Critical Infrastructure Protection against Cyber Threats

Lior Tabansky

Introduction

A functioning modern society depends on a complex tapestry of infrastructures: energy, communications, transportation, food, and many others. This article discusses the developing cyber threat to critical infrastructure while focusing on several dimensions: aspects to the threat that require an interdisciplinary approach; defense against the threat; the existing Israeli response; and the developing challenges. An informed public debate is likely to lead to improved protection of national infrastructures in the civilian and public sectors.[1]

The article begins by defining the subject of critical infrastructures, and discusses the origins, uniqueness, and innovativeness of the threat to them. It then discusses levels of coping with the threat, using conceptual parallels to the world of military content. The existing Israeli response will be reviewed briefly, with an emphasis on the central challenges the cyber threat poses to public policy. Finally, directions for future research and action will be presented.

What are Critical Information Infrastructures

An infrastructure is a system that combines various facilities and enables certain activities, for example, a pipeline that conducts water from wells to homes and fields, paved roads, bridges and intersections that allow movement of people and goods, flight, communications, fuel, and health services. One of the properties of an infrastructure is the dependence of

Lior Tabansky is a Neubauer research associate working on the Cyber Warfare Program at INSS, which is supported by the Philadelphia-based Joseph and Jeanette Neubauer Foundation.

various spheres of activity on it. In the past, the dependence stemmed from physical or geographical relationships only. With the development of cyberspace, which includes data communication systems and computerized methods of automatic command and control, there are additional relationships, which in turn create further vulnerability. These are computerized relationships (for example, command and control by remote electronic means) and logical relationships (such as the international financial market as a factor influencing inputs and outputs of critical infrastructures), which are innovations that would not exist without information technologies. It is therefore worth distinguishing between infrastructures in the traditional sense and the modern use of this concept, which includes a cyber dimension.

In the information age, traditional infrastructures become information infrastructures because they incorporate computers. In addition, new critical infrastructures have been created that are purely information infrastructures: computerized databases that contain important data, such as records of capital in the banking system, scientific and technical intellectual property, and the programmed logic that manages production processes and various business processes. In the information age, the concept of "infrastructure" also includes computerized components, and thus "infrastructure" today necessarily refers to an information infrastructure.

Infrastructure is defined as critical when it is believed that disrupting its function would lead to a significant socio-economic crisis with the potential to undermine the stability of a society and thereby cause political, strategic, and security consequences. Different countries have offered a variety of definitions of critical infrastructures.[2] What all have in common is the existence of a computerized element upon which other physical systems are dependent and which, if harmed, would likely cause widespread damage in physical terms.[3]

Three factors can define a critical infrastructure. The first is the symbolic importance of the infrastructure. Thus, several democratic countries include heritage sites, museums, archives, and monuments among critical infrastructures that should be protected from cyber threats.[4] Another source of symbolic power is the perceived control of a government. For example, a hostile disruption of traditional media used by the state for communicating with its citizens will immediately harm the government's

ability to function. Moreover, in the longer term, such disruption may diminish the citizens' confidence in the existing government, or even the general form of government or regime.

The second factor is the immediate dependence on infrastructure, such as the electricity grid or telecommunications network, which is obvious for most processes in society. The emergence and prevalence of cyberspace created a situation in which computerized networks constitute an infrastructure in and of themselves. Cyberspace is a representative example of an infrastructure that has become critical because of the interface of most of society's activity with computerized communications networks.

The third factor involves complex dependencies. The accelerated trend toward adding connectivity capabilities enables unanticipated effects beyond the local level (the "butterfly effect").[5] The relationships among various infrastructures are presumably not fully known, and the failure of one component is liable to cause a wide range of results and damage. The types of failure fall into three classes:

a. *Common cause failure*. For example, various facilities (fuel storage, airports, and power stations) that are located in geographic proximity are likely to be harmed from a single incident of flooding. It is hard to imagine a cyber attack that would directly cause a failure of this type.
b. *Cascading failure*. Disruption of a control system in one infrastructure (for example, water) leads to disruption of a second infrastructure (for example, in transportation, the flooding of a railway line), and then a third (for example, food supply chain) and so on, even if it is not directly dependent on it. A cyber attack could directly cause such a failure.
c. *Escalating failure*. Disruption of one infrastructure (for example, a communications network) harms the effort to fix other infrastructures that have been damaged by another entity (emergency services, commerce).[6] A cyber attack could directly cause this type of failure.

