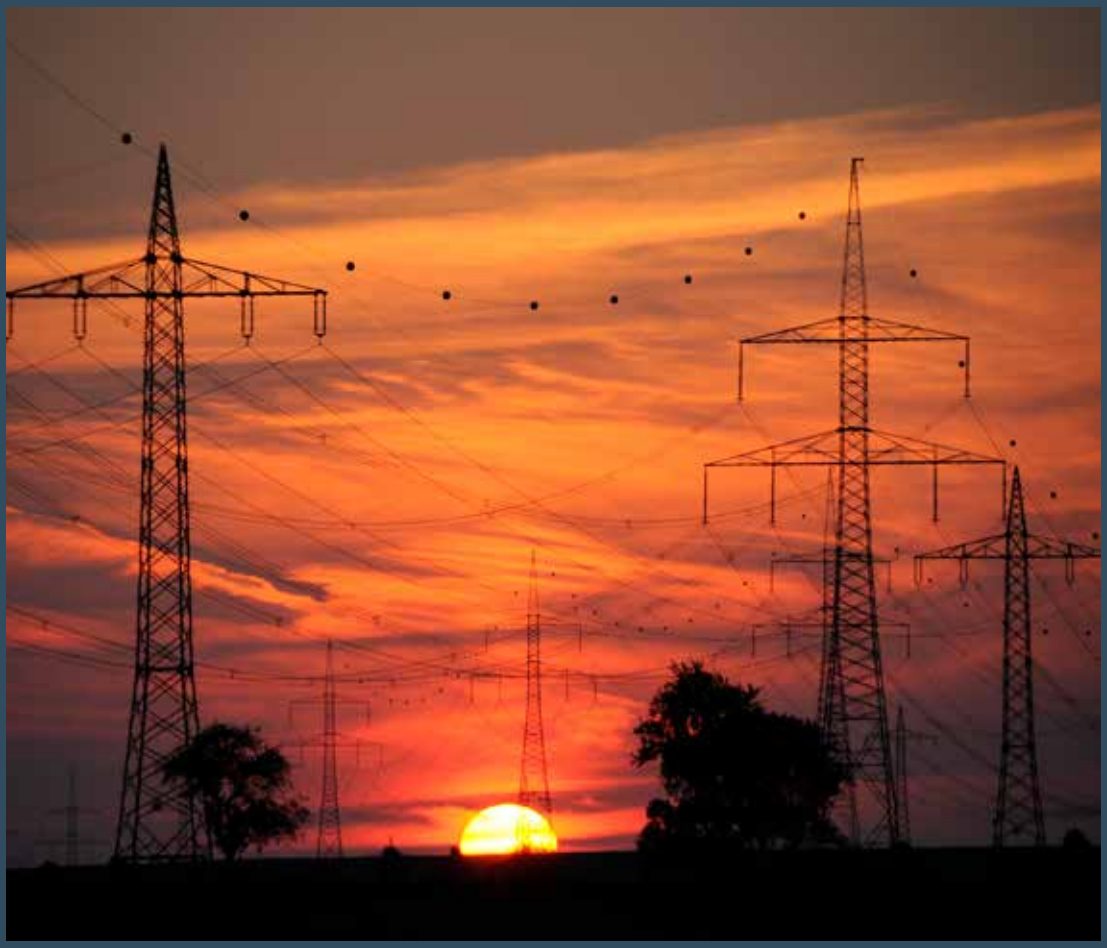

Securing the Electrical System in Israel: Proposing a Grand Strategy

Dan Weinstock and Meir Elran

Memorandum
165

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Securing the Electrical System in Israel: Proposing a Grand Strategy

Dan Weinstock and Meir Elran

With the assistance of:
Alex Altshuler, Ehud Ganani, Sinaia Netanyahu,
Eitan Parness, Amir Steiner, Shai Toledano

Institute for National Security Studies

The Institute for National Security Studies (INSS), incorporating the Jaffee Center for Strategic Studies, was founded in 2006.

The purpose of the Institute for National Security Studies is first, to conduct basic research that meets the highest academic standards on matters related to Israel's national security as well as Middle East regional and international security affairs. Second, the Institute aims to contribute to the public debate and governmental deliberation of issues that are – or should be – at the top of Israel's national security agenda.

INSS seeks to address Israeli decision makers and policymakers, the defense establishment, public opinion makers, the academic community in Israel and abroad, and the general public.

INSS publishes research that it deems worthy of public attention, while it maintains a strict policy of non-partisanship. The opinions expressed in this publication are the authors' alone, and do not necessarily reflect the views of the Institute, its trustees, boards, research staff, or the organizations and individuals that support its research.

Securing the Electrical System in Israel: Proposing a Grand Strategy

Dan Weinstock and Meir Elran

with the assistance of
Alex Altshuler, Ehud Ganani, Sinaia Netanyahu, Eitan Parness,
Amir Steiner, and Shai Toledano

Memorandum No. 165 June 2017

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

ביטחון מערכת החשמל בישראל
הצעה לאסטרטגיה רבתי

דן וינשטוק ומאיר אלרן

Graphic design: Michal Semo-Kovetz, Yael Bieber
Cover photo: Power line. CC0 Public Domain.
Cover design: Michal Semo-Kovetz
Printing: Elinir

Institute for National Security Studies (a public benefit company)
40 Haim Levanon Street
POB 39950
Ramat Aviv
Tel Aviv 6997556 Israel

Tel. +972-3-640-0400
Fax. +972-3-744-7590

E-mail: info@inss.org.il
http://www.inss.org.il

June 2017

ISBN: 978-965-92569-9-0

Contents

Executive Summary 7

Preface 9

Major Points from the Research 13

Chapter 1 The Threats to the Electrical System and Their Significance 21
Background 21
The Kinetic Threat: Missiles and Rockets 22
Natural Disasters and Climate Change 24
Cyber Threats 31

Chapter 2 The Electrical System in Israel 37
Components of the Electrical System 37
The Current and Future Electrical System 44

Chapter 3 The Current Response to the Threats to the Electrical System 47
Preparedness for Kinetic Attacks: Missiles and Rockets 47
Preparedness for Natural Disasters and Climate Change 50
The Level of Preparedness for Cyber Attacks 53
The Level of Preparedness in the Face of EMP Threats 55

Chapter 4 What Can Be Learned from International Experience? 63

Chapter 5 Conclusions 67
General 67
Selecting a Comprehensive Strategy 68
Technological and Operational Guidelines 72
Guidelines regarding Organization and Structure 78
Community Guidelines 80
Summary 84

Appendix: Basic Terms in the Electrical System 85

Notes 89

Authors and Contributors 99

Executive Summary

Many countries in the West, including Israel, have realized that their national security depends in part on the resilience of the home front. This resilience relies largely on the reasonable and continuous functioning of the various systems that serve it, first and foremost the orderly provision of the basic products of the critical national infrastructures. The electrical system has a major place among these infrastructures because of the potential risk of a protracted blackout over large parts of the country and the paralysis of its vital systems.

This research, the first of its kind, examines the major external threats facing Israel's electrical system and the current responses to these threats. This analysis provides a basis for our recommendations regarding what should be done in order to improve the preparedness of the electrical system to cope with significant risks to Israeli national security.

The security of the electrical system during emergencies and a reduction in the risk of an excessive and protracted blackout are critical issues that demand national attention and response. We maintain that the current systemic responses to threats against the electrical system are inadequate in light of the unique geostrategic characteristics of the State of Israel. Hence, they demand a broad and integrated approach by the government and the industry in order to improve the level of preparedness and the capability to cope with these threats.

The security of the electrical system depends ultimately on the existence and operation of a comprehensive systemic strategy for the various components of the national infrastructure in general and the secure supply of cheap and available energy to meet Israel's civilian and military needs in particular. Such a strategy does not currently exist in Israel, but should be formulated as soon as possible. This is the responsibility of the Israeli government and the ministries associated with electricity: the Ministry of National Infrastructures, Energy, and Water and the Ministry of Defense (through

the National Emergency Management Authority). The systemic response to emergencies must be based, as much as possible, on the response in routine conditions and on the capacity for flexible and rapid transition from routine to emergency conditions.

Preface

This research was conducted as part of the Institute for National Security Studies program for homeland security research. It reflects a first attempt to address in depth a major issue in the field of Israel's essential national infrastructures and to present overall conclusions and recommendations. The decision to conduct research on the security of Israel's electrical system reflects the understanding of the importance of the subject of national infrastructures and their degrees of resilience to relevant threats. Such investigation is needed to provide a basis for both public debate and decision making in the area of government and industry.

It is widely recognized that the electrical system, more than any other infrastructure, is central to the general operational continuity of Israel's economy. Major damage to this system is liable to cause not only significant disruptions to the electricity supply but also to other essential systems and subsequently to the economy, the state, and the functioning of the Israel Defense Forces (IDF).

The current research is based solely on open sources. We adopted a systemic and strategic approach. We did not examine or check the degree of resilience of each and every sub-component of the electrical system, their importance notwithstanding. We made the assumption that those responsible for electricity in Israel – both the companies engaged in this and state regulators – are more qualified to address these components professionally. However, during our research, it became clear that this subject is not addressed in an adequate, professional, continuous, or integrated manner from either a strategic or a comprehensive systemic perspective. Such perspectives would examine the various threats in light of the existing responses, check whether there are inappropriate gaps between them, and subsequently devise the course of action necessary to minimize these critical differences in the shortest amount of time possible.

The main contribution of our research includes a thorough evaluation of the subject and its major elements, increased awareness of its essential nature, and a presentation of our conclusions to the interested public and decision makers. We submit our recommendations in order to improve the existing situation.

This paper is limited to an evaluation of the security of Israel's electrical system within the context of Israel's ability to withstand external threats in two areas: man-made hazards and natural hazards. Man-made hazards in the military field include kinetic damage, damage during cyber attacks, and malicious man-made damage by means of electromagnetic pulse (EMP) systems. We chose not to address the subject of possible malfunctions inside the system, assuming (and hoping) that those responsible know how to locate and deal with them in good time. Natural hazards include earthquakes, climate change, and tsunamis. Although the electricity supply systems in Israel are strongly associated with economic, organizational, and political systems and considerations, we have been careful not to delve into these areas; at most, we refer indirectly to their influence during the formulation of protection strategy against the threats examined.

Due to the complexity of the subject and the need for professionalism, we chose a relatively broad team of researchers to address the various aspects of the field in question. In addition, we consulted with leading experts in Israel and abroad. Our examination included a comparison of the situation in Israel regarding electricity with the situation abroad, mainly in the US. We found that despite the differences between the various countries and the uniqueness of Israel's situation – regarding both the size of the system and the fact that Israel is "an energy island" – it was possible to learn a great deal from the approach and activities of other countries seeking ways to improve the security and resilience of their electrical systems. There is also much existing academic literature from which Israel can learn. We refer to this research in Chapter 4.

We would especially like to thank our colleagues who collaborated with us on this research. Before publication we consulted senior experts in the field of electricity who took the trouble to read the various drafts and make important comments that contributed considerably to the professional quality of this paper. We express our particular thanks and appreciation to the following people: Nurit Gal, deputy director-general of the Regulation and Electricity Division of the Electricity Authority; Moshe Ben Yair, head of the Engineering

Department of the Electricity Authority; Prof. Abraham Alexandrovitz and Prof. Yoash Levron from the Faculty of Electrical Engineering at the Technion; Amos Laskar, former CEO of the Israel Electric Corporation; Sa'ar Shapir, deputy director of the Alternative Fuels Administration at the Prime Minister's Office; Nissan Caspi, CEO of Global Power; Shlomi Angi, CTO of Alcatel-Lucent; Yossi Cohen, head of the Energy Group at Alcatel-Lucent; Dr. Erez Sverdlov, head of the Strategic Consulting Department of the Security Division at Matrix; Dr. Peter Vincent Pry, executive director of the American EMP Task Force on National and Homeland Security; and Robin Manning, former executive vice president of transmission electric power at the Tennessee Valley Authority.

Major Points from the Research

Data from the World Bank indicate that Israel's electricity consumption in 2011 was approximately 7000 kWh per capita.[1] This rate of consumption was higher than in most countries, including European countries such as the Czech Republic, Denmark, Italy, and Spain; similar to France, Germany, and Holland; and less than Australia, Canada, South Korea, and the United States.

In most countries in the developed world, it is the industrial sector that consumes the greatest amount of electricity, totaling about 40 percent or more. In Israel, however, industry consumes less than 25 percent, while the domestic sector consumes about 30 percent, similar to the share of the public and commercial sector. This implies especially high dependency on the supply of electricity by the domestic sector, which represents the heart of the Israeli home front, and is characterized by a lack of any alternative means of supply.

The increasing dependence of the Israeli economy on electricity supply may be described with the economic term "the cost of non-supply of electricity," which refers to the price in NIS/kWh that a person is prepared to pay for electricity during a shortage. The higher this cost, the greater the economy's dependence on the continuous supply of electricity. (The cost of non-supply of electricity in New York or in London is, of course, far greater than the cost of non-supply in Rwanda.) For many years the cost of non-supply of electricity in Israel, generally fixed by the Ministry of Energy, was approximately 25 NIS/KWh. According to research conducted by the Ministry of Energy and published in late 2011,[2] the updated cost of non-supply of electricity was 111 NIS/KWh, indicating the very high dependence of the Israeli economy on the continuous supply of electricity.

This paper is composed of five chapters. Chapter 1 maps the major threats to the security of Israel's electrical system, identifying and analyzing four major threats: attacks by missiles and rockets; natural disasters and climate change; cyber attacks; and electromagnetic pulse disruptions. We

do not deal with the risk of internal malfunctions in the system that do not originate in external factors, although this field also deserves serious consideration. Chapter 2 gives a brief presentation of lessons that may be learned from different countries about the protection of the electricity infrastructure. As background to our analysis and for the benefit of those not familiar with the laws of electricity, Chapter 3 introduces a number of basic concepts in the professional field of the national electrical system and gives a concise review of the structure of the Israeli system that has, in recent years, undergone rapid development and transformation. Chapter 4 addresses possible responses – some already exist and some are yet to be implemented – to the threats outlined in Chapter 1. We show that some of the threats can be prevented or their damage limited; others, however, are unavoidable, but their damage can certainly be reduced and the period of recovery and subsequent return to routine functioning shortened. Chapter 5 includes recommendations for improving the security of the electrical system and boosting its resilience during emergencies.

What follows are some of the salient points that emerge from the research.

Those responsible for the security of Israel's electrical system must draw a balanced map of threats based on the unique characteristics of the country (i.e., "an energy island" with limited flexibility), its needs (i.e., high dependence on the electricity supply), and its limitations (i.e., surrounded by enemies). This map should also address in an appropriate and balanced manner new hazards emerging mainly as a result of climate change – even if their prospects are relatively low. Evaluation of these threats must take into account a combination of the various risks at a single point in time (for example, simultaneous kinetic and cyber attacks).

We estimate that the major threats in the specific context of the electrical system comprise:

1. *Missiles and rockets*: This is the largest, most immediate, and most foreseeable threat. Improvements in the accuracy of the systems held both currently and in the future by the enemy (mainly Hezbollah, north of Israel in southern Lebanon, but also Hamas in Gaza, southwest of Israel, and other possible future organizations); the potential for launching (also salvos); and the size of warheads will magnify the threats, mainly against power stations and switching stations.
2. *Cyber threats*: These will increase with development of the adversary's capabilities and with expansion of computerization and telecommunications

in the electrical system.[3] The major damage expected from these threats will affect vital components of command and control.

