Protecting Critical Assets and Infrastructures from Cyber Attacks

Gabi Siboni

The impact of computer and communications systems in recent decades has not bypassed the national security of states in general, and the State of Israel in particular. Most systems in developed societies rely on computer and information infrastructures, and this growing dependence on information and communication technologies means that a blow to computers and information flow processes is liable to disrupt, paralyze, and sometimes even cause substantive physical damage to essential systems. Computer-based capabilities and their near-global ubiquity expose states to harm in cyberspace by various elements, including hostile countries, terrorist organizations, criminal elements, and even individuals driven by personal challenges or anarchist motives. The threat is particularly acute as management, control, and monitoring systems can be disrupted through changes to a computer program, and no physical attack is needed. Thus, it stands to reason that the face of future conflicts will be transformed beyond recognition.

The strength of a sovereign state is a function of economic, societal, and scientific strength combined with military strength, and the purpose of the military strength is to protect the state's territory and its citizens so that they can cultivate and maintain economic strength. The vulnerability of computers and communications systems to cyber attacks entails a dramatic change in the concept of military strength. For the first time, it is possible to mortally wound national economic strength by paralyzing economic and civilian systems without using firepower and force maneuvers. Thus, the ability of states to operate in cyberspace for

Dr. Col. (ret.) Gabi Siboni is head of the Military and Strategic Affairs Program at INSS and head of the Cyber Warfare Program at INSS, supported by the Philadelphia-based Joseph and Jeanetter Neubauer Foundation.

both defensive and offensive purposes coincides with classic military capabilities to play a significant role.

In the past two decades, states, along with their progress, profitability, and wellbeing – and their production and provision of national services in particular – have been exposed to new threats, yet insufficient attention has been paid to the appropriate means of confronting such threats. In the recent past, industry (private and public) was protected by the state. For example, excluding workplace accidents, power stations producing electricity, whether in private hands or publicly owned, were exposed to physical damage only if the state encountered a physical war, and it was the state's job to protect such infrastructures along with economic institutions, industrial facilities, and so forth. Public institutions were protected by the state by virtue of their existence in the territorial space under its authority and control. That has changed. In addition, the trend in recent decades to privatization has placed a large portion of the infrastructure plants that were traditionally in the hands of the government in private hands, including those relating to communications, transportation, electricity, energy, and heavy industry. Moreover, traditional industries have in recent decades been joined by new industries in the hi-tech realm that constitute a significant component of states' GDP.

Due to the universal understanding that "he who defends everything defends nothing,"[1] various countries have developed ways of protecting infrastructures and systems that are critical to their functioning. In 2002, the State of Israel established the Information Security Authority, "in charge of professional direction of the bodies for which it is responsible regarding securing essential computer infrastructures from the threats of terrorism and sabotage to the security of classified information, and from the threats of espionage and exposure."[2] In this context, a steering committee was established in the National Security Council whose role is to examine the risks in information security. It was also decided that the rules of the steering committee would apply to a number of bodies and institutions whose information systems are defined as critical, including the electric company, banks, government offices, and the like, and the committee is authorized to add to this list.[3]

The public service bodies that are required to protect themselves from a cyber attack have been under the direction of the Information Security

Authority for quite a while. At the same time, changes in the structure of the Israeli economy and the emergence of elements, processes, assets, and projects – which if damaged could potentially cause significant harm on a national level – have exposed and increased the range of weak points and the targets for cyber attacks. Moreover, potential damage is not restricted to what can be quantified in financial terms or what impacts on the GDP: significant damage can also be caused to assets and values that have Israeli and Jewish national importance. Thus, for example, in the United States, defensive plans also apply to heritage and memorial sites.[4]

Consequently, it is highly important to be able to examine which additional entities require guidance by the Information Security Authority. This article proposes an approach that will make it possible to implement a systematic process using existing statutory tools, in order to identify other bodies (mainly from the private sector) whose damage might impact on national security, and therefore requires them to operate appropriate defensive mechanisms for their critical assets and infrastructures.

What Should be Protected?

In a US Department of Homeland Security document,[5] Patrick Beggs[6] reviews how authorized officials in the United States see the interface between defense-critical infrastructures and resources and their physical and cyber infrastructures.

In the United States, the mapping of defense-critical infrastructures covers water, energy, communications, transportation, the chemical industry, agriculture and the food industry, information systems, banking, commercial and financial services, health services, and finally, areas of importance to the American collective memory (national monuments, heritage sites, and so on). These sectors are grounded on two basic infrastructure components: the first regards physical infrastructure components, such as power stations, dams, airports and sea ports, roads, railroads tracks, various types of delivery infrastructures,[7] hospitals, factories, and the like. The second component concerns cyber infrastructures, including software and hardware systems, internet servers, command and control systems, and information systems.