The commercial aviation sector, which has attracted the attention of enemies of the developed states and prompted noticeable acts of hostility – hijacking of commercial planes, the September 11 attacks, and other terrorist attacks using civilian airplanes – can illustrate the importance of critical infrastructures and the significance of an attack on them. Civil aviation is a basic infrastructure for developed societies: in 2009, commercial air transport carried more than 2 billion passengers on 28

million flights on 27,000 airplanes operating from 3,670 commercial airports around the world.[7] In addition to commercial flights, military aircraft (some unmanned) also populate the skies. Intra-state laws, regulations, and procedures, along with international cooperation, regulate the administrative aspect of the airline industry. Airports are connected to each other through scheduled air traffic, and the air traffic control system in each given location is part of the international aviation infrastructure. Air traffic control is based on computerized systems: methods of detection, monitoring, surveillance, automation, communications, command and control, and so on. Disrupting the proper functioning of air traffic control systems would harm all air traffic.

The Novelty of the Threat

Recent years have brought increased concern over the potential vulnerability of the infrastructures that are the basis of developed modern societies,[8] yet the fact that this discussion is taking place now is surprising. Critical infrastructures have always been critical and their importance is obvious. International and internal conflicts are not new to the world, and in war it is reasonable to anticipate attempts to harm the adversary's critical infrastructures with the goal of weakening and defeating it. In 1917, during the Bolshevik Revolution, Lenin and Trotsky ordered their activists to take over the post office, telegraph systems, bridges, and train stations. In prolonged wars, such as the Second World War, attempts have been made to harm critical infrastructures in order to interfere with the enemy's fighting ability and spirit.[9] A country's critical infrastructures, whatever they are, are elemental targets during a conflict, and therefore organizations and states have labored throughout history over defense systems for their infrastructures: camouflage, guarding, fortification, defensive forces, deterrence, and so on. Why, then, is there a growing fear of damage to critical infrastructures, particularly in the strongest countries?[10]

A critical infrastructure is a tempting target for an enemy, be it a terrorist organization or a hostile state. However, the developed countries currently enjoy total military superiority over their respective enemies. The US and Europe have not experienced wars on their territories in recent decades. Israel is the only developed country that is under ongoing military threat that is manifested in a variety of ways (missile attacks in 1991, rockets in the north and south of the country,[11] and suicide bombers in 2000-

2005). Several developed countries have been harmed by hostile acts that directly attack the civilian population by circumventing the military that was supposed to protect it. The terrorist attacks could not threaten the countries attacked, but they did succeed in causing a change in their policy in one way or another.

In all forms of traditional warfare, the identity of the enemy is disclosed following the attack because in order for the attack to be carried out, the weapons must physically reach the target. In the event of a missile launch as well, there is no doubt as to the location of the launch site. The hijacking of commercial aircraft in the 1970s, the suicide bombings in Israeli population centers, the attacks in the United States in September 2001, and the attacks in Madrid in 2004 and London in 2005 all required the attackers to be physically present at of the attacks.

Identifying the enemy is critical for response and deterrence. Thus what prevented harm to critical infrastructures in the past was the defensive force placed in the path of the enemy, and even more so, the deterrence that promised to exact a heavy price. This familiar state of affairs came to an end with the development of cyberspace. For the first time in history, it is possible to attack strategic targets (such as critical infrastructures) without physically being in the place where they are located, without confronting defensive forces, and without exposure. In today's reality, the existing computerized infrastructure can be exploited through penetration of communications networks or the software or hardware of the command and control computers in order to disrupt, paralyze, or even physically destroy a critical system.[12] The threat stems from the vulnerability inherent in the properties of cyberspace,[13] and because of these special characteristics, the cyber threat challenge differs fundamentally from the challenges of traditional threats.

