collective problem of the entire business sector, and for which the government bears responsibility.

As mentioned, the situation for the government is the reverse. The government is more worried about a cyberattack by enemies, for which its responsibility is regarded as greater in comparison to a malfunction in a specific company causing damage on a similar scale. Nevertheless, the government and the private sector share a range of risks in the cyber field as well as many defense solutions unrelated to the type of attack and identity of the attacker, so that cooperation between the parties is necessary in any case. Each party has relative advantages in support of cooperation. For example, the government has an advantage in intelligence; broad connections with local organizations and foreign countries;[22] overall perspective; and organizational and regulatory capability to coordinate between all the players for the purpose of setting up and operating an optimal defense system. Organizations in the private sector, on the other hand, have numerous computer resources (in which sensors and defense systems can be placed, within the legal restrictions); the ability to provide the government with information and indications about attacks; technological capabilities needed to create means of defense; broad access to communications systems in the country; and an "army" of civilian cyber personnel who can be harnessed for the common goals.

One obstacle to full cooperation between the government and the private sector is that private organizations do not want to expose their cyberspace to government agencies ("Big Brother"), among other things, because of the need to maintain the privacy of their customers, suppliers, and employees, and due to the concern that their reputation will be damaged by reporting a cyber event. This is particularly true when the state does not offer them significant assistance in exchange. It can be assumed that the private sector expects the state to improve the level of nationwide cybersecurity without imposing any additional costs.

Part B
A Strategy to Integrate the Private Sector in National Cyber Defense

Deep structural change in the Internet and government regulation of internet traffic for the purpose of protecting society might dramatically change cyber defense; in the meanwhile, the state must find cyber defense solutions that can be implemented in the Internet. The goal of the strategy proposed here is to integrate the private sector in national cyber defense, both as a consumer of cyber defense and as a participant in the cyber defense system, in order to create optimal protection for the national cyberspace, while efficiently utilizing national resources.

Principles of the Strategy

Perimeter and Regional Defense in Cyberspace

The objective is for the state to create an optimally protected national cyberspace,[23] up until the "organizational point of entry," just as the state ensures, for example, a stable supply of electricity, clean water, well-paved roads, transportation, and so forth. This approach requires the state to give priority to entry points and nodes of Israeli cyber infrastructure; this includes instructing and closely supervising communications companies and Internet access providers in order to reduce the likelihood of remote attacks on cyber systems in organizations and people's homes. The objective is that cyber generators in the country will not merely defend themselves, but also will thwart attacks. The state will also augment its supervision of computer companies, information security services, and more in order to improve cybersecurity in general, including within the organizational cyberspace.

The State's involvement in Cyber Defense of Private Sector Organizations
The state will seek to improve the organizational cyber defense in private sector organizations, which exert a great influence on national security (in the civilian and defense spheres), in accordance with the priorities established. The state's involvement in instructing and aiding private organizations for the purpose of defense against extraordinary security and civilian threats will form another layer in their regular defense system currently used to cope with high-priority civilian threats (criminal activities, malfunctions).

A General Effort to Strengthen Defense in the Private Sector
The state will seek to strengthen the expediting factors and weaken the delaying factors in the development of cyber defense in the private sector. The state will employ regulation sparingly, after prior consultation with this sector. At the same time, it will provide special services and information based on economies of scale, an overall perspective, acquired expertise, and access to intelligence information and sensitive technologies (within the restrictions of information security). The state will recommend defense systems and methods to the private sector, provide warnings, advise, and even intervene in a crisis, all according to the priorities to be established. To complete the picture, the state will continue its national passive and active cyber defense operations.

Directions for Action

The directions for action in the proposed strategy are as follows:

1. *Mapping the national cyberspace and conducting a comprehensive risk survey of the private sector in cyberspace.* The various economic sectors and the connection between them should be researched in this framework. The risk factors should be analyzed, and the critical routes and points typical of each sector, and those shared by all should be identified. The survey will include the use of penetration checks, so that high priority can also be assigned to defend small companies at nodes that are critical

for national defense. In addition, lessons should be learned from the experience of other countries.