3. *Electromagnetic pulse (EMP) disruptions*: This threat will damage transformers, switching stations, and substations, as well as control rooms that are not protected from an electromagnetic threat.
4. *Natural disasters*: Although these are less likely in the short term than man-made threats, they could nonetheless cause very serious damage to the overall electrical system, including the distribution segment.[4]

The level of preparedness in Israel to counter these different threats is not uniform. For example:

1. While the Israel Electric Corporation (IEC) has made many preparations for emergencies, they remain inadequate. The IEC should also not be working alone; preparation for emergencies requires close cooperation between the government and the various industries. A great deal of work is still necessary in order to ensure proper levels of security.
2. The electrical system is reasonably prepared for earthquakes. The probability of damage by earthquakes to the core installations of the system is relatively low.
3. The electrical system is not sufficiently prepared for other natural disasters, particularly extreme climatic events such as a tsunami or a rise in sea level.
4. The electrical system is only partially prepared for accurate and concentrated missile attacks and for wide scale cyber attacks.
5. The electrical system is not prepared for the electromagnetic pulse threat, although there is growing awareness of this risk and the beginnings of some professional evaluation of how to counter it.

Every response to threats against critical infrastructures in general and the electrical system in particular must be based on a strategic and systemic approach. Various questions must be asked. Most importantly, who has the responsibility and authority to manage the electricity sector prior to, during, and after an emergency? Other questions include: Who is responsible for determining the balance of threats versus responses and, in particular, for evaluating the cost effectiveness? Who is responsible for the integration of the national infrastructures in general and for the security of the electrical system in particular? Who formulates the comprehensive policy before disasters, and who is responsible for the systems and the integration needed

with other systems during the incident so as to ensure the minimum necessary degree of operational continuity?

There are no clear regulations in Israel regarding the security of the critical national infrastructures, just as there are no regulations regarding defense of the home front in general. This is mainly due to political and bureaucratic limitations that make it difficult to design and implement a balanced and systemic response. As long as there are no such regulations in place, the system will struggle to achieve the level of preparedness necessary for emergencies.

A grand strategy is required for the security of the national infrastructures, including the security of the electrical system.[5] Such a comprehensive strategy should include reference to the action necessary both before and after the crisis occurs: what has to be done in terms of prevention and protection on the one hand, and manifestation of the necessary skills to ensure the system's rapid recovery after the disruption on the other.

The formulation of such a strategy should be the government's responsibility, and should form the consensual basis for the long term work plan of all parts of the electricity industry concerning preparedness for emergencies. To date, this vital subject has not been dealt with successfully,[6] and the system therefore continues in an ill-advised fashion; electricity supply standards lack familiarity and transparency, and there is no framework demanding action within a defined time period. There is a need for a common language between the different providers of national infrastructure sectors and the electricity industry, if only to promote a minimal level of preparedness based on planning scenarios (that have not yet been completed) and the formulation of a concept that will measure the level of operation of the various providers. While the National Emergency Management Authority has begun laying the ground work, we are still only in the very early stages.[7]

Another issue that must be addressed relates to the budget needed for the maximum security of Israel's electrical system. There is no limit to the protection and security of the system or to the costs, which are likely to be totally unrealistic. Consequently, there is a need to set very clear priorities distinguishing between what is really needed and what is just nice to have; between what is needed now and what can wait until later. These priorities must be based on the level of damage that could stem from a continuous disruption of the electricity supply.

The holistic strategy for the security of the national infrastructures must also focus on foreseeable future developments in the management of the electrical grid. Methods for storing energy and of maximizing the use of energy in urban areas are rapidly developing all over the world. The future electrical grid is expected to have numerous varied interfaces for external systems, be it for local energy storage installations in urban areas or for domestic electrical appliances. The complexity of this future system requires preparation for the smart management and monitoring of the electrical grid. Such advanced management will need to introduce optimization of the energy system as well as the availability of energy during emergencies, including in an environment of cyber attacks.

Special importance should be attached to a number of basic and essential responses regarding the security of the electricity infrastructure:

1. Command and control security of the electrical system, both at the national and other levels of this system and of all the systems feeding it, with careful attention to the interdependence between the relevant systems.
2. Cooperation and maximum integration within the electrical system, both among its various elements and between the electrical system and the interfacing systems.
3. Cooperation with the community, the various customers, and the first response teams.
4. High overall preparedness in the area of risk management, one of the important responses to all the threats. There is a substantial delay in this essential area, and it has, in fact, still not been determined how to achieve appropriate risk management.[8]

Following are several central proposals for systemic techno-operational handling of the electrical grid in terms of risk:

1. One of the problems in Israel's electrical system is its growing dependence on the supply of natural gas and the gas transportation system. Israel's electricity production is currently largely dependent on a single pipeline that transports natural gas. Any interference with the orderly supply of gas (or its substitute, fuel oil) would pose a grave challenge to the production system.[9]
2. Dispersion of the production sites could improve the survivability and resiliency of the electrical grid and strengthen the security of the system as a whole. More specifically, regulations must be implemented to support the decentralization of the electricity supply to allow for local

production at times of natural disruptions, emergencies, or the absence of power from the main electrical grid. A distributed power grid makes efficient use of the resources of the electrical grid and significantly minimizes the significance of a natural disaster or an emergency to the level of a local incident.

3. With the means of production increasingly based on fossil fuels, such as gas, coal, diesel oil, and fuel oil, renewable energy has an important role to play in the diversification of production sources and the dispersion of production sites. Management of an electrical system that is connected to solar energy, wind energy, and pumped storage plants may improve its chances of survival and strengthen the system's overall security. Israel is, therefore, advised to advance and accelerate its development of renewable energy and to amend the current regulations that forbid small domestic photovoltaic systems from producing electricity in the absence of power from the electrical grid.
4. The current regulations concerning pumped storage plants set the quota at the capacity level of 800 MW. However, since these regulations were issued, the total capacity has increased, as have the number of production installations using renewable energy that require storage capability. It would now seem appropriate to expand the quota allocated to pumped storage facilities, because of both their high level of protection from various threats and their contribution to the increased potential to build power plants that use renewable energy.
5. The threat of the electromagnetic pulse on the one hand, and the relatively low cost of protection against it on the other, justifies the immediate allocation of the financial resources needed for a thorough evaluation prior to suitable preparation.
6. Any discussion of building electrical grids underground must also take into account the contribution to the security of the system and the resilience to damage from weather and missile and rocket attacks. This consideration is currently absent from the discussion.
7. As part of the efforts to improve weather forecasting capabilities, funds must be invested in the better assessment of severe weather conditions that have the potential to damage the electricity infrastructure.
8. A mapping of the shortage of accessibility is needed, which should also include a cost assessment for the procurement of the necessary means. An evaluation of cost-benefit and the feasibility of procuring special

machinery by the ECI versus using military equipment in times of crises is also called for.

There are already encouraging signs concerning the onset of quite a few processes aimed at developing suitable integrated responses to the security and safety risks facing the electricity system. These processes must be formulated and consolidated by means of a joint initiative between government and industry, increased awareness, public debate, government level decision making, methodical planning, and controlled implementation.

Chapter 1

The Threats to the Electrical System and Their Significance

Background

The traditional distinction between natural disasters and man-made emergencies raises numerous questions in today's reality. Should damage to buildings and infrastructures – including the electrical system – as a result of a major earthquake be classified as "man-made disasters"? The usual answer to this question attributes a great deal of responsibility to individuals and to the various organizations and government institutions, since they were "unprepared" and did not "prevent" or "foresee" the scenario that actually took place, nor did they take all the necessary steps to prevent the damage to people and property.

Modern technology enables better preparedness than in the past for coping with the various risk factors regarding both prevention and post-disaster treatment. While we might ask what are the priorities and the allocation of resources on the organizational, local, and national levels for dealing with these risk factors, there is no one definitive answer to this question; rather it is a question that involves values, beliefs, past experience, and the interests of various parties. Views vary among decision makers, professionals, and the general public regarding these issues that are dynamic in nature due to the different influences, processes, and events and the interpretations given to them.

It seems almost universally agreed that it is neither economically nor politically feasible to achieve absolute disaster preparedness, since this can only come at the expense of other equally pressing needs. However, there is growing recognition that "burying one's head in the sand," "hoping for the best," "praying it won't happen to me," or "it won't happen during my term

of office" are not real options. Instead, a dynamic and intelligent balance is required that will be determined from time to time according to an analysis of changes in the risk factors (assuming such information is available). This balance should be achieved with the delicate use of a scalpel and not the arbitrary blow of an ax. The Israel Electric Corporation, in fact, seems to be striving for rational preparedness for both wars and earthquakes in the areas of its jurisdiction.[10]

Both natural disasters and man-made emergencies constitute a challenge that is not just local but is global, complex, protracted, and multi-dimensional.[11] According to data from the World Bank,[12] the extent of damage to people and property as a result of disaster is on the rise. During 1980-2011 natural disasters were responsible for the deaths of over 2.5 million people worldwide, and the ensuing financial damage was estimated to be more than 3.5 trillion dollars. The accelerated urbanization and economic development of regions threatened by natural disasters increase their exposure to potential disasters and their dependence on a regular supply of energy. These risks are further heightened by the effects of global climate change. In addition to natural disasters and technological disasters, there is also the global and regional threat of terrorism. Similarly, there are certain regions, such as the Middle East, where long term instability leads to violent conflicts and wars. In such circumstances, it is particularly important to examine the significance and the ramifications of these risks to the major national infrastructures; without their continual strong protection it would be impossible to conduct a reasonably functional normal life. Most significant is the interdependence of essential infrastructures, headed by the electricity industry, which is critical for any national or international efforts to protect systems against the various threats.[13] This is why the security of the electrical system has become so important in the study of mass disasters; research in this area is currently led by the US, a country that has experienced numerous disruptions and that is greatly dependent on the regular supply of electricity.[14] In Israel, there have been some early attempts to conduct research into this vital issue.[15]

The Kinetic Threat: Missiles and Rockets

Wars and military confrontations are not uncommon in Israel and cause harm to the civilian population.[16] The potential risk to Israel's infrastructures, the electrical system among them, will grow over the years due to improvements in missile accuracy[17] and increases in the stockpiles of missiles held by Israel's

enemies. There were reminders of these risks during the Second Lebanon War and the confrontation with Hezbollah in the summer of 2006.[18] In more recent years, the focus of the confrontation has been with Hamas in the Gaza Strip as reflected in the rounds of fighting in the winter of 2008-2009 (Operation Cast Lead), November 2012 (Operation Pillar of Defense), and the summer of 2014 (Operation Protective Edge).

In a lecture at the annual international conference of the Institute for National Security Studies on January 29, 2014, Maj. Gen. Aviv Kochavi, head of the Intelligence Branch of the IDF, stated that about 170,000 missiles and rockets were currently threatening Israel.[19] This leads directly to the question: what is the significance of this threat for the State of Israel? The increasing accuracy of the missiles possessed by Hezbollah and soon, most likely, by Hamas (not to mention Syria and Iran) is likely to cause great harm to Israel's civilian population and infrastructure.[20] It should be stressed that currently most of the stockpiles of high trajectory weapons held by Israel's enemies comprise unguided and inaccurate rockets whose range is limited to under 80 km. These rockets are, therefore, able to hit mainly the north and south of the country. Israel's enemies do, however, possess a not insignificant number of long range missiles with high accuracy. The major threat remains Hezbollah with its significant arsenal, which includes large quantities, a growing capacity of precision guided accurate weapons, and larger warheads. These capacities are likely to represent a higher level of risk than ever before, which may be reflected mainly in large scale salvos directed either at single strategic targets (such as major cities or essential installations like those located near the Haifa Bay) or at a limited number of priority targets at short range. These salvos are expected to cause significant damage to persons, property, and essential infrastructure installations, including the electrical system.

In the face of these threats, it is important to mention Israel's active defense systems: the Iron Dome and Arrow systems, as well as Magic Wand and Iron Beam, which are in advanced stages of development.[21] These systems contribute to a significant reduction in the likelihood of missiles and rockets hitting Israel's civilian population and infrastructure, but the current order of battle of the active defense systems is not adequate for counteracting possible confrontations with Hezbollah. The dilemma that emerges in such confrontations is whether to make use of the existing yet insufficient systems

to protect population concentrations or to protect IDF installations, mainly IAF bases, or critical infrastructures.

Israel has not, as yet, faced a threat of this kind, but it must prepare for it – and the sooner the better. The intensified damage sustained during Operation Protective Edge,[22] reflected mainly in the length of the confrontation, provides additional testimony to the inherent limitations of any preparations for a threat and to the intentions and courses of action of the various parties in the turbulent and ever-changing Middle East.

A possible massive attack by accurate missiles against production, transmission, and transformation installations of the electrical system will not necessarily cause a prolonged disruption of the electricity supply. However, this scenario must be considered a significant risk that warrants a serious response. For example, according to Maj. Gen. (res.) Giora Eiland, former head of the National Security Council of the Prime Minister's Office, there is a scenario in which a missile attack on the Hadera power station could leave Israel without electricity for up to six months.[23] Eiland added that in war time, numerous sensitive installations remain unprotected and that government ministries simply pass budgetary responsibility for this issue from one to another. He stated that: "It is not only that there is no financial investment in this, but the discussion concerning who will decide has not yet started." Indeed, at that time (2011) there was no agreement about who would bear the cost of the various electrical installations. The view that the essential factories will themselves be responsible for the budget is not realistic, as was proved in the case of protecting the natural gas installations in the Mediterranean Sea. This question demands serious attention that should include an estimation of the extent of economic damage expected from both significant damage to the electricity supply and a long power disruption.

Natural Disasters and Climate Change

In the area of natural disasters, the most significant challenge facing Israel is the possibility of a major earthquake, especially if accompanied by a tsunami. Israel could be exposed to other natural disasters due to the impact of climate change, such as the December 2013 snowstorm and cases of extreme heat intensity. While the problem of a power failure that lasts several days and affects many people is clear, it is not necessarily on the level of a national emergency, which is more likely to be caused by a devastating earthquake. The current trend of climate change and global warming could lead to an

increase in the frequency and intensity of extreme weather events harming both the welfare of the population and the country's essential systems. Extreme weather events are expected to significantly increase the demand and consumption of energy, posing a risk of grave damage to all infrastructures as a result of floods, gales, and the expected rise in the sea level.[24]

A Destructive Earthquake

A major earthquake is expected to cause a serious national emergency. In addition to a corresponding tsunami, it is likely to bring in its wake technological disruptions and severe damage to numerous infrastructures. The Dead Sea depression (the Syrian-African rift), which separates the Arabian tectonic plate from the African plate, passes through Israeli territory[25] and is regarded as seismically very active.[26] The last major earthquake in the region occurred in 1927, and while the timing, location, and intensity of earthquakes cannot be currently forecast using seismological and geo-physical means, research literature concurs that over the last few centuries, major earthquakes have occurred approximately every eighty to one hundred years.[27] Since it is impossible to predict the timing of a major earthquake, the exact areas it will harm, and the extent of the damage, the Israeli government has, over the years, adopted various approaches in order to determine the "possible scenario" of such an earthquake. This is intended to define a common basis whereby all the involved organs are required to analyze the implications of the deployment necessary in their field of activities. A stringent reference scenario was formulated in 2004 that was intended to reflect all the possible ramifications of a major earthquake.[28]

In 2012 the government adopted a different approach; it maintained that it was impossible to select a single specific scenario and instead numerous scenarios were likely. However, for the purpose of preparedness of the various relevant bodies, a new concept was coined and adopted by the government: "a preparedness framework for an event whose probability is 5 percent over a period of 50 years." This framework specifies that preparations must be made for a situation in which a major earthquake could cause the deaths of 7,000 people, medium or serious injury to 8,600 people, and mild injury to 37,000 people with 28,600 buildings likely to be totally destroyed or seriously damaged and 170,000 people left homeless.[29]

A major earthquake will undoubtedly present the State of Israel with a hitherto untried complex and large scale challenge that apart from the

more obvious practical trials, also entails awareness, from the level of the individual through the levels of the family, the community, and the relevant agencies right up to the state.[30] The working assumption of the inter-ministerial committee for preparedness for earthquakes is that "great differences are expected in the ability to provide services to the population in all fields. It is impossible to eliminate these differences using routine courses of action. The operational concept must be changed and standards of service fixed that are inferior to those customary during times of peace or war."[31] It is unclear whether this directive has been totally implemented by the bodies authorized to handle Israel's electricity supply in the event of an earthquake.