Levels in Confronting the Threat

This article focuses on the cyber threat to the computerized part of the infrastructures, based on the realization that such a threat has become possible, available, significant, and is liable to disrupt the functioning of developed society.

Confronting the threat to critical information infrastructures includes prevention, deterrence, identification and discovery of the attack, response, crisis management, damage control, and a return to full function. When

examining ways to confront threats to national security, the accepted practice is to divide the discussion into the tactical, operational, and strategic levels. Proposed here is a division of methods for confronting the threat to critical communications infrastructures into a number of levels: technological, technical-tactical, operational, and national-strategic.

The technical level focuses on an organization's computerized system, which is the most common activity in this realm. Given the large volume of activity, the technical aspect of "information security" is often emphasized, though it is actually a concept that deals with both defense of critical infrastructures and cyber security in general. In addition, activity that examines the issue from a comprehensive national perspective, referred to below as the national level of cyber security, is underway.

All the levels are required to confront the threat, but given the different focus, it is worthwhile distinguishing between these levels of protection. The proposed division will help identify the essence of the challenges of protecting critical infrastructures particular to cyber security.

The Technical Levels: Tactical and Operational Levels

Since the threat is derived from the properties of computer technologies, the response to the threat is generally sought among computer experts. As expected, the proposed solutions are also based on computer technologies. The problem is perceived as a technical problem, and therefore, the proposed solution is an engineering solution. The technical and operational levels for confronting the cyber threat, which come from engineering, mathematics, and computers, focus on identifying vulnerabilities in an organization's computerized systems and seek an engineering solution that reduces this vulnerability.

Table 1 displays common issues confronted by the technical levels of protection.[14]

The primary means of attempting to build resilience[15] is to invest in backup, redundancy, air gap, and the like. Accordingly, important computer systems are built twice, in separate locations, in order to enable continued function in the event of physical damage to the system.

Today, most solutions to the engineering problems identified are implemented through the private market. Information security is a wide ranging field, and describing it is beyond the scope of this article. In the division proposed here, information security lies in the technical-

Table 1. Types of Vulnerability and Responses

Vulnerability	Response
Access passwords for devices and systems are not changed from the default.	Password management
Passwords are saved and sent without encryption.	
Access passwords are not changed periodically.	
Physical security is lacking.	Physical access security
People who do not deal with critical equipment have access to it.	
Faulty management of user permissions gives a low level employee access to a critical process.	Computer access security
A firewall configured improperly allows unnecessary types of communication.	
The process network is not separated from the office network.	
The possibility of remote access to the computer system has been left open.	
The computer system can be accessed from a wireless network.	
The remote access process uses an open protocol and weak passwords.	
The manufacturer of the system supplied security updates but they were not installed in the system.	Configuration management
Administrator rights were given to regular users.	
Access to critical system components was not monitored; no log information was collected.	
Information log is not checked on an ongoing basis.	

operational levels. Information security is a developing discipline that brings together many resources for research and development, consulting services and outsourcing, a security product industry, and the like. The worldwide information security market is expected to grow, and some market analysts claim (perhaps with some exaggeration) it will reach $125 billion in 2015. Most of these revenues will go to US and European

companies that offer combined solutions of technical goods and services, together with technological-business consulting.[16]

The issue of cyber security, and especially of critical infrastructure protection, came about as a result of technological change. At first, it was expected that the solution to a problem of technical origin would be technical. However, there is a growing understanding that this problem cannot be dealt with on a technical-operational level only, since a precise engineering formula for dealing with the cyber threat is not possible: society's structure, values, and institutions are integral parts of the environment.