2. *Setting priorities for the State's involvement in cyber defense in the private sector*. The priorities will be set according to criteria formulated by the state in cooperation with the private sector. The priorities will be reflected in the level of the state's involvement in organizations in the private sector under various scenarios.
3. *Preparation of a work plan to reduce cyber risks*. This work plan will maximize the total planned national spending on cyber defense and the budgets allocated by the state for this purpose. The plan will include the private sector.
4. *Arranging responsibility, authority, and coordination between the government institutions and organizations dealing in cyber defense*. Given the list of governmental agencies relevant to civilian cyber defense and their tasks, it is proposed to determine or refresh the definition of the fields of responsibility of these agencies, the substance of the connections between them, and their connection to the private sector from a system-wide perspective. For example, the division of work and synergy between the ISA, National Cyber Bureau, and the National Cyber Defense Authority should be determined, as well as the role of the Ministry of Communications, under which the cyberspace generators operate, and the mechanism for clarifying disputes between the agencies.
5. *Arranging the responsibility, authority, and coordination between the organizations for external security dealing in cyber warfare.* It needs to be determined the agency responsible for the alert chain in cyberspace, which includes collection, research, generating of warnings, and their dissemination.
6. *The force of regulation.* Regulation should be simple, easy to enforce, and should have clear cost-benefit value. Excessive regulation in the private sector is liable to create additional costs that will detract from profit and jeopardize the survival of companies. The levels of damage that the state and the economy will suffer as a result of an attack on a specific organization will affect the force of regulation according to the priorities set. It is best to make cyber defense an exception in the antitrust field, so that business companies from the same sector can share information among themselves and cooperate in the area of cyber defense.

7. *Responsibility of private sector towards government.* The responsibility of the private sector towards the government needs to be established, for example, by reporting penetration of the organizational cyberspace to the authorities, suppliers, customers, and consumers under relevant circumstances.
8. *Providing incentives to companies and organizations for cyber defense*. Among other things, this includes subsidizing the monitoring of penetrations of the defense systems in organizations; consultation on policy and defense methods; acquisition of defense products recommended by the state; and support for companies developing special products and services for cyber defense.
9. *Setting standards for improved cyber defense*. Supervision, guidance, and incentives concerning cyber defense for businesses in the private sector should be stepped up. Companies providing cyber defense consultation, services, and tools should be checked and authorized.[24]
10. *Easing of bureaucratic restrictions*. The bureaucratic restrictions delaying cyber defense operations should be eased. The establishment of a national computer emergency response team (CERT) is a basic need that has been recognized for years, but the setup process reached the bidding stage only in 2015.
11. *Positioning the status of CERT*. Action should be taken so that the computer emergency response team becomes the link between the state and the private sector for the two-way transfer of information in the cyber field. CERT should provide a high added value to the private sector, and should be available in crisis conditions, so that it is perceived as a useful agency.
12. *Improved capability of organizations and the state in cyber defense in the private sector.* This should be subject to democratic values by means of legislative amendments; guidance for the private sector, such as having the employees sign a consent form concerning the company's intention to monitor their work stations; and increased use of technologies for spotting anomalies without exposing private content.

Part C
Setting Priorities for Government Involvement in the Private Sector

The need to set basic priorities for government involvement in cyber defense is important, due to the constraints of the state's resources. The concrete priorities will also be affected by situational assessments based on regular risk surveys, intelligence information, and other factors. The general principle is that the state has a special interest in cyber defense within the private sector in two situations: when there is a risk of a system-wide event that could negatively affect the entire country (economy, population, and so forth), and when there is a risk of an attack by an enemy. The government will give great attention to a risk involving both of these situations, and the most effective way of handling this risk will be the government's top priority.

The three main criteria for priority in government involvement in cyber defense in the private sector are the estimated expected damage,[25] the cause of the risk (an attack by an enemy or criminal enterprise, malfunction, disaster), and the cost of reducing the risk (in terms of time and money), compared with the expected damage. The basic priorities for cyber defense are examined below according to each of the criteria. The details presented (i.e., which type of organization should receive top priority in defense, and so forth) are designed solely in order to illustrate the method.

First Criterion: Expected Damage

The government has an interest in the private organizations – from both a prior regulatory perspective and in dealing with a crisis – whose damage will have a broad system-wide effect, regardless of the cause of the event (even a malfunction). The systems and organizations rated by the government as having a high priority in state involvement are likely to be in Priority A, large organizations and/or those with a very strong system-wide effect such as the following:[26]

1. *The cyber generators – Computer infrastructure and large computer organizations.* These organizations create the national cyberspace and link the country with the world. The state will give high priority in preventing attacks that pass through them. The high degree of concentration in the communications sector exposes Israel to major cyber risks, but also provides an advantage in defense.