An earthquake is likely to be accompanied by significant destruction to the electricity infrastructures, leaving thousands without electricity for an extended period, even if their homes have not been destroyed and it is possible to continue living in them. Israel Standard 413 addresses regulations for earthquake-resistant buildings.[32] The second part of this standard specifies general requirements for the survivability of structures in case of an earthquake, including systems such as road bridges, railway bridges, dams, nuclear reactors, and offshore rigs. Subsection 2.1 focuses on systems of steel storage shelves; 2.2 on aboveground tanks for the storage of liquids; 2.3 on raised tanks for liquids and gases; and 2.4 on aboveground pipelines in industrial installations. These standards are not official and numerous electricity installations still exist that do not comply with the published standards.

The following is a summary of the damage estimation to electricity infrastructures as a result of an earthquake in northern Israel in the region of the Syrian-African Rift.[33] The major electricity production infrastructures that are expected to be damaged are the steam-driven power stations in Haifa and Hadera and the gas turbines in the power stations of Hagit, Alon Tavor, and Caesarea.

1. The Haifa power station is steam-driven, relatively old, and located near the port. It is assumed that it will absorb a relatively high impact and thus suffer significant damage that will prevent it from producing electricity for a number of months. The Hadera power station is further away from the projected epicenter of the earthquake. Based on estimates made by the Geophysical Institute of Israel, the intensity of the earthquake in the area surrounding the power station could be 7 on the Richter scale, and most of its components should be capable of withstanding an earthquake of this, or even greater, intensity. Even if the Hadera power station suffers

damage, it is safe to assume that it will resume production within a few hours or days.
2. The intensity of the earthquake in the gas turbines in Alon Tavor, Hagit, and Caesarea is predicted to be 8 on the Richter scale, an intensity that they should be capable of withstanding. The damage they sustain is likely to shut down the gas turbines for a few days or weeks but is not expected to affect components that will halt their operation for a longer period.

The major substations and switching stations in the projected region of the earthquake are:

1. Zevulun substation (very close to the predicted epicenter of the earthquake);
2. Eleven substations / switching stations in Haifa and the Krayot;
3. Fifteen additional substations / switching stations at a radius of 30 km from the predicted epicenter of the earthquake.

The 400 KV line in the northern region passes between the Yagur junction (Zevulun substation), Yokneam, the Hagit gas turbine, and the Caesarea substation (a total of about 40 km in this segment). From the Caesarea substation the line splits into two: one leading to the Hadera power station and the other toward the center of the country. Except for the 400 KV line, there are about 300-350 km of high voltage lines (161 KV) at a radius of 30 km around the projected epicenter of the earthquake, and in addition, hundreds of kilometers of medium voltage lines are deployed over the length and breadth of the region.

Electricity lines have, in general, a fairly high resistance to earthquakes, since both the pylons and the lines themselves have a certain degree of movement (partly because of the need to withstand strong winds). As a result, their movement following an earthquake is not expected to cause the electricity pylons to fall or the lines to break. It is, rather, the possible sliding of the ground that is more likely to bring down the pylons, for example, in the lower regions of the Carmel or the falling of external objects that could cut the electricity lines. Of most concern are the distribution lines that pass through towns and between buildings.

The reference scenario of earthquakes adopted by the Israeli government includes the following elements:

1. The shutdown of the Haifa power station for a number of months.
2. Damage to the gas turbines in Hagit, Alon Tavor, and Caesarea that will cause closure for a period of days or weeks.

3. The falling of four pylons on the 400 KV line between the Zevulun substation and the Yokneam region, and two pylons on the 400 KV line between Yokneam and the Caesarea substation.
4. Heavy damage to the Zevulun substation (building and equipment) that will shut it down for a number of months.
5. Heavy damage to equipment in one substation and one switching station in Haifa that will shut each down for a number of weeks, and various kinds of damage to equipment in another three substations and three switching stations at a radius of 30 km from the epicenter of the earthquake that will shut each down for a number of days.
6. The falling of 10 medium voltage pylons on the lower slopes of the Carmel and 10 high voltage pylons at a radius of 30 km from Yagur, and the breaking of the lines passing over them.
7. The breaking of about 100 medium voltage lines within the city of Haifa, 50 medium voltage lines in the Krayot, and 50 medium voltage lines in settlements between Haifa and Nazareth.
8. The breaking of up to 20 medium voltage lines in the Lower Galilee and the Zevulun Valley and up to 30 medium voltage lines in the area between Haifa and Tel Aviv.

Some of the supply of diesel fuel for the gas turbines involves pipelines, some of which are likely to suffer damage in an earthquake. Therefore, the supply of fuel for the gas turbines – even those that have not been damaged – is likely to be disrupted.

Climate Change

Climate change as a result of global warming is expected to influence climatic, environmental, social, economic, and geopolitical systems, both cumulatively and as a result of extreme events. The Fifth Estimation Report of the Intergovernmental Panel for Climate Change (IPCC) declared that "the warming of the climatic systems is unequivocal,"[34] adding that events have been observed since 1950 that did not occur in previous centuries: an increase in the temperature of the atmosphere and of the oceans, a reduction in the quantity of snow, a rise in the sea level, and a greater concentration of greenhouse gases.

In each of the last three decades the surface of the earth has been hotter than in any previous decade since 1850. In the northern hemisphere, the 30-year period between 1983 and 2012 was hotter than in any of the preceding

1400 years. Since the middle of the nineteenth century, the sea level has risen at a greater speed than the average rate during the previous 2000 years. Human influence on the climate is extremely clear; the increase in the level of greenhouse gases in the atmosphere is indisputable.

According to all forecasts, by the end of the twenty-first century the earth's surface temperature is expected to rise by 1.5°C or even 2°C more than the period between 1850 and 1900. This rise in temperature is expected to continue beyond the year 2100. The influences of climate change are not expected to be uniform over the earth's surface; significant differences in precipitation are already discernible between humid and dry regions and between wet and dry seasons.

According to reports written by researchers from the Israel Climate Change Information Center (ICCIC), temperatures in Israel indicated a trend of temperature decrease (minimum, maximum, and average) from the 1950s until the 1970s followed by temperature increase from the 1970s until the beginning of the 2000s and stability in the last decade.[35] It should be noted, however, that temperatures throughout the last decade have been higher even in comparison to those of the 1950s.

Global scenarios (that have not yet been empirically substantiated) predict an ongoing increase in Israeli temperatures at an average rate of 0.3-0.5°C per decade depending on season and location. There is also a trend of increasing uncertainty concerning the temperature regime. It has been found that for most of the parameters reviewed (temperature regime, rainfall regime, and extreme weather events such as heat waves and air pollutant concentrations), there are stricter scenarios such as a rise in temperatures, a decrease in rainfall, and increases in the frequency and intensity of specific types of extreme weather. Not all these trends, however, have been found statistically significant. If these scenarios do, in fact, occur, they are most likely to influence various geostrategic fields including water, agriculture and food, public health, beach preservation, energy, and ecological systems. Many studies, including the IPCC report, have indicated the various influences of climate change on socioeconomic and demographic pressures and on regional conflicts, including the issue of migration and its ramifications.[36]

Not surprisingly, levels of vulnerability and public exposure to the threats of climate change vary greatly according to socioeconomic conditions and constraints, the proximity of residences and property to forests, beaches or rivers, the absence of drainage or failures of drainage maintenance, and

limited means of preparedness. Climate-related hazards are an additional burden on these vulnerable populations, particularly people who live in poverty, serving to increase the threat and negatively influencing their lives. There is broad agreement that violent confrontations may even be expected among people living in regions influenced by climate change. The possibility of such threats should be taken into consideration in our region as well.

Tsunami

Information on tsunami events that have hit Israeli shores is limited, making predictions of future risks difficult. According to a study by the Geological Survey of Israel, the seismic-tectonics of the Hellenic and Cyprus arc have been defined as the major sources of earthquakes that generate tsunamis on the eastern shore of the Mediterranean.[37]

An examination of tsunami scenarios as a result of earthquakes in more remote regions, such as southern Italy and the edges of the continent in North-West Africa, indicates that they do not constitute a serious threat to the Israeli coastline. According to the same research, a significant risk lies in earthquakes originating in the Dead Sea faults. The risk of such events lies in their potential to indirectly cause large submarine landslides in the eastern Mediterranean that will result in a tsunami hitting the Israeli coast. Historically speaking, nearly 80 percent of all tsunami events in the land of Israel occurred in this way.

The study *Geological Survey of Israel*, which specified the areas liable to flood as a result of a given scenario, stated that considerable flexibility exists in the selection of the parameters causing a tsunami that determine the gravity of the scenario. The tsunami in the Indian Ocean in 2004, which was significantly graver than was forecast, emphasized the importance of a conservative approach during risk estimation. In the absence of solid data for the Mediterranean Sea, thorough judgment is called for when building conservative scenarios with risk maps providing relatively extreme scenarios. In a seminar held in May 2011 on the subject of Israel's preparedness for a tsunami event, the Israel Electric Corporation presented an initial estimation of possible damage to its installations as a result of a tsunami event.[38]

The global phenomenon of climate change, as reviewed here, has both direct and indirect influence on the level of resilience of the critical infrastructure systems. All plans for strengthening the security of the electrical system and increasing its ability to withstand natural disasters must also be based

on the understanding that climate change constitutes a major element in the survivability of the system. This consequently demands a suitable response also in this broad context.

Cyber Threats

Definitions, Characteristics, and Trends

The cyber threat has become a global problem in recent years. The understanding that damage to computer networks is liable to cause serious damage and even to disrupt and shut down a country has led to attempts to find one uniform formula for confronting cyber threats. One of the notable documents in this field (not yet approved by NATO) is the Tallinn Manual, which contains a list of rules addressing the aspects of cyber attacks and an interpretation of these rules.[39]

For the foreseeable future, cyber warfare is expected to be a major medium of combat for both states and non-state terrorist organizations. The modern world's reliance on computer networks connected to the internet accelerates the trends of advancing and developing offensive capabilities that override the huge efforts invested in defense. In time, cyberspace will dominate the struggle against extremist regimes and terrorist organizations.[40]

The Cyber Threat against the State of Israel

In the last ten years the cyber threat against the State of Israel has become both continual and increasingly significant.[41] The Israeli government's decision to set up the National Cybernetic Taskforce,[42] alongside the establishment of a cyber campus in Beer Sheva[43] and budgetary support for various state entities such as the National Information Security Authority (NISA), testifies to action in the field of long term strategic planning for the development of technologies and human capital to protect Israel's cyberspace. The promotion of national preparedness[44] and of national regulations and government leadership in the field of cyber protection[45] were two decisions with great significance for increasing Israel's preparedness and management of the cyber field. It has been acknowledged by all stakeholders that the cyber threat is a real threat to the security and resilience of the state, and that numerous resources, including budgets, manpower, and the advancement of regulations, must be allocated in order to meet its future challenges.

The struggle against cyber threats in Israel has become an integral part of the covert and overt fight against enemy countries, terrorist organizations,

and criminal organizations.[46] As a result of its capabilities in this never-ending war, Israel has become one of the leading countries in the field of cyber protection and information security. Evidence of this can be seen in the number of Israeli start-up companies, such as CyberArk and Trusteer, that have established an international reputation.

In Israel, as in many other countries, a major fear regarding cyber threats relates to the critical national infrastructures. Many countries currently rely almost completely on computerized infrastructure systems that serve the vital life-support systems – electricity and water, banking, transportation, telecommunications, and health. Any damage to these infrastructures in Israel is likely to cause damage totaling hundreds of millions of shekels, and in certain cases, lead to human casualties.

Cyber Threats against Israel's Electrical System

The rapid development of cyberspace, together with the motivation of enemy countries and terrorist organizations to harm Israel, strengthens the assumption that the critical and sensitive infrastructures of the state, such as the electrical system, constitute a major target for cyber attacks. The cyber threat has in recent years become a major problem for the Israel Electric Corporation, which faces a significant number of the attacks by countries that have an interest in harming Israel and its national infrastructures, such as Iran, and terrorist organizations, such as Hezbollah.

The routine battle of the Israel Electric Corporation against cyber attacks changes according to the regional political situation. When there are specific plans by terrorist groups and their supporters to attack Israel, the number of cyber attacks on the IEC is significantly greater than during "quieter" periods. The IEC is sometimes forced to cope with as many as 10,000 cyber attacks in an hour. During many months of 2014 alone, the number of attempted cyber attacks on the company's systems ranged from 183,000 to 293,000 a day. From July-September 2014, at the time of Operation Protective Edge, there was a significant increase, with attempted cyber attacks reaching an average of about 865,000 a day (approximately 36,000 attempts an hour).[47]

The types of cyber threats and attacks against the IEC include:

1. DDOS (Distributed Denial of Service) attacks – denial of service for legitimate users of the computer due to an overload on the server.

2. Gaining control from afar ("backdoor attacks") – breaking into a computer that allows remote connection and thus enabling access to information in that specific computer or others.
3. Spear phishing/ Phishing – theft of information by impersonation on the internet.
4. Viruses of various kinds – such as viruses directed at the SCADA (industrial automation control) system used for the command and control of electrical systems.[48]

Cyber attacks can cause various kinds of damage to the Israel Electric Company: leaks of classified information, leaks of business information, and damage to the company's reputation (from defacing to denying service to customers). This can be done, for example, by inserting images of flags of a terrorist organization and thus changing the visual structure of the company's website.

In recent years there has been a significant increase in awareness and preparedness by European countries and, in particular, the US for combating cyber attacks against critical infrastructures. The major cyber attack Stuxnet caused the shutdown of a nuclear reactor in Iran in 2010. This sharpened the sense of complexity and difficulty in protecting against cyber attacks, some of which are aimed at the SCADA controllers.[49] The potential risk of the capability of cyber attacks to shut down the supply of electricity to civilians and to critical systems has led the US to invest significant resources in the improvement of the security of the control services. The establishment of a recovery body, such as the North American Electric Reliability Corporation (NERC),[50] and the compilation of standards and documents, such as the National Infrastructure Protection Plan (NIPP) of the Department of Homeland Security, were intended to aid the country in combating the growing threats. Analysis of the cyber threats against Israel's civilian sector and critical infrastructures was conducted in 2013 as part of the Institute for National Security Studies cyber security research program. This provided comprehensive recommendations for the organization of civil defense systems, including critical infrastructures.[51]

In recent years, changes have occurred in the electrical system characterized by automation and advanced telecommunications infrastructures – necessary infrastructures without which it is impossible to set up, maintain, and manage a smart electrical grid. These components increase the exposure of the electrical system to cyber attacks, especially those directed at the critical

network infrastructures and at the future advanced management measures for the electricity supply. Theoretically, it will even be possible to gain malicious access to private domestic electricity installations. The IEC will be forced to seek a secure solution that will enable advanced management of the electrical grid while providing suitable, sophisticated, and up-to-date protection of this grid.

In addition, in the Israel Electric Corporation, as in other large organizations, there is increasing exposure to the theft of confidential information via mobile devices used by company employees: mobile phones, laptops, and the like. Such penetration into employees' mobile devices is generally done by means of innocent applications (such as downloaded games). The employees' information security is then compromised and a Trojan horse is implanted through a loophole in the device which can be exploited by the hacker to extract any private information stored in the device such as contacts and emails. Organizations throughout the world are working hard to overcome this loophole that endangers some of their resources.