The Top Level: The National Strategic Level

The national strategic level examines the threat to critical infrastructures in the framework of national security, with a national focus that goes beyond the boundaries of an organization or a business process. This approach sees the protection of critical information infrastructures as part of the protection of society as a whole. Protection of information infrastructures actually becomes protection of an information-based society.[17] Information security, which is at the center of the technical level, is a necessary but by itself insufficient part of the strategic vision. The highest national level is based on technical and operational foundations, but in a broader approach it is not sufficient to fix local problems of organizational systems. As in the military, the strategic level needs an appropriate operational level, but this is not sufficient to achieve the strategic goal.

In a wider national perspective, a comprehensive national policy on protecting critical infrastructures is needed, which in addition to the engineering foundations will take into account the complex social, political, economic, and organizational aspects. An organizational entity capable of taking into account the complex of relationships between critical infrastructures and a functional society and the state is also required. The national level of protection requires cross-organizational activities, backed by effective authority. Without a doubt, this is a complex challenge for public policy, considering the structural limitations of public service on the one hand and a required level of strategic focus of those in the private sector, on the other. Just as the state defends its entire physical space, it also sees an increasing need to protect cyberspace fully, in spite of its special characteristics, which make the task more difficult.

Issues for Policymakers

The information revolution continues to change the strategic environment, and it affects a range of social, cultural, and economic issues in complex ways. Cyber security, and in particular, protection of critical infrastructures, is already on the agenda. The development of cyber threats to a national security issue makes governments into the main customers of protection services. Even limited experience shows that there are differences in the framework of the discussion and the types of solutions proposed in different countries, in spite of the great similarity in the source of the threat. Since the threat is similar, the explanation for the differences must be the role social institutions play in the discussion and in determining the response. What follows are the main issues concerning cyber threats that call for a public debate.

Which infrastructure is critical?[18] Any discussion on protection and defense measures must begin with prioritization. Assessing and measuring the level of the threat to components, computers, and systems is a necessary precondition for effectively confronting the threat. The exact sciences and engineering have mathematical methods for measuring the relationships and the dependence between components and the system. These tools are also used in the technical levels of protection of critical infrastructures. Nevertheless, more comprehensive methods are needed for assessing risks that stem from the intricate relationships among complex technological systems that critical infrastructures contain.

An assessment of how critical an infrastructure is on a national level must address the full matrix of social values, goals, and interests. Therefore, the relative importance of infrastructure and the amount of public investment needed to protect it are not derived from an engineering formula, and require a wide ranging and informed public discussion. Representative political institutions are the place for such a discussion in a democratic society. Given the constraints of the political system, such a discussion will presumably be lengthy and at times frustrating. Nevertheless, only through a joint political process will it be possible to design an optimal response to the threat for the long term.

Cyber vulnerability: technical issue, economic risk, or security threat? What is the potential significance of the growth of cyberspace in general, and the harm to critical cyber infrastructures in particular? The topic clearly goes beyond the scope of computers, engineering, and information

security to the question of the role of the state in cyber protection of critical infrastructures. Is this task military, partially civilian, "homeland defense," or civilian-commercial? The answer directly affects the solution proposed, and it has wide political, budgetary, and organizational consequences. Until recently, the common assumption was that this is mainly a technical issue, and the response therefore was placed in the hands of computer experts. Commercial companies provided technical solutions for the military, commercial, and civilian sector, and governments did not play a significant role. Today it is clear that the optimal answer can be found only in a joint discussion between various sectors in society because it is derived from the values of the society, its political and social structure, and its national security concept.

A political process for finding the balance between the values of freedom, market ideology, and security requirements: Critical infrastructures and the information necessary for their proper functioning affect all areas of a citizen's life. They raise many issues that affect civil rights, such as privacy, confidentiality, and due process; the relative strength of the state, citizens, and corporations; and allocation of public funds. Therefore, the central challenge in designing a policy to protect critical infrastructures from cyber threats is not technical or operational, rather a challenge of a comprehensive national-strategic vision. Critical infrastructure protection is not the exclusive preserve of systems engineers and computer experts. The optimal response to the cyber threat in general and the threat to critical infrastructures in particular will be created only through a broad public discussion in the framework of a democratic political system.