2. *The financial system*. This includes banks and investment houses. In addition to their importance to the economy and society, high priority should be given to their defense as their primary activity takes place at the digital level; they are natural candidates for a cyberattack, because it is very difficult to attack them using kinetic means; and it is extremely difficult to reconstruct them following destruction of their databases and backup systems.
3. *Energy infrastructure.* Israel Electric Corporation (IEC), as a direct source of energy for the entire economy, is state-owned, but there are also privately-owned power stations. IEC is supplied with natural gas by the gas companies in the private sector. The oil refineries should also be included in this category.
4. *Air, land, and marine transport infrastructure.* Damage to the functioning of command and control systems in this infrastructure is liable to lead to disasters with many casualties. El Al and Zim are considered national carriers, even though they are not government companies.
5. *Water infrastructure.* In addition to the government company Mekorot, there are also private water suppliers. This category should also include Tahal Water Planning for Israel, which performs engineering work in the water sector.
6. *Food, agriculture, and pharmaceutical industries.* This private sector group plays a key role in the security of food and drug supplies during ordinary times and in emergencies.
7. *Hazardous materials.* This includes organizations that supply hazardous materials to Israeli industry, such as ammonia for cooling uses.
8. *Israel's intellectual property*. This criterion applies to high-tech industries, university research institutes, hospitals, and so forth.
9. *Leading companies in Israel* in national output, human capital, and exports.
10. *Critical suppliers.* This includes organizations that act as suppliers to critical government systems (sensitive databases of the defense establishment, the Ministries of the Interior and Justice, Israel Police, and so forth) and organizations to which the highest priority is assigned. This list should also include foreign suppliers.
11. *A specific sector or enterprise* for which information exists that it will be targeted for a concrete attack, or that it is actually attacked with extraordinary force.

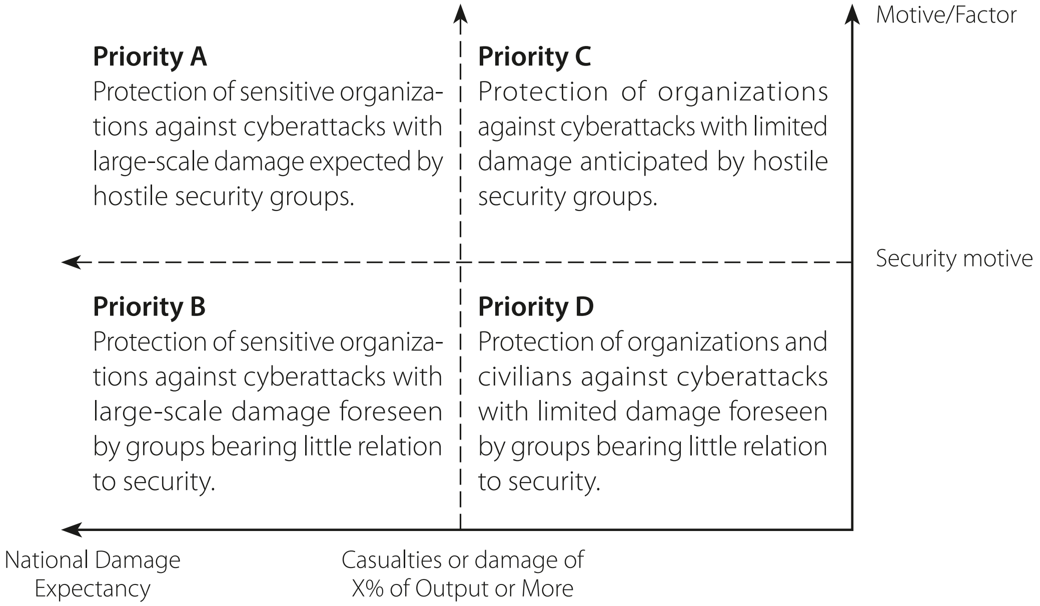
Priority B should be assigned to large organizations and/or organizations with major system-wide influence:

1. These include organizations from the sectors listed above (financial, communications, infrastructure, transportation, industry) whose influence on the nation and the economy is more limited than those with top priority;
2. Public or governmental services, with the exception of life-saving systems, which should be given top priority; private suppliers to the defense establishment, which do not have top priority, government organizations, and private organizations which are assigned top priority;[27]
3. The leading companies in Israel in national output, exports, and employment, which do not have top priority;
4. Important public databases (universities, research institutes); databases in advanced technology companies;
5. Systems and databases of hazardous materials, all which also do not have top priority.