The solutions available today mainly address unauthorized penetrations from the outside and provide a significant but not hermetic response. The current discussion, however, refers to penetration of private devices as result of the user's approval (i.e., permissions granted during the installation of a game) – an issue that should not be treated lightly. The hacker can fairly easily:

1. Extract private information located in the device (e.g., passwords, images).
2. Locate the worker on the map (exploiting vulnerabilities in the geographic deployment).
3. Remotely and covertly operate the microphone of the device to record closed meetings.
4. Remotely operate the camera in the device to photograph secret installations, access codes to safes and doors, and so on.
5. Hide the existence of the Trojan horse and simultaneously operate all the "horses" concealed in a large number of devices in order to execute a combined attack.

These dangers require a comprehensive approach that will supply protection at least as long as the device is connected to a controlled network (the cellular or WIFI network inside the organization). This protection must immediately identify a break-in as a result of suspicious network behavior (and not by

identification of a virus signature as in conventional anti-virus software that can sometimes take up to 180 days).

Electromagnetic Pulse (EMP)

Electromagnetic interference constitutes a threat against the current operation of Israel's electrical system. Such interference has two major sources: the first arises from space weather that affects the electromagnetic field of Earth and produces a long electromagnetic pulse (known as E3); the second is a malicious, man-made action that can create a long electromagnetic pulse (High Altitude EMP = HEMP) by means of a nuclear explosion at high altitude or a short electromagnetic pulse (E1) as a result of use of a weapon (IEMI) that creates electromagnetic interference within a small radius.

The first official report on the subject of electromagnetic interference and the security of the electrical system was published by the American administration in 2004.[52] Since then, the subject has gained traction and started attracting many researchers who believe that this threat has far reaching ramifications for the functioning of modern society as a result of either space weather or a malicious source.[53]

The rapid development of the electrical system in terms of size, technical structure, and dependence has been accompanied by a significant increase in the sensitivity to electromagnetic influence.[54] Modern societies comprise a network of national and private entities that allow for development and growth. These are also responsible for the functioning of critical systems such as food, drinking water, sewage, transportation, telecommunications, and others, all of which are totally dependent on a functioning electrical system.

A major difficulty when combating the threats of electromagnetic interference is the ongoing behavior of private and institutional bodies. Recently, the subject of advance preparation to deal with this threat has received considerable attention, calling for management and investment before the implementation of any work programs. It acknowledges the need for the involvement of numerous bodies in all countries. In Israel this includes: the Prime Minister's Office, the Ministry of Defense, the Ministry of Finance, the Ministry of National Infrastructures, Energy, and Water, the Israel Electric Corporation, and the Ministry of Internal Security. In the case of an electromagnetic disruptive event, the ability to restart the activity of the electrical grid is largely dependent on the refunctioning of the transformers in switching stations and substations. Without adequate protection and the

hardening of these systems, the chance for a rapid restart of the electrical system is significantly reduced.

Electromagnetic interference represents a threat against the current operation of the electrical system in Israel. Its probability is regarded as low, but should it happen, it would have a destructive effect on infrastructures and on contemporary Israeli society. The extensive impact of such an occurrence validates the need to take responsibility and create a high level of synergy between the various bodies responsible for the ongoing functioning of the relevant systems.

Chapter 2

The Electrical System in Israel

Chapter 2 reviews the major components of Israel's electrical system as a basis for analyzing the significance and ramifications of the threats.

Components of the Electrical System

Production

The technologies used by the electricity production units in Israel include:[55]

1. *Steam units* – These units are located along the Mediterranean coast because of the need to cool them using sea water. They are located in Haifa, Hadera, Tel Aviv, Ashdod, and Ashkelon and are characterized by high capacity (the largest unit has a capacity of 575 MW) and a long start-up time of a number of hours. Consequently, they are used to provide the base load of the electrical system. Due to their location, these power stations are exposed to the threat of a tsunami. Their exposure to earthquakes, however, is very low, especially those located in the south.
2. *Combined cycle units* – This technology is characterized by high efficiency of up to about 60 percent. New production units, both of the Israel Electric Corporation and of private electricity producers, generally employ this technology.
3. *Jet gas turbines* – The term gas turbine does not refer to natural gas but to the operating principle of these turbines based on exhaust gases. A gas turbine can run on natural gas as well as diesel fuel. These units have a relatively low capacity, low electrical efficiency, and short start-up times, and consequently are mainly used when the demand for electricity is high and cannot be supplied using only steam and combined cycle units.
4. *Industrial gas turbines* – These units have a higher electrical efficiency than jet gas turbines but their start-up time is longer.

5. *Photovoltaic systems* – These are systems that convert solar radiation into electrical energy. There are thousands of photovoltaic systems, most of which are connected to the low voltage grid. A few tens of photovoltaic systems are connected to the medium voltage grid, and a number (some currently under construction) are connected to the high voltage grid.

Additional production technologies that may be employed in Israel in the future include:

1. *Pumped storage* – There are a number of significant projects in construction in the private sector. A pumped storage power station comprises two water reservoirs, one upper and one lower. In stage one of operation (generally when the electricity tariffs are low), water is pumped from the lower to the upper reservoir; in another stage of operation (generally when the electricity tariffs are high), the water falls from the upper to the lower reservoir and generates electricity. The critical elements of the power station – the generators that also serve as the pumps – are located underground and are not exposed to critical damage (by missiles or rockets). These power stations can react to external damage and recommence operation very rapidly.
2. *Wind* – The extent of existing wind farms is negligible – a capacity of less than 10 MW – but 10-year plans exist for private sector construction of wind farms on a significant scale of about 800 MW, mainly in the north.
3. *Thermo-solar units* – Similar to the photovoltaic systems, these units also exploit solar radiation but convert it into heat energy from which electrical energy is produced. Two such units are presently under construction on the Ashalim site. These units are also capable of producing electricity using natural gas when there is no solar radiation.
4. *Motors* – These units are powered by natural gas and are generally located on the premises of the energy consumer. The motors can run on natural gas as well as diesel fuel and fuel oil. These units have a low capacity, a high electrical efficiency, and a very short start-up time.
5. *Nuclear power station* – There is a statutorily reserved site in the region of Shivta in the Negev that is intended for the construction of a nuclear power station. The Israel Electric Corporation safeguards specific professional knowledge regarding nuclear energy for the production of electricity, and many government experts support the construction of a nuclear power station. Due to geopolitical reasons and public opposition,

however, it seems that a nuclear power station for the production of electricity will not be constructed in Israel in the near future.

Most of Israel's electricity production capacity is concentrated in only 20 sites; in other words, there is a relatively low degree of geographical dispersion. This, of course, increases the exposure to various, particularly man-made, threats, since an efficient targeted attack against a relatively small number of sites could cause significant damage to the electricity production system. The vulnerability of these sites to security is, therefore, fairly high. In addition to the interdependence of the installations in the electricity industry, as well as in the accompanying industries that supply it and are supplied by it, the system can be quite easily challenged in the kinetic and cyber fields. Threats from natural disasters can also have a significant impact on a relatively small, densely populated area, such as the State of Israel.

Israel's electricity production sector is currently mainly based on steam units (especially coal-driven) and combined cycle units. Damage to these units is expected to have significant ramifications for the country's capability to supply electricity. Damage to jet gas turbines, industrial turbines, motors, or the photovoltaic system will not be so severe.

The main types of fuel used for the production of electricity in Israel include natural gas, coal, diesel fuel, biogas, and solar radiation. There is a difference between the nominal capacity of the production units driven by a specific fuel and the contribution of the said units to the annual production of electricity. For example, the nominal capacity of the two coal-driven power stations is 4,840 MW, which in 2013 constituted only about 36 percent of the overall production capability. In contrast, the actual share of these two power stations in the overall production in the same year was almost 57 percent. The nominal capacity of the diesel fuel-driven production units is 1,046 MW, which in 2013 constituted about 8 percent of the production capacity. In contrast, the actual share of these two power stations in the overall production in the same year was less than 3 percent.

The difference between the nominal capacity and the actual electricity production results from the number of working hours. The coal-driven units operate about 8,000 hours a year and are shut down only for maintenance and treatment of malfunctions. The diesel fuel-driven units are mainly used for backup and consequently operate only a few tens or hundreds of hours a year.

Damage to the supply of fuel used for the production of electricity is likely to have the following repercussions:

1. *Damage to the supply of coal* will have a medium impact. On the one hand, coal is still a very high component in the production of electricity in Israel; stocks will, however, suffice for a few months of production under full load.
2. *Damage to the supply of natural gas* will have a very high impact due to the growing and increased component of natural gas in the production of electricity in recent years and the increasing dependence in the coming years. At present, there is no site for the storage of natural gas except for the pipeline between the reservoirs and the shore and a reliance on a single developed gas reservoir and a single marine pipeline.

   To the best of our knowledge, there is no country in which the percentage of electricity production from natural gas is so high while the natural gas transportation system from the reservoirs is so fragile. This is a very dangerous situation, since the repair of a malfunction in an underwater section of the natural gas system could take a long time. For example, the oil giant BP needed no less than 87 days just to seal off (not even repair) the leak in its oil well in the Gulf of Mexico in 2010. It goes without saying that BP had at its disposal resources that Israel is unlikely to have.
3. *Damage to the supply of diesel fuel* will have a medium impact. Diesel fuel has little weight in the production of electricity in Israel, but it also serves as a backup fuel for most of the electricity production units.
4. *Cyber damage to the system management unit* will disrupt the activities of the power stations, especially those that are unmanned and are dependent on the maintenance of reliable and serviceable telecommunications.

Delivery

Most of the significant blackouts around the world are the result of defects in the supply system and not necessarily in the production. The delivery sector includes two major elements: the transmission system and the transformation system.

Transmission System

The electrical capacity is produced in the power station at a voltage of between 11 and 22 KV, but such voltages cannot be transmitted over significant distances. Thus as early as the 1960s, a 161 KV transmission system was constructed in Israel. With the construction of the large production units

at the beginning of the 1980s, the need for a higher voltage transmission system of 400 KV emerged. Some of the production sites are connected to the 400 KV system and others to the 161 KV system. The 400 KV system is, in fact, still in various stages of construction. Progress is extremely slow due to regulatory issues, and it seems likely that it will take at least another 20 years to complete.

Table 1. The 161 KV and 400 KV transmission systems

	400 KV	161 KV
Height of pylon (m)	60	33
Width of corridor (m)	70	40
Number of pylons per km	2-3	3-4
Width of the base of the pylon (m)	2-7	1.5-4
Power transmission capability	1,800	300
Overall length (km)	735 (approx.)	4,400 (approx.)

On both sides of the transmission lines there is a corridor in which construction is forbidden for reasons of safety, including prevention of electrification and exposure to electromagnetic fields. In order to reduce the number of corridors and the construction costs of the transmission lines, it is customary to construct two-circuit lines. In some special cases the pylons support three or four circuits, a practice that increases exposure in the event of physical damage to the transmissions, since the collapse of a pylon carrying three circuits will cause greater damage than one with a single circuit.

In dense urban areas, such as Tel Aviv, Jerusalem, and Haifa, where a surface power line transmission grid cannot be constructed, underground transmission cables are laid. An underground transmission grid is up to 10 times more expensive and has a smaller transmission capacity (about 30 percent) than a surface elevated grid. In Israel there are only 161 KV underground transmission lines.

Transformation System

Switching stations constitute junctions for routing the transmitted electricity and usually connect 400 KV systems to 161 KV systems. There are ten switching stations in Israel. Substations connect the 161 KV transmission system to the distribution system. There are about 200 permanent substations in Israel, most belonging to the Israel Electric Corporation with a few

belonging to large private consumers. There are also mobile and temporary substations that serve the short term system demands.

There are two switching station and substation configurations: open and closed. A closed station is better protected, but its repair following damage tends to take considerable time due to the special equipment it needs.

Possible forms of damage in the transmission segment include physical damage to the super high voltage pylons, physical damage to a substation, physical damage to high voltage pylons, and cyber damage to the system management unit. Some experts have suggested that damage to switching stations and substations is not as significant as damage to the production units or their fuel supply. This opinion is based on the short time needed to repair the typical damage to a switching station or a substation compared to the long time needed to repair damage to a production facility.

We believe that this approach is flawed for two principal reasons. First, the time needed to repair a malfunction or serious damage to a switching station is not short and can, in fact, take several days. Second, damage to specific switching stations might cause a significant imbalance in the electrical system and serious disruption to its operation. The Israeli Ministry of National Infrastructures defines "a special situation in the electricity sector" as an event in which 25,000 consumers (1 percent of all the consumers in Israel) are cut off from the supply for eight hours or more. We believe that certain damage to switching stations may have far reaching ramifications. Damage to production units is linear. For example, damage to a specific percentage of the electricity production capability will allow for the continued functioning of the entire system; at most, it will be necessary to organize a blackout on a forced or voluntary basis. There is often no alternative other than to repair damage (even if just temporarily) to critical junctions of the transfer of energy.

Distribution

The distribution system is composed of medium voltage electricity lines, distribution transformers, and low voltage lines. The medium voltage electricity lines leave the substations and feed distribution transformers from which low voltage lines leave to be connected to the clients. Low voltage is 400V between phases and 230V between a phase and the ground.

There are three levels of medium voltage:

1. 12.6 KV in certain parts of the Tel Aviv metropolitan area, Jerusalem, and Haifa.
2. 22 KV in most other regions in the country.
3. 33 KV from Beer Sheva southwards and on the other side of the Green Line (the Palestinian territories).

Transition from medium voltage to low voltage takes place using distribution transformers that are fitted to pylons or installed in internal stations or small transformation stations. There are approximately 50,000 distribution transformers, 25,000 km of medium voltage lines, and 20,000 km of low voltage lines.

Until a few years ago the distribution system was almost entirely non-automated. On completion of the wide scale distribution management system (DMS), there will be improved control capability over the distribution system, mainly in the medium voltage grid. While this system will allow for swifter repair of the grid in the event of malfunctions, it is also likely to be subject to cyber attacks.

The nature of the distribution grid is changing. In the past it was mostly client oriented, with barely any connection to production units. The only exceptions were the generators fed by diesel or fuel oil. These generators usually served as backup during emergencies and provided supply to nearby consumers. Today, however, numerous production systems are connected to the distribution grids, mainly photovoltaic production systems. These will be joined in the future by production units with a low nominal capacity that will be connected to the distribution grid. When the low or medium voltage line to which these systems are connected is disconnected for reasons of safety, the convertors of the photovoltaic systems are disconnected and the systems cannot feed electricity into the grid. There seems no obvious reason why these systems should not provide electricity to the consumers connected to them – assuming such consumers exist.

While it is generally thought that physical damage to the distribution system is not as significant as damage to the transmission grid, due to the relatively few consumers who would be affected by a single incident, we have a number of reservations:

1. Wide scale damage to the distribution grid, such as following an earthquake or a cyber attack on the automatic distribution system, should also be considered.

2. Although the number of consumers in the distribution grid is fairly small (approximately 3,000), they constitute about 40 percent of the total consumption of electricity in Israel. Damage to the distribution grid would, therefore, cause damage to a significant part of total consumption.
3. In contrast to the transmission grid, which contains many backup options, the distribution grid, and especially the low voltage distribution grid, has limited backup options. Consequently, any damage to the distribution grid, even if it affects only a few consumers, is likely to last for many hours in the event of local malfunctions and several days in the event of system malfunctions.

The Current and Future Electrical System

The structure of the electrical system changed very little in the last century.[56] Today, however, it is facing significant changes. The current system can be characterized by the following main features:

1. There are very few production units (a few dozen in the case of Israel, the photovoltaic systems notwithstanding); each is large (several tens or hundreds of MW). In addition, they are all concentrated in a small number of sites.
2. The flow of the electricity output is uni-directional: from the power stations, via the transmission and distribution systems, to the consumers.
3. Interfaces between the electrical system and external systems – mainly command and control systems – are limited. This is true even in the case of the Israeli electricity system, which is advanced and extensively computerized.