The private market and cyber security: The cyber threat is affected by the decentralized nature of economic activity in an era of rapid technological change, globalization, and privatization. The global market economy has created the situation in which large parts of the critical infrastructures are privately owned.[19] The unprecedented mutual dependence in international trade is one of the prominent expressions of globalization and privatization. The industrialized nations import most of the raw food that their citizens consume and export finished products and services. Food retailers do not keep inventory beyond several days' worth of typical consumption, and they depend on the continued undisturbed function of the extensive logistical supply chain to satisfy demand within a short time.[20] Given that disruptions in food supply would be a grave problem of wide social

implications, this supply chain could be perceived as a "critical information infrastructure" and become an urgent policy issue.

Open societies[21] with free economies shy away from state intervention in business processes. In the world of free markets, any attempt at government intervention in market processes is viewed with suspicion. Thus, for example, the arguments against government regulation of the internet originate with the ideology that goes along with a free market. The solution adopted thus far was focused on regulation: in the United States, since the mid-1990s detailed standards have been developed and adopted for securing information in various sectors and industries,[22] and organizations for supervision and control have been established. However, the world financial crisis of 2008 illustrated the dangers of private ownership of critical infrastructures, even if subject to regulation.

In the past year, the critical infrastructures protection policy in the United States has shifted from an emphasis on market mechanisms and voluntary "private-public cooperation" to a model that gives the government broad powers to guide business institutions and supervise implementation.[23] Israel too has regulation of critical infrastructures, and there was a proposal to expand it to small businesses.[24]

The computer products market and cyber security: The state of the market in this area is not encouraging. Security is secondary, as opposed to quick time to market. Furthermore, it is much more difficult to make the effort necessary for resilience and reliability testing in a private commercial environment, because achievements are measured by the length of time it takes to receive a return on the initial investment and the reduction of expenditures not connected to the core activity, and there is protection of limited liability only. Today, manufacturers of computer systems have no incentive to invest in increased reliability and protection. Security is seen as an external function, an addition to the core system, sometimes from another manufacturer that does not receive the cooperation of the original manufacturer.

The level of reliability and information security in most software, hardware, and computer system communication is thus lacking today, and this broad vulnerability has undoubtedly contributed to the rise of the cyber threat. Security systems must be easy for any user to operate, require minimal computer resources, and not harm the functionality of the core system or the user experience. Given the legal, economic, and competitive

circumstances, it is difficult to expect productive voluntary cooperation between private companies in these fields. However, nationalization is not the answer, nor should it be expected as a condition for increasing cyber security. In light of the cyber threats, what is needed is developing government policies to direct the market towards a greater level of security overall.

The Israeli Response

Securing sensitive information and protecting computer infrastructures are not new issues for the State of Israel, and there are Cabinet decisions dating back to 1996 on defense against cyber threats.[25] The format for protecting computer infrastructures was laid out in decision B/84 of the Ministerial Committee on National Security, "Responsibility for protecting computerized systems in the State of Israel" on December 11, 2002. To this day, this decision serves as the basis of the Israeli response to the cyber threat to critical information infrastructures. The response mandated by the decision includes establishment of a steering committee which, from time to time, examines the identity of the institutions that it is critical to protect, and the establishment of a government unit to protect civilian computerized infrastructure, the Information Security Authority[26] (RE'EM). RE'EM was established within the Israel Security Agency (Shabak) in order to comply with legal restraints on government intervention in business, since by law only civilian authorities, such as the police or the GSS, can intervene in private businesses. RE'EM oversees IT security in institutions that have been defined as critical: provides guidance, oversees implementation, and is authorized to institute sanctions against those that violate its directives. The institutions bear the costs of the protection required. Other important institutions that are under the responsibility of a government ministry operate according to RE'EM professional guidelines but are not legally overseen by it. The IDF and intelligence community protect their specific infrastructures independently, with RE'EM formal guidance