Priority C includes medium-sized organizations of all types with a more limited influence on the country and the economy than those with the second highest priority. This includes non-governmental databases and public services, such as colleges. Priority D includes small businesses and ordinary citizens; this is the largest group of cyberspace users. An attack on personal security of exceptional scope is liable to become a national security problem, and a higher priority will therefore be assigned to negative events in cyberspace affecting large groups.

Second Criterion: The Cause of the Cyber Damage

In this criterion, the state assigns top priority to hostile parties operating out of security motives.[28] The state will give highest priority to an enemy cyberattack, due to its colossal responsibility for such a situation, in contrast to a malfunction, for example. The state's involvement is necessary because an enemy attack against a specific concern is likely to indicate a broader offensive, while organizations in the private sector are usually unable to cope with an attack by a sophisticated foreign group. Priority A will be assigned to attacks by criminal organizations specializing in cyberspace ("organized cybercrime"), and powerful earthquakes, as a result of the system-wide effect that such an event is liable to have. Priority B will be given to criminal elements, such as criminal groups, competitors breaking


Motive/Factor
Security motive
National Damage Expectancy
Casualties or damage of X% of Output or More

Priority A
Protection of sensitive organizations against cyberattacks with large-scale damage expected by hostile security groups.

Priority C
Protection of organizations against cyberattacks with limited damage anticipated by hostile security groups.

Priority B
Protection of sensitive organizations against cyberattacks with large-scale damage foreseen by groups bearing little relation to security.

Priority D
Protection of organizations and civilians against cyberattacks with limited damage foreseen by groups bearing little relation to security.

Figure 1: The Effect of the Security Motive on the Priority for State Involvement in Cyber Defense

the law, and attackers with other motives. Priority C will be assigned to natural disasters (although, as noted, a powerful earthquake will be assigned top priority) and other disasters (fires, for example). Priority D will be assigned to cyber malfunctions.

In more than a few cases, the question of attribution (who caused the event) is likely to arise. An uncompromising stand should be taken in such cases, taking cost-benefit into account.

Third Criterion: Cost-Benefit

The assumption is that it is right to invest the "extra shekel" in defense in order to reduce the damage. For example, if there are two industrial plants in which the expected damage of an attack on each one is equal, priority will be assigned to a plant in which risk reduction is quicker and cheaper. Another example is whether the provision of cyber defense in a communications company also reduces the cost of defense in organizations linked to the company, then it will be seen as cost effective. It is sometimes best to reduce certain risks that are not at the top of the list according to the above criteria, if these risks can be mitigated quickly and at low cost before they increase and spread.

Implementing the Priorities

The model presented above shows that in order to determine priorities for state involvement in the protection of a specific organization or groups of organizations, weighted priorities should be set, based on the three criteria. The state's priorities for organizations and the situation entitled to protection under Priority A and Priority B[29] means that the state will be deeply and directly involved in their cyber defense. This involvement, insofar as it is possible, will include the collection of intelligence, installation of means for identifying attacks, maintaining close connections with computer personnel in the organization, setting a rigorous policy and rules, enforcing the duty to immediately report all suspected cyber events, supervision, assistance in recovery, and so forth. Priority A will be reflected in greater state involvement in prevention, defense, and recovery in the context of an enemy attack. The state will require each organization assigned Priority C to adopt reasonable policy and rules, with occasional supervision of their implementation. These organizations will be in contact with the war room from which they will receive warning information with a low security classification. They will also be required to report suspected cyber events. Regarding organizations and situations in Priority D, the state will assist in public relations, in regulating and supervising the communications providers, and in protecting the public's information and so forth. These organizations will enjoy an improvement in the level of security in the national cyberspace as a whole.

Conclusion

National cyber defense in Israel is still far from crystallization and consolidation. The recommendation set forth in this article is to formulate a strategy for cyber defense in the private sector, based on a general principle that the state will supervise national cyberspace up until the organizational entry point. The state will implement this strategy by being involved in organizations that generate cyberspace in the country (computer and communications companies, Internet providers, and so forth), so that the chances of cyberattacks passing through them to organizations and private homes will be diminished. In addition, the state will impose supervision and regulation on "guided organizations" and others whose defense is critical for protecting the public and the interests of the state. The scope of this activity will be much greater than it is at present, with respect to the types of sectors in which the state is active, the number of guided organizations, and the range of solutions that the state can provide. In this framework, the state will assist these organizations and the public by providing information and referral to new technologies and up-to-date expertise. This shall be done according to the considerations of the public interest, and subject to security restrictions and protection of privacy.