The new structure of the electrical systems, known as the "Smart Grid," will be expressed in the following ways:

1. There will be more production units (thousands or even tens of thousands). Most will be small (a few KV or tens of KV) and will be located in close proximity to consumption sites.
2. The flow of the electricity output will be two-directional; sometimes from the large power stations to the consumers and sometimes from the small production systems located at the consumption sites to the electrical grid, and from there to other consumers via the grid.
3. There will be more interfaces between the electrical system and the external systems, even on the level of a single domestic electrical

appliance. These home appliances will be fitted with a component that enables intercommunication.

These predicted changes will have many implications for the security of the electrical system, some favorable and some detrimental. For example, it can be assumed that malicious damage to a very large number of production units will be far more serious than the damage to a small number of power stations. In addition, while the large number of interfaces will enable relatively rapid indications of malfunctions in the electrical system, it will also increase the system's exposure to cyber attacks.

Chapter 3

The Current Response to the Threats to the Electrical System

Chapter 3 reviews the responses of the electrical system in Israel and its surrounding areas to the threats presented in Chapter 1.[57] The discussion does not include technical malfunctions within the system, which are also capable of causing long blackouts and demand meticulous attention by those responsible for Israel's electrical system.

Preparedness for Kinetic Attacks: Missiles and Rockets

Protection

In July 2012 there were reports of the initiation of a special project for strengthening the protection of ten strategic installations around the country defined as top priority due to the risk of a missile attack.[58] The major aim of the project, launched by Prime Minister Netanyahu in 2010, was to allow for the swift recovery of critical infrastructure supply capabilities following their disruption by an external attack designed to hamper the supply of electricity or other essential services. It was further reported that the project, to be financed by industries such as the Israel Electric Company, would include the reinforcements of the installations by concrete a few meters thick and other physical defenses. The project was supposed to be managed by the national infrastructures branch established previously within the Home Front Command. This branch was at the time carrying out staff work, selecting the ten sites that urgently required protection against missiles. The Home Front Command was also planning to extend the project to some fifteen additional installations in the realm of water, fuel, oil refining, and telecommunications sectors in order to include protection against cyber threats.

In a discussion held in the Knesset State Control Committee on August 26, 2013, the senior member of the National Security Council responsible for the subject said:

> The Prime Minister has allocated NIS 20 million…for the Home Front Command. The National Security Council, together with the Ministry of Home Front Defense [since dismantled with its powers restored to the Ministry of Defense], the Home Front Command, and other ministries, has selected the ten installations….The Home Front Command, currently responsible for protection, will implement the programs and supervise the construction….Some of the ten installations have already been protected. The installations of oil and fuel infrastructures have already been protected. In fact, only yesterday, NIS 25 million were transferred from the Israel Electric Corporation to the Ministry of Defense to the Home Front Command in order to protect what we decided for them. In other words, this process is being implemented. [59]

Later in the discussion, Gilad Erdan (then Minister for the Home Front) referred to the budget for infrastructure protection:

> Someone has to make decisions, and at present…there is a problem in the decision making process, since every ministry is responsible for ensuring that its affiliates will function (properly) in times of emergency. But the ministries justifiably say…that the Ministry of Energy, for example, has private electricity producers; and if there is no law that empowers the Ministry of Energy…to instruct private industry in how to construct the power plants in a different way which is more expensive, then by virtue of what will they construct them?

As much as is known, hardening was constructed for two power plants and two switching stations, damage to which would, it was calculated, endanger the functionality of the electricity supply. This strengthening was not part of the original construction of the sites, and was added subsequently. This prompts the following questions:

1. Does the protection meet all or only some of the currently known threats?

2. Does the fact that damage to the other sites does not endanger the survivability of the system justify the absence of any protection at these sites?
3. Will the protection of future sites during their construction significantly reduce their costs?
4. Does the benefit from the addition of hardening justify the investment?

Active Defense

The majority of the large electricity installations, including power plants and switching stations, are located outside urban centers. According to threat estimation, there is a need to create a parallel response of active protection for both the population and the critical infrastructure installations, such as essential electricity installations that are highly vulnerable to kinetic weapons. A consideration of the need for reasonable active defense for IDF bases, particularly for IAF airfields, makes it apparent that there is no alternative other than to increase the number of anti-missile batteries significantly and prepare for their operational deployment during emergencies, so as to provide adequate defense for the infrastructure installations within the range of these batteries as well.[60]

In an interview in *Haaretz* on March 29, 2013, the commander of the Home Front Command stated: "For years there has been a controversy within the defense establishment about the correct deployment of the batteries during a war." He went on to claim that the position of the Home Front Command is:

> To protect the functional continuity of the state and the capability of the IDF to maintain an ongoing offensive effort until victory has been achieved. This implies the protection of power stations and IAF bases before the protection of the large cities. It is possible that in the future we will be able to protect both, but currently, with the number of batteries and interceptor missiles at our disposal, we have to designate an order of priorities for the deployment of our assets. We have to make a difficult, painful, and clear-cut decision.[61]

Preparedness for Natural Disasters and Climate Change

Earthquakes

There has been growing awareness in Israel in recent years of the possibility of an earthquake.[62] Management of this threat has become part of the national agenda, and preparations have intensified: for example, the Home Front Command's national exercise Turning Point 6, which took place in 2012, addressed the scenario of a serious earthquake.[63] Prior to the exercise, the Geological Survey of Israel prepared a document detailing the different levels of damage expected in the event of an earthquake. Accordingly, the most significant damage to infrastructure installations is expected to be concentrated in northern Israel in regions around the epicenter of the earthquake and the tectonic fault that causes the earthquake. The closer the infrastructure installation is to the epicenter and the lower its resilience, the greater the expected damage.

Geological and historical evidence indicates that most tsunami events affecting the Mediterranean coastline occurred following a ground earthquake with an epicenter located to the east of the impacted region (as far as it is possible to estimate the location of the epicenter). A tsunami of this kind occurs as result of a slide in the slope of the continent to the west of the earthquake's epicenter. In most cases, the damage was limited to one area, but there is a possibility that a tsunami could occur to the north or the south of the epicenter, producing waves that could affect a wider area. Consequently, if the epicenter of an earthquake were in the Hula Valley, Israel's northern coast would, it seems, be more susceptible to damage from a tsunami.[64]

According to the Home Front Command website, due to the extent of damage expected from a destructive earthquake, "citizens must be prepared for an earthquake, assuming that in the first few days they will be forced to cope with the destruction and its consequences by themselves."[65] This directive is presumably also relevant to the electrical system; in other words, the population should be prepared for blackouts.

Tzvi Harpak, senior vice president of the Organization, Logistics, Security, and Emergency Division of the Israel Electric Corporation, said in an interview with *Calcalist* on July 21, 2011:

> Israel has defined three national scenarios for earthquakes, and for each of them we have conducted a simulation of cases and responses….The Israel Electric Corporation has mapped all of its

> production sites and transmission lines, including voltage lines, substations and switching stations, with the aim of examining the various effects of an earthquake on the population….In the last decade, the Israel Electric Corporation has held three large exercises in which every scenario was examined. A full war game was also conducted in which certain sites were shut down virtually.

He added that:

> The Israel Electric Corporation possesses a number of technologies for the supply of electricity, such as bypasses of high voltage lines, mobile substations, and a further set of solutions. However, in the event of an unusual event, there will undoubtedly be blackouts of undetermined length.

On the subject of the existing alternatives, namely redundancies, Harpak said:

> If a power plant is affected and there are others as backups, then the electricity supply will be affected in a relatively minor way. If the system redundancy is not high – and this is the current situation [2011] – the State of Israel must examine whether we are organized for such situations.

He could not rule out the possibility that the Israel Electric Corporation would shift the various demands between Israel's cities, so that "some of the unharmed places will not receive electricity for some hours of the day." An additional question raised in the interview concerned the restoration of the system after damage. According to Harpak: "This is liable to take between half a year and a number of years, depending on the damage….If an entire power station is shut down, the generators in operation will not meet the demand."[66]

Presumably the Israel Electric Corporation's activity over the years regarding earthquakes has, in general, been effective. Their power stations and switching stations should therefore be expected to function reasonably, albeit not fully, in the aftermath of an earthquake.

A significant part of Israel's electricity production capacity – the five power stations of the Israel Electric Corporation (Haifa, Hadera, Tel Aviv, Ashdod, and Ashkelon) and the private power station run by Dorad – are located on the Mediterranean coast. A tsunami in the Mediterranean Sea is

liable to cause extensive damage to the production capacity of these power stations. We propose installing generators and water pumps in the perimeters of the power plants, which would start operating automatically in the event of flooding, and the construction of levies.

There is an ongoing debate regarding the probability of a tsunami in the Mediterranean Sea. According to the head of the reference scenarios division of the Ministry of Defense, 25 percent of all known cases of tsunami have taken place in the Mediterranean. The Israel Electric Corporation, on the other hand, claims that the probability of a tsunami in the Mediterranean is very small. In our opinion, this issue should be examined by a professional consulting organization such as the Geological Survey of Israel.

Questions to be asked regarding the occurrence of an earthquake and its ramifications on the electrical system in Israel include:

1. Is the Israel Electric Corporation doing its best to protect its installations and to ensure rapid recovery after an earthquake? Presuming that the professional establishment has the necessary knowledge for maintaining appropriate levels of preparation for earthquakes, this is mainly a conceptual and budget-related question. Conceptually speaking and from the perspective of cost effectiveness, how justifiable is it to protect the system, cognizant of the not so high probability of an earthquake in the foreseeable future (a dilemma that demands a decision at the highest governmental level). And from the budgetary point of view, who will bear the high costs of the level of preparedness regarded as appropriate, and who will determine what this level of preparedness is – the industry itself, including the small suppliers, or the government?
2. Since it is ultimately the consumers who bear the cost, it should also be asked whether there is a full and open dialogue between the government and the industry about these important issues, and why, as of now, there are no full and transparent answers to this question.
3. Do the manufacturers of private electricity, both current and future, engage in reasonable protection of their electricity production installations in order to ensure their continued functioning in the event of an earthquake?

Other Weather Hazards

While earthquakes are particularly serious natural disasters, there are other weather phenomena that could cause damage and disruption to the electrical system. Weather hazards cannot be avoided, but it is possible to improve

both preparedness and recovery time. Attention should, therefore, be paid to the overall level of systemic preparedness as well as to local and individual levels of preparedness. The ability of citizens to cope with disruptions is marginal, and the capacities of the local government authorities in this field vary greatly. In all cases, however, such an event will be limited to a few days.

Building Underground Electrical Grids

A Ministry of National Infrastructures directive from the early 2000s stated that all new medium voltage and low voltage grids that pass through urban regions will be built underground. Due to the current rate of replacement of the grids, it will be many decades until all the medium voltage and low voltage grids in urban regions move underground. The current situation is as follows: an extra high voltage 400 KV grid is completely aboveground; and a high voltage 161 KV grid is mainly aboveground, except for certain segments in urban regions that are underground and whose overall length is about 3 percent of the length of the grid.

The advantages of building electrical grids underground include:

1. Extremely high resistance to weather hazards (strong winds in winter, fires in summer).
2. Space saving, since the safety margins of underground electricity infrastructures are significantly smaller than those required aboveground.
3. Higher reliability of the electricity supply.
4. Improvement of environmental aspects thanks to reduced scenic damage and better aesthetic appearance.
5. Reduction of public concern regarding electromagnetic radiation (regardless of whether these fears are justified).

The disadvantages of building electrical grids underground include higher initial costs and the fact that location of malfunctions in underground grids and their repair often takes longer than in aboveground grids.

Any discussion of building electrical grids underground must also include a consideration of its contribution to the security of the grid and its resistance to weather hazards. These considerations are currently absent from the discussion.

The Level of Preparedness for Cyber Attacks

Cyber threats against the State of Israel in general and the Israel Electric Corporation in particular force decision makers to take steps to minimize

or eliminate these threats. The Israel Electric Corporation and additional national infrastructure companies are under the supervision of the National Authority for Information Security and act according to regulation and directives that attempt to create standardization in coping with cyber threats.

The Israel Electric Corporation attaches great importance to the subject of cyber security and the protection of the electrical system infrastructure. As such, the chairman, the CEO, and designated committees of the board of directors are personally involved in this challenge. This importance is reflected in a number of ways: allocation of resources and participation in international programs addressing cyber, European research (FP7),[67] and the follow-up European program (Horizon 2020).[68]

In the cyber field the Israel Electric Corporation is active in the following ways:[69]

1. The Advanced Cyber Center (ACC) serves as a command and control center 24 hours a day and is based on a predefined model of defense against cyber threats. The ACC is staffed by cyber experts and analysts who respond immediately to every incident.
2. The IEC partners with CyberGym, a company that offers a training arena and simulation in the field of cyber defense. Since 2013 the company has operated in the Israel Electric Corporation's Hefziba Training Center and serves a wide variety of customers in Israel and abroad.
3. The IEC cooperates with mPrest Systems in establishing Sarig Meda, a system for the management and overall monitoring of the physical security of energy installations and organizations, which forms a major, additional layer in protection against the cyber threats.

The Israel Electric Corporation is run and managed in accordance with recognized standards, including ISO standards, hygiene standards, and the COBIT standards (control objectives for information and related technology) which provide a framework for the development, implementation, monitoring, and improvement of information technologies. The practices of management based on the COBIT standards assist meeting the challenges of computer risks in accordance with the ISACA (Information Systems Audit and Control Association) standards and with other different regulations. By meeting the various standards of information security, the Israel Electric Corporation is able to purchase and implement new systems in accordance with clear criteria and thus achieve standardization in this field. Every implementation

of a new system or its work with suppliers is approved by the National Authority for Information Security.

The Israel Electric Corporation also engages in the hardening of critical systems, including the separation between critical and administrative networks. It conducts numerous training programs in the field of cyber security; conducts periodic drills and national exercises; and employs its own hackers to test penetrability, preparedness, and response capability in the event of an attack. Information security is an integral part of the Israel Electric Corporation's organizational culture, and substantial financial investments are made in campaigns and in internal communications on this issue. Senior directors are also very involved in enforcing the requirements and standards for information security. In addition, the company periodically conducts a strategic risks management exercise on information security.

The following elements can thus be highlighted in the Israel Electric Corporation's approach to cyber threats: a strategic (rather than tactical) approach to the problem, increased awareness of the threats, and a deepened understanding that it is those who feel protected against cyber attacks who are, in fact, most at risk. Several major questions remain open, however. For example, to what extent is the Israel Electric Corporation maximizing its capacities in the field of cyber security and making optimal efforts to be adequately prepared for future extreme threats? How aware are the other companies that engage in the production and supply of electricity in the electrical grid (whose share of the supply of electricity to the Israeli market is increasing) of the various risks and threats, including in the field of cyber, and to what extent are they investing in the necessary preparedness? As we do not possess enough information to answer these questions, suffice it to say that the function of the regulator is to ensure proper preparedness by all suppliers in Israel's electrical system for confrontation with all threats to the production and supply of electricity.

The Level of Preparedness in the Face of EMP Threats

Coping with the threats of electromagnetic disruptions is a unique challenge. The large number of systems and organs that are dependent on the current functioning of the electrical system demand a high level of prioritization in the allocation of resources, a hardening of critical systems, and the formulation of rehabilitation programs. In order to fully understand the ramifications of coping with electromagnetic incidents, it is important to distinguish

between the sources of the threat and the different types of the threats. This is because pulses at various levels and frequencies will affect different parts of the electrical system. The numerous research papers published in this field have defined three levels of protection: full protection, partial protection and rapid recovery, and partial protection and gradual recovery. The aim of this categorization is to improve the ability to deal with the threat in accordance with its severity.