In order to enable an appropriate basis for formulating defense plans, the US uses a methodology called Cyber Resiliency Review (CRR) of institutions and critical infrastructures that belong to the sectors described above. This approach makes it possible to assess a number of aspects, including the definition of defense-critical assets, management of communications, continuity of services, technological management, dependence on external components, management of unforeseen incidents and accidents, ability to assess the situation, and identification and management of weak points. From this review, decision makers can formulate a plan of action to improve the cyber resiliency of the organization.

The process is organized and well ordered once the organization or body is identified for review through this methodology. However, lacking is an effective way to identify these bodies and organizations. The situation in Israel is fairly similar. From time to time, the Information Security Authority brings additional bodies to the steering committee of the National Security Council that will need to examine and meet the agreed upon guidelines. At the same time, there is no binding systematic statutory process that allows these organizations to be identified.

Because an area or a sector that constitutes a critical national infrastructure comprises a large number (hundreds, and sometimes thousands) of organizations and systems, protecting a "sector" is meaningless. Rather, in practice, protection entails actions taken by specific organizations, companies, facilities, and processes. Therefore, the question is how is it possible to locate these bodies, since almost every company or government office interfaces with sectors that are defined as defense-critical infrastructures. For example, protection of water supply and water quality infrastructures in Israel does not only affect processes in Mekorot, Israel's national water company, but also dozens of other water suppliers, associations, water corporations, desalination and delivery facilities, sewage and wastewater treatment facilities, and so forth. A large number of these facilities are operated by private entrepreneurs who do not see activating protective mechanisms as a top priority. The situation is similar in other industries.

Furthermore, in many cases it is also necessary to protect interfacing systems that are connected to the supervised bodies. For example: an industrial factory that has been declared an essential component of a particular sector works under the direction of the Information Security Authority. Sometimes this factory is dependent for its operations on other manufacturers (smaller satellite manufacturers) that supply input (sometimes critical) for the production process of this protected factory. In many cases, some of these satellite manufacturers are not included in the group of critical infrastructures for protection and therefore they do not use satisfactory information defense processes. Thus, it is possible that cyber damage to one of these manufacturers will cause significant damage to a protected factory.

The use of information technologies in Israel is widespread, both in the public and the private sectors. As such, Israel offers a wide range of targets for a potential cyber attack. Therefore, identifying additional bodies for guidance by the Information Security Authority is an essential task for building an optimal defense system. Reviews taken from time to time and information from various government offices are essential to this process, but they are not sufficient. A built-in mechanism must be created that will allow a significant improvement in these processes, especially concerning certain projects in the private sector that if exposed to cyber damage could suffer extensive damage that might have an impact on national security.

The Proposed Process: Use of Existing Statutory Tools

The principal proposal aims to make cyber protection a built-in component of the existing statutory process, both in the establishment stages (i.e., the approval of the projects in the various planning commissions) and in the operational process (the business licensing law). It is proposed that in the framework of the national planning processes, every project submitted to the planning commissions for approval will be required to submit a Cyber Resiliency Assessment. This assessment will constitute the main statutory tool for examining the project's exposure to the possibility of cyber attacks and the measures protecting against these exposures. This assessment will also provide the Information Security Authority a tool for identifying and managing the critical infrastructures for defense. At the same time, in the framework of the business license, which is a license requiring periodic renewal, the relevant authority can check the ongoing compliance with cyber protection instructions of the body under review.

The establishment of every project in Israel, including national infrastructure projects, requires compliance with the customary processes of statutory planning. Thus, projects that are required to build facilities and structures must be approved by various planning commissions in accordance with the relevant regulations on the local, regional, and national levels. Review of the planning documents submitted for approval is the planning authorities' central tool of control over these projects. Among the documents submitted for review by the planning commissions today are reports concerning firefighting, public health issues, environmental aspects, handling of hazardous materials, home front defense, and so forth. These documents define the steps that the project initiator will take in order to comply with the necessary requirements in each of the areas described above. These steps are then relayed to the authorized regulatory authorities, which employ experts to ensure that at the end of the process, the project is implemented with public interests in mind and that public security is maintained throughout the various spheres. In Israel, dozens of projects that if damaged might harm national security are discussed every year, including infrastructure facilities, water and sewage treatment facilities, delivery systems, transportation projects, energy facilities, and communications. Expansion and establishment of industrial factories and a wide range of other projects are discussed as well. Cyber damage to some of the projects and ventures is liable to harm the country's economy, not only directly, such as through the inability to supply an essential service, but also in the form of commercial damage, e.g., the inability of Israeli companies that were attacked to supply their products for a given period.

An example that clarifies the proposed process is the requirement to submit an Environmental Impact Assessment. The goal of the assessment is to identify the environmental hazards that are likely to be caused by the project, along with ways to minimize this damage to a tolerable level. Submission of the review is anchored in the planning and building regulations (of 1982, and in its final version of 2003). The idea for this review originated in the enhanced public awareness in the United States of environmental issues, which in 1970 led to legislation requiring preparation of an Environmental Impact Assessment as part of the planning process.