In comparison with the situation abroad, it appears that at the time this decision was made and implemented, Israel was relatively advanced in designing and implementing protection of critical infrastructures on a national level. However, cyberspace has continued to develop rapidly since then, and new systems and relationships have developed that cannot necessarily be defined as critical national infrastructures. One

example is small and mid-sized businesses dependency on commercial communications providers and open internet. The bloom of commercial and consumer "cloud computing" applications raises new issues and indicates yet again the increasing importance of cyberspace in all realms of life.

The Israeli policy for critical infrastructure protection was set up nearly a decade ago and served it well. Nowadays it may lack a comprehensive view of the interconnectivity developing in cyberspace that serves all civilian commercial activity. It is therefore worth reexamining the existing and anticipated challenges and the desired response. Last year, the government launched a National Cyber Initiative to advise the government on cyber security issues.[27] The National Cybernetic Task Force, an expert committee of academics and practitioners working under the auspices of the National Council for Research and Development in the Ministry of Science and Technology, formulated recommendations.[28] On August 7, 2011 the government of Israel decided:

> To work to promote the national capability in cyberspace and to better confront the current and future challenges in cyberspace: to improve protection of national infrastructures that are critical for normal life in the State of Israel and to protect them, to the extent possible, from cyber attack, while promoting Israel's status as a center for developing information technologies, encouraging cooperation between academia, industry, and the private sector, government ministries, and special institutions...Accordingly, pursuant to decision number B/84 of the Ministerial Committee on National Security, dated December 11, 2002, and without prejudice to the authority given to any other party under any other law or Cabinet decision [it is decided]:
>
> 1. To establish a national cyber headquarters in the Prime Minister's Office.
> 2. To arrange responsibility for handling the cyber field.
> 3. To promote the ability to protect cyberspace in Israel and to promote research and development in the cyber field and in supercomputing.[29]

The Cabinet decision is likely to lead to improved regulation for an Israeli response to the cyber threat in general, and the threat to critical infrastructures in particular.

Conclusion

The renewed discussion on critical national infrastructure protection focuses on the cyber dimension. Since all infrastructures have been affected by the information revolution and all now include computerized components that are mainly for command and control, this rapid technological change has created a new, additional security threat. The nature of cyberspace allows an attacker to disrupt the functioning of critical infrastructures without being physically near the target and without risking unequivocal discovery by the party attacked.

Although at first glance it appears that the subject of protecting critical information infrastructures belongs in the realm of computer engineering, upon further examination it becomes clear that it should be expanded beyond the technical aspect. Indeed, the major challenge in protecting critical infrastructures from cyber threats is not technical, but strategic and political. Today most states have legal and technical regulation for selected sectors. Since 2002, through the oversight and guidance of a particular organization, the State of Israel has been protecting infrastructures it deems critical. However, the development of cyberspace has left its civilian and non-critical sectors unprotected, and at the same time, raised both the level of vulnerability and the potential severity of effects. The recommendations of the new National Cyber Initiative are expected to set a policy process in motion.

The cyber threat to critical infrastructure is perhaps the most significant issue in the realm of cyber security. Only a thoughtful, informed process can design a policy of effective critical infrastructure protection from cyber threats and thus reduce the risk confronting the State of Israel and other developed countries from cyberspace. The major recommendation, therefore, is to broaden the public discussion of cyber security to include social and cultural aspects, which will make it possible to cope with the threat optimally on a national-strategic level with a comprehensive national perspective.

Notes

1 This article was written before the launch of the National Cyber Initiative, which also dealt at length with the topic discussed here. However, the recommendations of the National Cyber Initiative have not yet been released publicly.