Defense against Electromagnetic Interference

The first thought in the process of coping with any threat tends to be whether it can, in fact, be prevented. Currently, it is often suggested that this approach has very limited practical significance. Electromagnetic interference as a result of space weather cannot be precisely predicted; and even when it is predicted, the ability to defend existing systems from its impact is fairly limited.[70] In the event of malicious electromagnetic interference, it is still impossible to state categorically that any attempts to cause harm could be prevented. As of 2003, over 20 countries possessed or were engaged in the development of electromagnetic weapons capable of creating a high altitude electromagnetic pulse (HEMP).[71] Consequently, there is now greater availability of weapons capable of hitting targets than previously. There are companies that are currently developing "EMP suitcases" that while intended for the testing of equipment only, can, it seems, be used as weapons in every respect.

There are currently a wide range of technical responses and work procedures that can significantly reduce the influence of electromagnetic incidents, including, for example, the mapping of sensitive areas. The training of response teams and the upkeep of a limited stock of critical parts can be decisive factors in the restoration of affected electrical activity. Raising awareness of electromagnetic threats and emphasizing their importance can encourage the rapid development of the means of protection and prediction that will improve the level of defense.

At present, the electrical system in Israel is very far from integrating meaningful protection measures against electromagnetic hazards. Note that the implementation and integration of such measures have significant added value: the use of protection systems and work procedures in the area of EMP might create a systemic synergy that enhances the resilience of any

potentially threatened infrastructure to other risks, particularly those in the cyber domain.

Computerized simulation, conducted by leading companies in the electromagnetic field,[72] has examined the possible influences of former electromagnetic storms over the electrical system today. The results indicated a collapse of the electrical system. The simulation also proved that the use of means of hardening has a dramatic effect on the extent of the damage and can even prevent the system's collapse.

A large number of electricity companies in the US and elsewhere have embarked on the development of programs for the protection of their grids against electromagnetic incidents at levels E1 and E3. The steps currently taken by these electricity companies include:

1. Hardening the transformers in switching stations and substations.
2. Developing means of identification for short electromagnetic pulses – E1.
3. Developing current blocks for transformers in switching stations and substations.
4. Establishing control centers and command and control systems that are protected against short electromagnetic pulses – E1.
5. Developing an internal telecommunications infrastructure protected against E1.
6. Using control cables that are protected against E1.
7. Maintaining reserve transformers for switching stations and substations in protected areas.
8. Developing recovery training programs.

Much of the material written about preparedness for electromagnetic threats addresses the development of means of analysis and modeling in an attempt to formulate an ultimate response. Although these stages are very important, the existing knowledge and understanding of electromagnetic interference resulting from space weather are still limited. We are, it seems, still far from developing technological capabilities for forecasting electromagnetic interference; nor can analysis of the probability of a malicious electromagnetic event be modeled precisely. The development of analysis capabilities and the formulation of precise models demand in-depth mapping and analysis of all the transformers in the electrical system – a process that requires considerable time and resources – while the contribution of such a solution is not certain.

The absence of sufficient development and reinforcement of the protection measures is not, however, the main reason for the lack of protection against electromagnetic threats; rather, it is the lack of awareness of these threats. Raising awareness among elected representatives of the public, regulatory bodies, and private companies will pave the way to increased protection of the electrical system against electromagnetic threats. Cooperation between all relevant bodies is critical due also to the specific structure of the electricity market. In the US, for example, there are more than 3,300 different electricity suppliers, making the creation of a uniform standard very difficult and significantly increasing the time required for the implementation of any potential defense mechanisms. In this respect, the situation in Israel is far easier. The almost complete control of electricity by the Israel Electric Corporation is a clear advantage in the implementation of a defense program against electromagnetic threats.

Stages in the Development of the Defense Program

In 2013, Dr. Peter Pry, former director of the US EMP Task Force on National and Homeland Security, published a book that presents three different approaches for the defense and preparedness of the electrical system against electromagnetic events.[73] In 2011, similar research was conducted in Israel by the Unit of the Chief Scientist in the Ministry of National Infrastructures, Energy, and Water Resources in cooperation with the Electric Infrastructure Security Council (EIS)[74] with the aim of assessing the sensitivity and repercussions of electromagnetic interference on Israel's electrical system. These two studies should form the basis for the next stage in which strategies will be presented for tackling the threat, taking into account its source and character, according to three levels of defense. These strategies will establish the principles for the management of priorities for each part of the electrical system, in accordance with its importance, its public functioning, and its contribution to the continued functioning and restart after a crash. Such a program will be required to include clear and detailed standards for work procedures and technical details for all regional levels of the electrical system.

The Three Levels of Defense against Electromagnetic Threats

Level A – Full Protection. Use of the most advanced measures in order to harden the existing infrastructure and ensure continuation of its ongoing

operation during and after an electromagnetic event. This level is intended for the electrical system's command and control centers and also for systems and entities in which their functioning and the security of their digital information is of primary importance.
Level B – Rapid Recovery. Use of measures to ensure the rehabilitation and rapid return to routine after an electromagnetic event.
Level C – Gradual Recovery. Minimum use of protection measures while concentrating on the planning of rehabilitation procedures after an electromagnetic event.

Matching the Levels of Protection to the Source and Type of Threats

In the case of an electromagnetic episode, maximum importance is attached to the type of interference created, since electromagnetic pulses at various frequencies and intensities affect the elements of the electrical system in different ways. The standard division is:

1. Long electromagnetic pulse (E3) – This interference is created following a geomagnetically induced current (GIC) that is the natural result of severe space weather events or the result of a nuclear explosion at high altitude. A long electromagnetic pulse affects an extensive area and, in some cases, an entire hemisphere. Its major outcomes include damage to power stations and transformers in switching stations and substations, the melting of underground electricity cables, the burning of overhead electricity cables, and damage to electronic equipment and telephone line infrastructures.
2. Short electromagnetic pulse (E1) – This interference is commonly of a malicious nature and may be caused by a nuclear or non-nuclear electromagnetic pulse. The major threats from a short electromagnetic pulse include damage to the command and control centers used for supervision, control, and data acquisition[75] and to relays, central distribution units, and end units.

Strategies for Protection against Electromagnetic Pulses

The development of strategies for protection against electromagnetic pulses is based on matching the source and type of the influence to the three levels of protection:

1. Level A protection (full protection) and level B protection (rapid recovery) against a long electromagnetic pulse – The extensive influence

of a long electromagnetic pulse constitutes the major difficulty for the development of level A and level B capabilities of protection. In other words, the possibility of damage to a large number of critical elements (such as transformers) necessitates an approach based on an automatic mechanism that will prevent the entry of GIC into the systems. The first approach is based on early identification and an automatic system that disconnects the transformer. However, transformers today consist of protective measures, which make the disconnection approach efficient only at a certain range. The second approach calls for the prevention of the arrival of the geomagnetic current at the transformer by introducing a current limiter within the basis of the transformers of the switching stations and substations. A number of designs exist for these current limiters, some of which have already passed the stages of trials and tests. An additional method of preventing the entry of the geomagnetic current to the system is by inserting a series of electrical cables on the medium voltage lines. This method proved very successful when implemented in Quebec after the electromagnetic storm in 1989 and later in California.[76]

2. Level C protection (gradual recovery) against a long electromagnetic pulse – The structure of the electrical system and its active elements increase the risk of a long electromagnetic pulse. At present, protection of the electrical system against these effects is minimal. In the US most of the large electrical systems have adopted work procedures and ways of coping with the excessive loads created by such electromagnetic pulses. These work procedures include the reduction of electricity production, the formulation of standards for the construction of installations, and the training of crews in supplementing alternative transformers.
3. Level A protection against a short electromagnetic pulse – This level of protection is intended for sensitive installations and for command and control systems that are critical to the functioning, control, and initialization of the electrical system. This requires the installation of protective devices in designated containers. Research conducted in this field has also emphasized the importance of the selection of building materials for the installations as a factor strengthening their protection.[77] In order to provide full protection, the technical design of the electronic devices in the installations defined for this level of protection should also be examined. Additional protection options include means that are specifically adapted to protect against short electromagnetic pulses.

4. Level B protection against a short electromagnetic pulse – This level of protection is intended for a limited number of installations in the electrical system. It includes existing preventive elements of level A protection as well as spare parts (including transformers in switching stations and substations) that can replace the damaged parts in the electrical system. An important component of this level of protection is the training of response teams.
5. Level C protection against a short electromagnetic pulse – This level of protection is intended for all parts of the electrical system not covered by the requirements of levels A or B. Level C protection is mainly based on the replacement of non-functioning parts and the advance preparation of teams and detailed work procedures with the aim of optimizing the means of rehabilitation. Since a short electromagnetic pulse has a limited region of influence, the cost of protection and rehabilitation is expected to be minimal.

Costs

The estimated cost of the protection of Israel's electrical system against the effects of electromagnetic interference is $30-40 million for level A protection and about $200 million for level C protection. The project is expected to take three to five years. These estimates are based on research conducted in 2013 that addressed the strategy of combating and protecting against electromagnetic interference directed at Edison's Electric system in southern California,[78] in-depth research studies conducted in Israel in 2011 by the Ministry of National Infrastructures, Energy, and Water in cooperation with the Chief Scientist's Office and the Council for the Security of the Energy Infrastructure, and a number of additional projects. Given that the electrical system operates as a single unit, the preliminary design of its protection will allow a reduction in costs. According to the research cited above, the design of electronic systems that are protected from electromagnetic interference would cost only an additional one to five percent of the total planning expenditures of these systems.

Chapter 4

What Can Be Learned from International Experience?

The security of the electrical grid and other critical infrastructures constitutes a major contemporary global issue. Two events that emphasized the importance of this subject are the damage caused to Pakistan's electrical grid in 2015, which left 80 percent of the country without electricity,[79] and the mass blackout in 45 of Turkey's 81 provinces in March 2015.[80]

As the global leader on the subject of security of the electrical grid, the US is the main source of information in the field. In 2013, the Department of Homeland Security published the latest version of its National Infrastructure Protection Plan (NIPP 2013),[81] which details how government and private sector participants in the US should act together in order to manage risks. NIPP 2013 evolved from an earlier version that was released in 2006. This updated version meets the requirements of the Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21)[82] that was published in February 2013 and was prepared in cooperation with 16 critical infrastructure sectors in 50 states at all levels of government and industry.

This integrated program for the protection of infrastructures specified three guiding principles for the major spheres of activity:

1. Identification, deterrence, detection, and preparation for major risks to critical infrastructures.
2. Mitigation of the level of vulnerability of systems, assets, and vital networks.
3. Reduction of the potential ramifications of accidents and hostile acts on the functioning of vital infrastructures.

The US program for the protection of national infrastructure emphasizes that the optimal implementation of the guidelines and the promotion of the most effective decision making processes are conditional on the greatest

use of the inputs, capacities, and expertise of the relevant stakeholders: the public, the private sector, and the nonprofit organizations. In addition, the program claims that joint activity by the relevant stakeholders regarding the resilience of essential infrastructures should be advanced proactively by means of the establishment of partnerships, the advancement of innovation in the field of risk management, and the focus on outputs.

One of the most up-to-date and comprehensive studies on electrical grid security was published in the US in October 2014 by the Center for the Study of the Presidency and Congress (CSPC).[83] This research project continued for about a year and included ongoing collaboration work and mutual learning between government officials, legislators, and representatives of the private sector. Its main aim was to understand all the threats facing the US electrical system and to find the most effective ways to strengthen its resilience. The research expands on the following subjects:

1. Characteristics of the US electrical system.
2. Analysis of various attacks against the electrical grid, mainly over the last decade. For example, cyber attacks, physical attacks, extreme weather events, and electromagnetic events.
3. Review of the elements threatening the US electrical system: countries (Russia, China, Iran, North Korea), non-state organizations, and private entities.
4. Analysis of possible responses to various threats: physical protection, cybernetic protection, preparedness for electromagnetic pulse and extreme weather, and recovery from various attacks.
5. Actions that must be performed by the various US bodies (federal, state, and industrial).
6. Economic incentives and insurance-related aspects.
7. Future structure of the US electrical grid.

The major insight that emerged from this research is that the subject of security of the electrical system must be addressed using a structured and strategic approach based on risk analysis. The electrical system faces a large variety of threats. A focus on one specific threat is liable to prevent management of the others. It is not, however, possible to provide a perfect response to all the different threats.

Among the insights relating to the short term:

1. It is crucial that the US administration continue to take steps to increase the security of critical infrastructures in general and of the electrical system in particular.
2. It is recommended that Congress set up a legislative infrastructure for the sharing of cyber security information.
3. It is recommended that this information sharing of cyber security be conducted via automatic processes as much as possible.
4. It is important to develop programs that will permit relevant public sector employees to work for a limited period of time in the private electricity companies and vice versa for the purpose of comprehensive mutual learning.
5. It is important that the business plan for the continuation of investment in the security of the electrical system include most of the relevant private sector parties.

Among the insights relating to the short term:

1. The report recommends that the US Department of Energy continue to coordinate the overall management of security of the electrical system with the private electricity industry. The Department of Homeland Security should be the major agency for dealing with the subject of cyber in close cooperation with the American intelligence community.
2. It is important to deepen analysis of the influence of security of the electrical system on other critical infrastructures.
3. The report also proposes that Congress establish and expand the legislative infrastructure in order to increase the coordination and cooperation between all parties involved in the electrical system. It is, at the same time, important to form and strengthen partnerships between government officials and the electricity industry in order to improve the security of the electrical system.
4. Major national bodies, such as the National Guard, should be mobilized to increase the security of the electrical system.
5. It is of utmost importance that all issues concerning the smart networks, local networks, and renewable energy be thoroughly examined, including the security and credibility of the electrical system.

In May 2015, the US Department of Housing and Urban Development published a memorandum focusing on the planning aspects of the national infrastructure.[84] This report emphasizes the importance of the planning stage in the context of infrastructure resilience. It examines the various risk

scenarios, attaching special significance to disruptions caused by climate change. In order to supply real incentives for the correct execution of the planning processes, the memorandum lists the various sources of financing and technical consultation that various US government bodies may supply for infrastructure projects. The document also emphasizes the importance of ongoing cooperation between all the relevant parties at the federal, state, and local levels in order to increase resilience.

An additional important and pertinent study analyzes the ramifications and significance of Hurricane Sandy in 2012 for infrastructure resilience. It was conducted by a team of researchers from various American research institutes, led by Prof. Stephen Flynn from Northeastern University.[85] Its conclusions emphasize the need to 1) reinforce integration (regarding both inter-organizational mechanisms and technological aspects) between the various stakeholders and the various infrastructures before, during, and after emergencies; 2) fortify the various building standards for infrastructures in order to increase their resilience; and 3) provide economic incentives for extensive advanced preparedness.

In addition to this study, a comprehensive multiyear process has been underway in the US for the past few years. It is led by the federal agency the National Institute of Standards and Technology (NIST) in cooperation with various stakeholders and, by means of a dialogue with relevant bodies and foreign experts, aims to formulate comprehensive planning standards regarding infrastructures. A series of documents have, in fact, already been published for comments by the public and stakeholders. The last document in this series was published in April 2015.[86] The process aims to determine standards that will increase infrastructure resilience, identify differences that may affect this resilience, and reduce them, thus addressing both theoretical aspects and practical organizational aspects. The next planned stage is the establishment of an official advisory committee on the subject of resilience of infrastructures, the Disaster Resilience Standards Panel (DRSP), which will represent all the relevant parties and will aid in the development and integration of standards for strengthening the resilience of infrastructures.

The recommendations and the insights of the above studies were formulated for the needs of the American arena. Still, they seem in essence to be applicable to Israel and other countries. The core issues are quite similar, and therefore the US guidelines can be used in a flexible and rational way in Israel.