Notes

[1] "Israel Establishes National Cyber Authority," *Bridges for Peace,* February 15, 2015, http://www.bridgesforpeace.com/il/news/article/israel-establishes-national-cyber-authority.

[2] "Cabinet Approves Establishment of National Cyber Authority," February 15, 2015, http://mfa.gov.il/MFA/PressRoom/2015/Pages/Cabinet-approves-establishment-of-National-Cyber-Authority-15-Feb-2015.aspx.

[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, June 2011), p. 15.

[4] The private sector includes all the entities in the country that are not under government control: Israeli citizens as individuals, non-government companies (both private and those listed on the stock exchange), non-profit corporations, and so forth. The government sector includes the government ministries and their institutions, the local authorities, government companies (the Israel Electric Corporation, Israel Aerospace Industries, and so forth), and other corporations.

[5] Amos Harel, "Assessment: Iran behind the Cyber Attack on Oil Companies in the Persian Gulf," *Haaretz,* September 11, 2012, http://www.haaretz.co.il/news/world/1.1821619.

[6] Shahar Argaman and Gabi Siboni, "Commercial and Industrial Cyber Espionage in Israel," *Military and Strategic Affairs* 6, no. 1 (March 2014): 43 – 58.

[7] "Cybersecurity Privacy Practical Implications," *epic.org,* May 31, 2015, https://epic.org/privacy/cybersecurity.

[8] Irit Avissar, "Senior Bank of Israel Official: We're Considering the Establishment of a Banking Cyber Center," *Globes*, January 24, 2014, http://www.globes.co.il/news/article.aspx?did=1000911843.

[9] "Iran's Cyber Attack against American Banks," *Ynet,* January 9, 2013.

[10] Harel, "Assessment: Iran behind the Cyber Attack on Oil Companies in the Persian Gulf."

[11] Ran Dagoni, "Yadlin: In Cyber Warfare, a Country Must Attack, not Just Defend," *Globes*, April 29, 2015.

[12] Yaron Rapaport, "The ISA in the Cybernetic Era: A Look from Within," *Israel Defense*, April 11, 2014.

[13] ISA website, http://www.shabak.gov.il/Pages/homepage.aspx.

14 "The National Cyber Bureau," Prime Minister's Office website, http://www.pmo.gov.il/branchesandunits/cyber/pages/default.aspx.

15 "Cabinet Approves Establishment of National Cyber Authority."

16 Ibid.

17 Instruction for Management of Information Security Risks of Financial Institutions," Ministry of Finance – Capital Market, Insurance, and Savings Department, October 16, 2006.

18 Avissar, "Senior Bank of Israel Officials: We're Considering the Establishment of a Banking Cyber Center."

19 Irit Avissar, "Bank of Israel to Banks: Appoint Manager for Defense against Cyber Attacks," *Globes,* July 21, 2014, http://www.tbk.co.il/article/3120778.

20 ILITA website, http://index.justice.gov.il/Units/ilita/Odot/Pages/Odot.aspx.

21 "Police Setting up New Cyber Warfare Unit, *Channel 2 News*, November 12, 2012, http://www.mako.co.il/news-israel/local/Article-a65e89befe3fa31004.htm.

22 Eviatar Matania and Tal Goldstein, "The Goal: Global Cooperation against Cyber Threats," *Israel Defense*, June 2013.

23 The national cyberspace is defined as an area in the global cyberspace in which the state has the ability to exert sovereign influence on the way communications, computer, and Internet infrastructure are set up, managed, and operated, while emphasizing access to this infrastructure and freedom to transmit information on it.

24 When the market in this matter is unscreened, and the consumer is unable to assess the quality of the service, the consumer and related parties are liable to be exposed to cyber risks, including damage when checking a penetration.

25 The expected damage is the estimated damage to the country in the event of an attack, multiplied by the estimated (subjective) likelihood of an attack at the current level of defense. The estimated likelihood is also based on intelligence obtained. The estimated expected damage is therefore dynamic.

26 Several of these organizations are already included in the list of critical infrastructure organizations, as instructed by the National Information Security Agency. At the same time, many organizations and certain economic sectors are not included in this list.

27 A cyberattack can be made against an organization through its suppliers, and even through its customers (if they are hooked up to the organizational network), but the organization is able to defend itself against such attacks. An organization can therefore be rated as top priority, while its suppliers may be rated only the second highest priority.

28 It can be assumed that countries have highly developed and repeat capabilities in cyberspace, compared to unorganized attackers, although exceptions are certainly possible.

29 A given organization can be assigned Priority A under one security scenario and Priority B under a different scenario.