2 Critical information infrastructures are systems and facilities whose destruction or interference (by means of computers) would: "a. cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction; b. impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety; c. undermine State and local government capacities to maintain order and to deliver minimum essential public services; d. damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services; e. have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or f. undermine the public's morale and confidence in our national economic and political institutions." See U.S. Government, White House, Homeland Security, Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003, http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#content.

3 Elgin Brunner and Manuel Suter, *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies* (Zurich: Center for Security Studies, ETH Zürich [Swiss Federal Institute of Technology], 2008); John Moteff, Claudia Copeland, and John Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical?* (Washington, D.C.: Congressional Research Service, Library of Congress, 2002); Myriam Dunn, "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)," *International Journal of Critical Infrastructures* 1, no. 2-3 (2005); U.S. Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2009*, http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm; Tyson Macaulay, *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies* (Boca Raton, FL: CRC Press, 2009); Robert Radvanovsky, *Critical Infrastructure: Homeland Security and Emergency Preparedness* (Boca Raton, FL: CRC/Taylor & Francis, 2006).

4 For example, Australia and the United States, which are countries that clearly attribute great importance to their political history as a central element in their collective national identity and social and political strength. *International CIIP Handbook 2008/2009*, Table 1; U.S. Department of Homeland Security, U.S. Department of the Interior: *National Monuments & Icons: Critical Infrastructure and Key Resources, Sector-Specific Plan,* 2010, http://www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf.

5 This refers to a tenet of chaos theory describing how tiny variations affect complex systems. The chaos theory attempts to describe the phenomena through mathematical methods.

6 Harm to the government's level of functioning, which harms services to citizens, creates escalation: public confidence in the government drops, and this is liable to be expressed in political change (a change of government in a representative regime) or even regime change (a revolt against an

authoritarian regime or a change in the structure of the regime in a democracy).

7 IATA (International Air Transport Association), *Air Transport Facts (2009),* http://www.iata.org/pressroom/facts_figures/fact_sheets/Pages/economic-social-benefits.aspx. The IATA represents 93 percent of scheduled air traffic in the world.

8 The United States was a pioneer in this field, initiating a discussion on the presidential level in 1996: United States, President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection* (Washington, D.C.: U.S. G.P.O., 1997).

9 In the "strategic bombing campaign" in World War II, the allies concentrated their aerial effort on attacking German factories producing ball bearings and lubricating oils, refining facilities, and railroad junctions. The operation was intended to harm the critical infrastructure for weapons manufacturing.

10 The United States has led the response to cyber vulnerability since the mid-1990s, having enormous technological and military strength and being the only superpower.

11 Since 2001, terrorist organizations have launched rockets and mortars from the Gaza Strip at towns in the Negev. The rockets have thus far caused nineteen deaths, and the mortars ten, and they have seriously disrupted life in the region. Following an escalation, Israel launched Operation Cast Lead in December 2008, which ended with a military victory. High trajectory fire from the Gaza Strip continues to this day, although there is less than before the operation.

12 The feasibility of using cyber means to cause physical damage has been shown in experiments. A CNN broadcast that discussed the Aurora experiment, ordered by the US Department of Homeland Security and conducted at Idaho National Labs, noted that broadcasting instructions to the command and control system of the electricity generating system caused a generator to stop working and then to explode.

13 Following is a summary of the challenges stemming from the characteristics of cyberspace as it exists today: the major vulnerability of computerized systems; the difficulty in distinguishing between a glitch and an attack, making the connection between an event and the result, tracing the source of the damage, and identifying the attacker, even if the source of the damage is known; and the widespread use of off-the-shelf commercial technologies. For a discussion of cyberspace in the context of national security, see Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2011): 75-92.

14 Jason Stamp et al., *Common Vulnerabilities in Critical Infrastructure Control Systems* (Albuquerque, NM: Sandia National Laboratories, 2003), http://energy.sandia.gov/wp/wp-content/gallery/uploads/031172C.pdf.

15 Resilience is the system's ability to absorb an attack and return to proper function quickly. In computerized systems, the result is achieved by restoring the original situation (going back in time) or by quickly adjusting to new constraints (adaptation).