Chapter 5

Conclusions

General

In the State Comptroller's Annual Report 65(b) from December 2014 it was stated that:

> A central and important subject in the report is the protection of Israel's sensitive installations against the relevant threats. This report includes references to the corrections of defects that were raised in a previous report in 2010. It has been found that there has been no real progress in providing a response to the threats nor have attempts to provide partial protection of the sensitive civilian installations, in accordance with the Prime Minister's instructions, yet been completed.[87]

Two main insights emerge from the current study. First, a general national overview to address the security of Israel's electrical system is necessary. This calls for a qualified and balanced professional evaluation based on cost effectiveness (or, alternatively, on the expected damage to the economy and to national security) and its translation into a long range national binding plan. Second, the government, as regulator, must, as soon as possible, take a principled decision regarding the central question of who is responsible for the operability of the electrical system in Israel, and who will therefore bear the high costs required to meet the standards ensuring the functional continuity of the system in the case of emergency. The question of who will bear these costs – the government or industry – is less critical than the fact that the current situation is preserved, whereby no decision is taken and hence the necessary preparedness is not achieved.

The following recommendations focus on four major areas: the selection of a comprehensive strategy; technological and operational guidelines;

organizational and structural aspects; and political and community-based issues.

Selecting a Comprehensive Strategy

The leading (almost default) common approach to various types of mass disasters can be characterized by denial. It is reflected in the political echelons by the saying: "not in my term of office (NIMTO)."[88] The active management of mass disasters demands extremely difficult decisions. There is a natural tendency to avoid taking the necessary difficult decisions, as many of them might incur a very high political and/or financial price. Such critical decisions can often contradict or interfere with other interests or more immediate needs. In many cases, decision makers at all levels prefer to prioritize the urgent over the essential, which impairs their ability to act in time in order to present comprehensive responses and solutions to the severe challenges of mass disasters. This is true concerning expected scenarios and all the more so, less expected novel scenarios.

Decision makers have increasingly been pressured to abandon this simplistic strategy of denial and deferral and confront seriously the growing risks of mass disasters in a more resolute and comprehensive manner. The processes of globalization and urbanization that characterize the world intensify the risks of such disasters or serious disruptions, and create extremely high exposure to their potentially severe damage. In addition, there is growing international awareness that the adequate strategy for coping with mass disasters is to implement the "all hazards approach."[89] This relatively new paradigm advises against distinguishing between natural and man-made disasters; rather, it suggests that when addressing different hazards, it is more appropriate to focus on their consequences and severe implications than on their causes.

An approach of resistance is gradually replacing the former approach of denial and deferral. The prevailing focus among most decision makers centers on taking tangible steps to thwart, prevent, postpone, and as far as possible, provide concrete protection or mitigate the damage of the expected hazard, be it natural or man-made. This resistance approach is based on the assumption that it is possible to forecast the disruption and its dimensions, including its location, its timing, its trajectory, and perhaps even the extent of its damage, and that it should therefore be possible to prevent its very occurrence or at least mitigate its damage. The practical expression of this

strategy is the construction of "fortified walls" of various kinds, which are becoming more prevalent and more technologically sophisticated with the aim of protecting the systems, the public, and the critical infrastructures against all imminent disruptions.

The increasingly popular resistance approach has led many nations to invest huge amounts of taxpayers' money in constructing technology-based systems in the hope of preventing disruptions and mitigating their consequences. It has been widely suggested that the larger the investment in physical protection of the public and the infrastructures, the better the level of preparedness. Advanced and expensive systems, which are based on lessons learned from previous mass disasters, can in fact usually provide an adequate solution for disruptions that have already occurred or their like. A good example is the ongoing vast investment in the protection of international flights against terrorism and hijacking all over the world, years after this real threat has long diminished – precisely, according to some, due to these extreme means of protection. The fight against terror attacks has imposed a heavy financial burden on the civil aviation industry. The demand for flights is fairly flexible, and the airlines realized that in order to minimize a reduction in this demand and thus the risk to their business they would have to absorb a major share of the costs of the protection measures against attacks. In contrast to the aviation industry, the demand for electricity is generally fixed and unlikely to be affected by the threat of terrorism.

Herein lies the fundamental weakness of the resistance strategy. It is a predicted strategy which, to a great extent, provides adequate solutions for the need to cope with various kinds of expected mass disasters. At the same time, however, it does not answer all the unexpected and new hazards that characterize many of the disasters that cause extensive damage. There is no resistance solution, no matter how sophisticated or expensive, that will provide hermetic protection or serve as an absolute response to the challenges of mass disasters.

The problem is that the proven successes of advanced defense systems, such as the very impressive achievements of the Iron Dome active defense system against rockets and missiles, give an exaggerated sense of preventive capacity, which leads quickly to blind reliance on such defensive systems in expected and known scenarios, and all the more so to unexpected risks. This drawback is neither known nor understood by the general public or by most of the decision makers. Even those dealing rationally with the limitations

of the defense systems tend to seek solutions in the realm of qualitative improvements and quantitative expansion of the existing systems. "Out of the box" solutions, crucial for unexpected disasters scenarios, are rarely sought. It is thus reasonable to suggest that the resistance strategy does not provide a full response to such unexpected hazards, and this highlights the need for another supplementary, if not alternative, strategy.

The frequent resounding failures in recent years to cope with large scale mass disasters, be they natural or man-made,[90] have inspired an alternative strategy that is currently gaining momentum. This is the resilience strategy that proposes ways of thinking and preparing that complement the resistance strategy. The extensive literature has proposed various definitions of the term "resilience" that has become prevalent in the official documents of leading countries, particularly the US and the UK.[91] The definition is often broad and contains different components from the field of preparedness for mass disasters, such as the definitive wording introduced by the US National Academy of Sciences in 2012 in the comprehensive study entitled: "Disaster Resilience: A National Imperative."[92]

In order to simplify and clarify the picture, we propose that resilience be used to express the capacity of any system – be it infrastructure, human, community, economic, or national – to cope successfully with natural or man-made disasters, to contain the impact of the disaster in accordance with its magnitude and severity, to accept flexibly the expected diminishing functionality ("bend rather than break"), and to bounce back rapidly and return to normal systemic functioning at a level permitting preservation of the original identity and functioning of the system or even its improvement.

Several essential elements regarding resilience should be emphasized:

1. Resilience will always be manifested in the context of a disaster[93] or a severe disruption that threatens the functionality and possibly the core identity of the impacted system, or at least significantly harms the central functions that define it.
2. The resilience concept assumes that there will always be a functional degradation of the system following a major hazardous episode. If there are no indications of a functional degradation, then no real damage has taken place, which means that no disaster actually occurred.
3. The key feature for resilience is the phenomenon of bouncing back following the degradation phase. The length of time it takes the system

to bounce back to the original level of functioning, or possibly to a higher level, signifies the rate of its resilience.

The leading idea in the resilience concept is the need to create or intensify the ability of the system in question to recover rapidly from a significant disruption and return to normal functioning.[94] This functioning does not have to be identical to the original level, provided that it manifests the core values or goals of the system. A system with a high degree of resilience will return to normative functioning more rapidly than a system that is characterized by medium or low resilience. The crucial benchmark can be gauged by the length of time needed for the return of the affected system to its original functioning level.

Another important notion holds that the generic level of resilience of a given system is neither constant nor guaranteed. In order to sustain the required level of resilience, there is need for rational, well planned, proactive, and continuous action to promote the effective functioning of the impacted system after the failure of the protective walls that were set up to prevent the disaster or minimize its damage. One of the difficult tasks in the resilience concept is the creation of tools, processes, and mechanisms that will guarantee the necessary level of system recovery after the disaster has occurred. From this perspective, the resilience theory offers a broad conceptual basis; it calls, however, for differentiation in the selection of the tools necessary for boosting the capabilities of the system in accordance with the relevant risks on the one hand, and the characteristics of all the systems, on the other.

The generic resilience strategy is supposed to supplement and reinforce the resistance strategy by focusing on the stage after the breakdown of the defensive barriers and ensure rapid recovery and the return to systemic functioning. The wide range of systems necessitates a wide range of means and their adjustment to the characteristics of the system. For example, the societal/community resilience approach requires the use of tools of preparedness and reinforcement, which are different in nature from those used to enhance infrastructure resilience. Likewise, within the realm of infrastructure, different measures should be adopted in order to promote the resilience of the various critical infrastructures, including the energy sector, in accordance with their particular specifications.[95]

What follows are a number of overall approaches, methods, and tools that are relevant for the enhancement of the resilience strategy in connection with the strengthening of the security of Israel's electrical grid.

Technological and Operational Guidelines

Deployment for Climate Change

In addition to global and local efforts to improve energy efficiency and the reduction of emissions, the most realistic response to the ramifications of climate change lies in promoting the resilience of the systems that might be affected by it. This can be enhanced by central and local governments, as well as by the public at large.

The Israel Electric Corporation's system management unit currently has excellent capabilities to forecast the weather, in particular the parameters (such as temperature and heat load) that influence the consumption of electricity as well as the conventional production of electricity. However, synergy must be created with affiliated systems in order to expand the practice of analyzing long term trends. Adaptation activities are already underway in many places throughout the world by means of planning with consideration for different time periods and levels of decentralization, and for the size and variety of the sources of production and the infrastructures (for example, in the electricity market in France after the protracted heat wave in 2003). In the coming years, with the increase in production capacity that is based on renewable energy, the Israel Electric Corporation's system management unit will improve its capabilities regarding weather parameters that are related to electricity production, such as solar radiation, wind velocity, and so forth.

Great importance is attached to the estimation and management of risks according to the various scenarios of climate change: incremental climate change (rise of sea level, frequency and intensity of storms and their influence on the location of coastal energy infrastructures) and extreme climatic events (heat/cold waves) that will influence both the functioning of infrastructure networks and critical services in the national energy supply system and the functioning of critical infrastructure systems that are supported by energy supply systems.

With regard to the planning contexts, it is important that the deployment and preparedness of the energy industry for different climate scenarios be adapted to every geographic region and its particular demands; there is no single, tailor-made solution for risk reduction. Each stakeholder, at every level, has a complementary role in planning and implementation of the adaptation design. All interested partners should strive to achieve synergy in the steps taken to reduce risks. In these processes the cost factor must also be considered, so as to moderate the financial burden on the customers.

One important way to ensure the effectiveness of risk reduction is to take an inclusive approach regarding other risk factors such as earthquakes and security threats. Various constraints are liable to lead to harmful adaptation actions that might be caused by lack of awareness, limitations of resources, inadequate integration, or over-emphasis on short term results.

It is possible to insure a localized system against the ramifications of a disaster. Damage at a national level, on the other hand, is usually insured by the state, which is capable of assuming responsibility for the damage. For example, the Israeli government knew how to create one of the most advanced insurance systems in the world for agriculture (a joint company of the government and the farmers called the Insurance Fund for Natural Risks in Agriculture [KANAT]). This company set up a mechanism for insuring against natural disasters while distinguishing between a "local" and "national" natural disaster, which enables management of the financial damage of a large natural disaster.

We recommend that the Ministry of National Infrastructures, Energy, and Water promote the recommencement of the writing of standards for additional sections of Standard 413 (which addresses the construction of earthquake-resistant buildings and houses), emphasizing the electrical installations that are not currently covered by the Standard and requiring critical electrical installations to comply with these standards. Furthermore, we propose the installation of transformers and water pumps around power stations near the coast that will automatically start working in the event of flooding.

Decentralized Conventional Production Facilities

The development of a distribution network for natural gas enables the establishment of local units for the production of electricity and thermal energy that are connected to the medium voltage electrical grid with a capacity of up to about 16 MW. These production units allow for the continual functioning of the specified area (kibbutz, university campus, commercial shopping center, etc.) even in the absence of supply from the electrical grid (although they are dependent on a regular supply of gas and are exposed to the risk of non-supply or partial supply depending on the nature of the backup installations to be constructed on every site).

The decentralized private production of electricity, with a capacity of up to 16 MV, will primarily serve the medium voltage consumers connected to the substations. No use, therefore, will be made of the high voltage electrical

grid, which is more exposed to unusual events, and the output of the power station will be transmitted short distances to the consumers connected to the substation.

The construction of decentralized power stations will facilitate the provision of significant output in their vicinity, while maintaining the option of the immediate transition to working in "island mode" in the event of a disruption, so as to respond to the required consumption.

Power stations with a low nominal capacity in the medium voltage electrical grid are generally characterized by the implementation of motor technology. A motor has a crucial technological capability that is expressed in its ability to achieve full production capacity within two minutes, while the time required for the most successful turbine to reach full production capacity is at least fifteen minutes. Only pumped storage electricity production technologies are capable of faster entry into electricity production (and this refers to storage, and not production). Consequently, the power stations that operate using motor technology can serve the system manager as backup units for a rapid response to a sharp drop in the production capability of the various manufacturers or to a sharp increase in the demand for electricity.

Production Facilities Using Renewable Energy

Renewable energy is defined as energy that does not incur environmental pollution and uses resources that are naturally replenished. The best examples of renewable energy are solar energy, wind energy, and energy generated from biogas. The best use of renewable energy is for the production of electrical energy, although it can also produce thermal energy, which in turn is used for numerous industrial and domestic applications such as heating, cooling, and so on

Over the past fifteen years, awareness has increased throughout the world, including in Israel, of the need to expand the use of renewable energy into a greater percentage of the total use of energy for the production of electricity. This awareness is reflected in government decisions[96] and in the Electricity Authority's regulations for the promotion of the construction of electricity generation facilities based on renewable energy. The most obvious and effective regulations have been in the field of solar and photovoltaic energy. In the coming years, significant developments are also expected in the fields of wind and biogas energy.

The production of electricity from solar, wind, and biogas energy has a number of outstanding characteristics that are relevant to the security of the electrical grid:

1. *Less dependency on a vulnerable infrastructure*. While it is possible to harm electricity production facilities that are driven by natural gas or coal by damaging the supply lines, sun rays or wind cannot be prevented from reaching the production facilities nor can the biological process producing biogas be obstructed. Sources of renewable energy are, therefore, regularly available even during any type of electricity disruption. Renewable energy can serve as an available substitute for some of Israel's electricity needs.
2. *Scalability of the system.* Production facilities using renewable energy may generally be constructed with a broad range of capacities, starting from a few KW and reaching tens or even hundreds of MW. This means that renewable energy production facilities may be used to ensure the supply of electricity (at least partially) for relatively small areas, such as private homes, condominiums, and even for neighborhoods, industrial zones, kibbutzim, and moshavim, regardless of any damage incurred to the transmission and distribution infrastructure that feed these areas.

   This characteristic, which provides a modular production solution, matches the widespread trend in the planning of modern electricity systems, namely, "islanding." Islanding refers to groups of consumers as a local system (micro-grid) that can, as a result of a malfunction, be separated from the national grid and yet continue to enjoy electrical functioning. Current regulations, however, do not permit working in this "island mode." In the absence of proper grid voltage and frequency, the convertors currently approved for use cannot transfer the capacity of the photovoltaic system to the electrical grid. This ruling is rational for medium and large photovoltaic systems that do not have close and identified consumers. However, we suggest a reappraisal of these regulations regarding small systems, particularly domestic.
3. *Survivability of the facility*. Production facilities using renewable energy with significant production capacities are generally deployed over a large area, thereby increasing their chances of being hit by missiles and rockets. However, these facilities are modular, and thus the unserviceability of one will usually not shut down the entire production facility. For example, a large photovoltaic facility with a capacity of about 40 MW

currently located in southern Israel is to be connected to the high voltage electrical grid. This installation comprises about 400,000 modules and 40 convertors. Damage to a few tens or hundreds of modules will have a negligible effect. Furthermore, the time required to replace damaged convertors is relatively short, and, assuming that there is a suitable stock, replacement will only take a few hours or days.