Together with the planning component of new projects, it is also possible to make use of the business licensing process, which requires periodic renewal to ensure that over the years the project meets the necessary criteria in various spheres, including protection from cyber attacks. According to Justice Mishael Cheshin, "the goal of the [business licensing] law is to preserve and protect various values that our society considers important . . . such as the value of public safety, with the value of maintaining public health and safety, and the value of preserving the environment and quality of life . . . protecting the goals of society."[8] Use of the tools provided by the business licensing law for cyber protection and upholding its goals provides the Information Security Authority with an additional legal tool to ensure that existing activities are required to meet the necessary criteria. In certain cases, there has even been a demand of private business owners to submit a Cyber Resiliency Assessment and a requirement to meet security guidelines.

Projects in the pre-establishment process and in certain cases those that have already been set up will be required to submit a Cyber Resiliency Assessment to the Information Security Authority, which can ensure that essential protection instructions are followed. A number of guidelines can be proposed for the content of this assessment and for those authorized to submit and those authorized to check it. From a statutory point of view, the review process must be applied comprehensively and govern all requests, unless the authorized authority grants an exemption. However, from a practical point of view, the Information Security Authority will be required to draft criteria that define the projects and ventures for which an assessment must be submitted. These criteria could address a number of components, such as the size of the project, its sector (for example, the energy sector, natural gas, and the like), the project's interfaces with elements already under the purview of the Information Security Authority, and the expected damage in the event of a cyber attack.

When a decision is made that the body must submit a Cyber Resiliency Assessment, the process will adhere to a defined procedure, as follows:

a. *Assessment guidelines*. It is the responsibility of the Information Security Authority to prepare guidelines for carrying out the assessment. These guidelines must be suited to the project or the specific body and cover a number of components, including: mapping the potential damage from a cyber attack; mapping the weak points of the project/plan; and issuing instructions that will make it possible to minimize exposure and damage.

b. *Assessment preparation*. The assessment will be prepared under the auspices and with the funding of the project initiator. For this purpose, there will be consultants from a group of designated consultants trained and authorized by the Information Security Authority. These consultants will work according to the assessment preparation guidelines.

c. *Checking the assessment*. By virtue of its responsibility, the Information Security Authority can use external advisors trained and authorized to check the reviews, with the cost charged to the project initiator. In this process, it is possible that there will be a number of rounds of questions and answers between officials in the Information Security Authority and the party under review.

d. *Approval of the assessment*, meaning examination and review by the authority's officials and a decision on guidelines in this context for the project. This approval can also address aspects of the stipulations for the business license, as well as instructions that should be applied to the project initiator's plans.

Similarly, the business licensing law also constitutes an appropriate platform for implementing instructions and guidelines in the realm of protection from cyber attack. Due to the restrictions applying to the security and flow of information, it will be necessary to define this process as a departmentalized process that is not open to the wider public, but only to specific authorized officials.

Conclusion

Threats to civilian companies have grown not only because of increased competition in the marketplace but also because of their exposure to attacks by hostile elements. Hostile parties identify the potential damage to the country's economic infrastructure inherent in attacking these companies. States tend to protect mainly bodies that have a direct connection to national security, which traditionally included primarily government offices; intelligence and security bodies; organizations engaged in sensitive classified security manufacturing; and classical critical infrastructures, such as electricity, water, transportation, and so on. The logic that defined the criterion of this privileged class was derived from the classic strategic concept: a list of national infrastructures susceptible to disaster in the event of war, and which if damaged could cause direct harm to the country's fighting ability and resiliency. However, what will be the fate of civilian companies such as

Teva Pharmaceutical Industries, or food manufacturing companies such as Tnuva, the Strauss Group, and the like? And what of cable companies and insurance companies, not to mention memorial and heritage sites? A quick examination shows that damage to these organizations is liable to cause significant damage to the country and harm the fabric of civilian life.

The establishment of the Information Security Authority and the steering committee of the National Security Council were first steps in the right direction. Now, with the increasing realization that cyberspace is becoming a combat zone before our eyes, the ability of the State of Israel and its economy to weather attacks of this type must be enhanced. Introducing cyber defense in the statutory processes can allow ongoing, systematic monitoring of the immunity of Israel's cyber security system.

Notes

[1] This saying is usually attributed to Frederick the Great.

[2] The website of the Information Security Authority, http://www.shabak.gov.il/about/units/reem/pages/default.aspx.

[3] Gal Mor, "Plan for Information Security Approved by Government," *Ynet*, December 11, 2002, http://www.ynet.co.il/articles/1,7340,L-2310234,00.html.

[4] Patrick Beggs, "Securing the Nation's Critical Cyber Infrastructure," US Department of Homeland Security, February 25, 2010.

[5] Ibid.

[6] Patrick Beggs is the director of Cyber Security Evaluations – National Cyber Security Division in the US Department of Homeland Security.

[7] The term "delivery systems" serves to describe infrastructures that conduct materials: water, sewage, waste water, gas, oil, electricity, communications fibers, and the like.

[8] Justice Mishael Cheshin, Criminal Appeals Authority (CAA) 4270/03, State of Israel vs. Tnuva.