16 See http://www.strategyr.com/Information_Security_Products_and_Services_Market_Report.asp.

17 James Der Derian and Jesse Finkelstein, "Critical Infrastructures and Network Pathologies: The Semiotics and Biopolitics of Heteropolarity," in Myriam Dunn Cavelty and Kristian Søby Kristensen, eds., *Securing "The Homeland": Critical Infrastructure, Risk and (In)Security* (London and New York: Routledge, 2008).

18 There is a great difference between the definition of critical infrastructure and the means taken to protect it in the various countries. See Brunner and Suter, *International CIIP Handbook 2008/2009*. The civilian aspect of protection of critical infrastructures in Israel is grounded in the Laws to Regulate Security in Public Places, 1998. The law authorizes the General Security Services to instruct various public institutions in physical security, information security, and essential computer system security, according to details appearing in annexes to the law. This law set punishments for failure to follow its instructions, including a civil fine and incarceration. In 2003, the government Information Security Authority was established, which is "charged with professional guidance of the institutions under its responsibility in the area of protecting critical computer infrastructures from the threats of terrorism and sabotage, in the area of classified information security, and in threats of espionage and exposure." See http://www.shabak.gov.il/about/units/reem/pages/default.aspx.

19 Most public transportation in the United States and more than 85 percent of the country's energy sector are controlled by private commercial companies. Some 85 percent of the communications of the US Defense Department uses commercial networks. See http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/energy1.htm.

20 The State of Israel, by virtue of its geopolitical situation, keeps an inventory of food and equipment in order to assure the needs of the economy in an emergency. The Supreme Emergency Economy Authority – Food and General Economy, which is part of the Ministry of Industry and Trade, is the body responsible for this issue today.

21 This concept comes from philosopher of science Karl Popper. See Karl Popper, *The Open Society and its Enemies* (Routledge: 2011).

22 See, for example, the publications of the US National Institute of Standards and Technology, http://csrc.nist.gov/publications/PubsFL.html, as well as the electrical standards of the North American Electric Reliability Corporation (NERC), CIP-002-3 through CIP-009-3, http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217.

pdf and http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf.

23 CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C.: Center for Strategic and International Studies, 2011).

24 Gabi Siboni, "Protecting Critical Assets and Infrastructures from Cyber Attacks," *Military and Strategic Affairs* 3, no. 1 (2011): 93-101.

25 See, for example, Cabinet decision1886 BK/9 from March 20, 1997: Establishment of a steering committee on computerization in every government ministry; Cabinet decision 3582 BK/77 from March 16, 1998: Responsibility for the subject of information security in government ministries; Cabinet decision 4956 BK/179 from March 23, 1999: Establishment of a council to secure sensitive information in the Prime Minister's Office; Cabinet decision TM/80 from November 26, 2000, on responsibility for computer information security in the IDF and cooperation with civilian authorities; Cabinet decision TM/14 from July 18, 2001: A secure internal network for government ministries.

26 http://www.shabak.gov.il/about/units/reem/Pages/default.aspx.

27 The National Cyber Initiative deals in part with the subject of protecting civilian cyberspace.

28 The committee recommended establishing a national cyber headquarters to report directly to the Prime Minister, with a budget of NIS 100 million; establishing an office to deal with the country's infrastructure and the civil sector; policy and regulatory change to encourage the cyber industry; encouraging cyber R&D; developing centers of excellence and encouraging academic and industrial research. Shmulik Shelah, "'Israel Vulnerable to Cyber Attack on Civilian Targets,'" *Globes* July 5, 2011, http://www.globes.co.il/serveen/globes/docview.asp?did=1000660740.

29 Cabinet secretary announcement at the end of the Cabinet meeting of August 7, 2011, paragraph 4: Promoting national capability in cyberspace, http://www.pmo.gov.il/PMO/Secretarial/Govmes/2011/08/govmes070811.htm. At the time of writing the organization is not yet functioning.