4. *Speed of set up/repair*. The modularity of the production facilities using renewable energy, especially solar photovoltaic energy, allows rapid construction and replacement of damaged parts in the facility, and in fact increases the speed of rehabilitation of the entire system following damage. For example, if a photovoltaic facility in Israel is damaged, it will only take a few weeks to replace the damaged modules. Damage to a conventional facility caused by rockets would, of course, be far more serious, and the repair time would therefore be far more protracted.

Most of the production facilities based on renewable energy currently have a significant disadvantage compared to those using conventional energy due to their dependence on an energy source that is not always available, such as sun or wind. The solution to this problem lies in storage facilities that can enable bridging between periods when the source of the renewable energy is available and when it is not available. Various methods exist for energy storage (thermal, electrical, water, and compressed air storage), and it is still too early to say which method is preferred. It is likely that different storage methods will match different quantities of energy.

Storage in solar thermal projects enables the continuous flow of renewable energy to the electrical grid. The Israeli government has initiated Ashalim, a project that includes two solar thermal power stations (as well as one photovoltaic power station): one is based on parabolic trough technology (that uses concave mirrors to focus sunlight on a heating element located in the center of the mirrors) with a nominal capacity of 136 MW; and the other is based on solar tower technology (that makes use of a field of moving mirrors, heliostats, which focus sunlight on a central heating element that is located at the top of a reception tower) with a nominal capacity of 125 MW.

In a world in which the means of production are based on fossil fuels, such as gas, coal, diesel fuel, and fuel oil, renewable energy plays an important role in a range of production sources and sites. Management of an electrical system which is connected to numerous sites of solar energy, wind energy, and pumped storage (see below) could improve the survivability of the system

and strengthen the general security of the electrical system. We therefore recommend accelerating the development of renewable energy in Israel. We also propose that Israel adopt a policy that will enable the continued supply of electricity following a disruption to ensure operational continuity in the private home and, subsequently, in other consumer sectors.

Pumped Storage

A number of pumped storage projects are currently being advanced in Israel, each with a capacity of hundreds of MW. Pumped storage facilities pump water from a lower to an upper reservoir during off-peak demands for electricity and release the water in the opposite direction, thus exploiting its energy for the production of electricity, during peak demand or according to the need of the electrical system. Pumped storage facilities have an especially rapid response and are, consequently, a vital tool in the hands of the electrical system manager for treatment of emergencies. These installations can also supplement the missing hours of the production of renewable energy and, by means of integrated management, enable the flow of electricity to the grid over a course of time.

The current regulation regarding pumped storage facilities fixes the quota at the overall amount of 800 MW. This figure was, apparently, determined either because this was the capacity of the proposed pumped storage project at the Israel Electric Corporation's site by the Dead Sea or because this figure constituted about 8 percent of the overall nominal capacity of the electrical system at the time and pumped storage capacity tends to lie between 8 and 10 percent of the total nominal capacity. In the intervening years since this regulation was issued, the total nominal capacity has increased and is today greater than 13 GW. The scale of the production facilities using renewable energy has also increased considerably, which necessitates storage capability. It therefore seems appropriate to enlarge the quota allocated for production facilities using pumped storage due to both their high defensibility against various threats and their contribution to the extended use of production facilities using renewable energy.

Accessibility

The Israel Electric Corporation explained some of the delay in restoring the electricity supply to consumers during the events of the winter of 2013 as a result of the difficulty in reaching sites where the electricity infrastructures

were damaged. This was due to both the shortage of suitable equipment and the behavior of civilians whose vehicles blocked the main routes. These events exposed the problems of accessibility and the availability of maintenance teams during serious disruptions.

This highlighted the need to monitor the shortage of vehicles with high accessibility, estimate the cost of their procurement, and examine the cost-effectiveness and feasibility of self-equipping by the Israel Electric Corporation. Self-equipping should be compared with the option of using military equipment at times of emergency, taking into consideration their immediate availability. Shared procedures must also be examined and formulated for the Israel Electric Corporation and the Israel Police to ensure the barring of civilians from regions of high risk as well as the free and fast flow of first responders to the affected arena.

Electromagnetic Pulse

In contrast to other threats that have already occurred, at least to some extent (attacks by missiles and rockets, natural disasters, cyber attacks), the electromagnetic pulse threat has not yet occurred. The potential intensity of this threat and the low cost of protection against it require the allocation of financial resources to the Israel Electric Corporation.

It is still not possible to accurately assess the likelihood that the electromagnetic pulse threat will be realized. Consequently, the risk it entails needs systemic attention, including the adequate preparation of programs and response teams as well as careful investment in the hardening of the relevant infrastructures. This will significantly improve the capability of the system to meet electromagnetic pulse threats and even to prevent the collapse of the electrical system. The major barrier to coping with this threat results from lack of awareness and insufficient familiarity.

Guidelines regarding Organization and Structure

For many years "Israel Electric Corporation" and "the electricity industry" were synonymous. It was therefore logical for the Israel Electric Corporation to be responsible for the preparedness of Israel's entire electricity sector, including in a state of emergency. This was enabled by the High Authority for Power (Electricity) During a State of Emergency that forms part of the National Emergency Management Authority (NEMA) (Hebrew MELACH) which is responsible for the civilian economy during times of emergency.

This authority was headed by the CEO of the Israel Electric Corporation, and most of its members were company employees. There are, we believe, at least two reasons to now change this historical situation.

First, the Israel Electric Corporation is tested and increasingly managed by means of business and economic considerations. These are not always identical to state and security considerations, especially prior to a crisis or during emergencies. The gap is therefore widening between the Israel Electric Corporation's interest in making investments from its own resources in preparedness for emergencies and the broader recognized needs for preparedness for emergencies.

Second, while still the major producer, the Israel Electric Corporation is no longer the sole producer of electricity in Israel; there now operate alongside it other significant producers. The Israel Electric Corporation's share in the production of electricity is likely to stabilize within a few years at approximately 60 percent of total production. In the field of transmission, the Israel Electric Corporation will, at least in the foreseeable future, remain the sole player, but in the fields of distribution and supply there are already additional players, albeit on a relatively small scale.

The future of the system management unit, one of the most important functions in the operation of electricity at times of emergency, is under examination and consequently is unclear at the moment. In discussions about the reform of the electricity sector, it seems that there has been some agreement, at least in principle, that the system management unit will cease to be part of the Israel Electric Corporation and will instead become a government company; however, the future of the entire reform remains ambiguous. We predict that if and when these discussions are renewed and reform subsequently implemented, the system management unit will operate, in some form or other, outside of the Israel Electric Corporation. Responsibility for the management of the electricity economy during emergencies will, therefore, not lie with the Israel Electric Corporation.

On the other hand, it seems that state agencies, mainly the Ministry of Energy, currently lack sufficient tools to replace the Israel Electric Corporation in the actual management of electricity during emergencies. Israel's security agencies are likely to have better and more efficient management resources for such management, but they lack the adequate professional knowledge. Furthermore, the defense establishment's availability to assist the civilian

electrical system during emergencies will be limited due to the more urgent needs of the day.

The preferred solution would be to set up a higher authority for power (electricity) inside the electricity administration of the Ministry of National Infrastructures whose major functions would comprise:

1. Formulation of policy for the operation of electricity during emergencies.
2. Advancement of primary and secondary legislation on the matter.
3. Determination of standards for the operation of the system.
4. Planning of the future system while determining responsibility, a timetable, and a budget in accordance with needs.
5. Supervision of the implementation of the policy and execution of the program by the Israel Electric Corporation and the other private utility providers.

If the decision is taken to set up this higher authority for electric power, it will be necessary to construct flexible but agreed mechanisms that will ensure horizontal collaboration and cooperation between the regulator and the other governmental parties, such as NEMA, the Home Front Command, and others, as well as vertically, with the Israel Electric Corporation and all other service providers in the electricity sector. While such mechanisms are essential, they are not easy to set up and operate. Israel's prior experience regarding preparedness for emergencies and operation of the electrical system during emergencies is not encouraging. We must learn from acknowledged failures and build an improved model that will ensure optimal operation of the system during a state of emergency. One important question in this context is: who will fund the preparedness and operation during emergencies – the state or the operator?

Community Guidelines

General

All future preparation for improving the capability of the electrical system to cope with mass disasters must take into account human, organizational, social, and political aspects as a basis for building a suitable response to threats against the system. All these aspects must form part of the preliminary design and the subsequent implementation in the field, in addition to and combined with the technological and organizational aspects set forth above. It should be emphasized that the overall resilience of the electrical system

necessitates a range of combined efforts in order to improve the chance of rapid recovery in the wake of serious disruptions.

Our basic assumption is that each of the elements is important in and of itself. However, only the strict integration of all – in preliminary thinking, planning, preparation, drilling, and ongoing control – will ensure the best results.

Our recommendations in this category will be presented in accordance with the different target audiences. They mainly address extreme emergencies including "black sky events."

Electrical Grid Operators

Electrical system operators constitute an essential and primary link in the restoration of normal functioning in the wake of severe damage. The operators themselves will be directly or indirectly affected by the disruption, which might postpone or reduce their capacity to achieve full and rapid recovery. This might constitute a significant drawback in the overall capability. A series of considerations must thus be made in advance such as: recognition of the professional challenge and ways to deal with it, and ways to enhance situation awareness; the presence of professional staff (quantitative and qualitative) on the relevant sites; and the training of the teams to act under unfamiliar conditions and in environmental chaos. It is important to find ways to overcome such barriers, including the careful planning of operational teams for extreme events; the preliminary placement of professional and semi-professional staff for long periods of time; the planning and execution of training schemes, exercises, and simulations based on expected (and less expected) scenarios; the employment of managers at the various levels needed for the engagement of expanded work teams at times of emergency; the formulation of plans for boosting the motivation of employees (and their families) in order to guarantee their full agreement to work under difficult emergency conditions over an extended period of time.

First Responders

In extreme events, the damaged electrical system will create high dependence on the external elements that are supposed to provide information, support, aid, and rescue for the system operators and internal emergency teams. The greatest and most immediate barrier to the proper functioning of the first response teams will be the damage to the orderly supply of electricity that

is essential for the operation of these teams. Such damage is also liable to disrupt the telecommunications required for the operation of the various teams in the field.

The command and control system is liable to be seriously if not totally disrupted, at least in certain, possibly critical, segments. Telecommunications are naturally vital in such cases not only between external aid bodies and persons in the damaged electrical system but also within the external aid agencies themselves. This refers not only to the essential training aspects of multisystem and multichannel telecommunications – a condition for the successful restoration of the system after a crash – but also to the decisive issue of command and control at different levels. This central issue must be addressed in advance.

The emergency system must be planned according to a possible shortage of fuel that is liable to seriously affect the arrival of the emergency teams at the relevant sites and their ability to function. The internal and external teams must be briefed and trained to act in time of extreme fuel and electricity limitations. There must be special procedures for such scenarios, in addition to alternative means of telecommunications. Extended dependence on external bodies creates unexpected obstacles, including the confinement of external forces to this and other sites. These also necessitate a program of prior coordination, joint procedures, and joint command and control systems, the setting of priorities in the allocation of forces, and ongoing joint exercises with all the external bodies likely to be cooperating in emergencies.

Customers, the Community, and the Public

Supplying electricity is currently regarded as the task of the authorities alone, both in the everyday and at times of emergency. This is in contrast, for example, to the case of water in which it is easy to explain to the public that they should be prepared for a minimum supply of water at times of emergency. Technically speaking, it is possible to supply a certain amount of electricity independently by means of simple and cheap devices that will enable the operation of basic domestic appliances: for example, outlets for low-power appliances such as computers, phones, refrigerators, and others. Subsidies or public explanations could be used to encourage the purchase of such devices. For example, systems currently exist for the local production of electricity with a nominal capacity starting from 1 KW that can supply most of the electrical consumption and thermal energy of a household. Each

household whose basic electricity means are thus supplied considerably aids the authorities in times of emergency.

The greatest challenge is the ability to change the approach of the electricity consumers from potential victims of a prolonged blackout and its possibly serious ramifications to an active and functioning community capable of functioning even at a time of protracted emergency. In many cases, a blackout is likely to be only one of the aspects of the disaster.

Our initial assumption is that a passive community is a vulnerable one that hinders both its own capacities and the capacities of the first responders and service providers. An active community, on the other hand, has greater resilience, which allows it to recover rapidly and cope effectively with various disruptions while mobilizing its own resources, including those damaged as a result of the serious disruption. The overall aim is to maximize the potential of the community and all its elements – the people, the groups, the informal organizations, and the volunteers – and to transform them from victims to assets.

Understanding this concept demands ongoing efforts in advance of the occurrence of disaster. Both the formal and informal leaders of the community must be aware of the expected risks and act accordingly in order to increase the social resilience of the community. In every community there are important bodies with great potential to help that can be recruited in advance, such as high school and college students and various volunteer organizations. Their recruitment and training, including for action during times of emergency, may be done by means of special emergency programs.

During emergencies special importance is attached to the circulation of relevant information to the public. Lack of sufficient information constitutes a major obstacle. Consequently, prior arrangements should be made for the distribution of information, even under restricted circumstances. There should also be special provisions and programs for people with disabilities both in institutions and in the community at large.

Efficient functioning at times of emergency demands prior training. We suggest holding a power outage drill in specific areas once every few years in which the functioning of all the emergency systems and forces can be examined. A decentralized electricity production system, for example, increases the community's ability to act independently and supply its own energy while attempting to stabilize living conditions at their routine level in a short period of time. The current establishment of production units with

a capacity of up to 16 MVA within the areas of kibbutzim and industrial zones may be an important step in this process.

The Media

The media is of special importance during times of emergency. Both traditional media and digital social media will continue to serve as major resources, assuming their relative availability. The issue of media availability and accessible and reliable alternatives demands prior attention. Credible media and the flow of public information is an absolute necessity for obvious psychological and emotional reasons.

Advance attention must also be paid to the planning and construction of an orderly flow of information and communication to the public during emergencies. We suggest a unified telecommunications center whose major role will be to update the public regarding developments and instructions. The electrical system must be part of this endeavor.

Summary

The need to provide a response to the threats to Israel's sensitive infrastructure installations demands an extensive and comprehensive national effort far beyond the electrical system's professional responsibility. Existing institutional regulations do not provide an adequate response. A fundamental change is necessary, alongside the creation of a system that will ensure societal resilience for the entire public in the event of serious long term disruption to the electricity supply.

A sense of national awareness and understanding must be fostered among decision makers that will form a solid basis for the formulation of clear national policy and for long term planning, the orderly distribution of functions, the allocation of priorities, and the ongoing monitoring of actual implementation. There are many different partners outside the electrical system involved in the proper handling of the challenge; this makes it even harder to manage than just the necessary technological preparedness.

System preparation for extreme conditions is a difficult, protracted, and multifarious process. It is possible, however, provided there is suitable awareness at the various levels. This is precisely why there is already a pressing need for the entire gamut of stakeholders to think, plan, and act; they will thus be ready to provide a proper systemic response in time and not, as has often been the case, be forced to improvise while under the pressure of disruptions.

Appendix: Basic Terms in the Electrical System

Voltage and Current

If the electrical system is compared to the fluid system, then electrical voltage corresponds to the pressure of the liquid. The electrical current corresponds to the flow of liquid, in other words, the rate of fluid flow. The voltage is measured in volts (V) or KV (thousands of volts), and the current is measured in amperes (A).

There are a number of standard levels of voltage in the electrical system in Israel:

1. Extra high voltage of 400 KV
2. High voltage of 161 KV and a few dozen kilometers of 110 KV
3. Medium voltage of 33 KV, 22 KV, 12.6 KV, etc.
4. Low voltage of 0.4 KV
5. In private installations (not in Israel Electric Corporation electrical grids) there is also very low voltage of 50 V, and in special applications, 24 V (agricultural sites) and 12 V (swimming pools).

Frequency

Most of the electrical systems operate using alternating current (AC), and their currents and voltages vary cyclically. The frequency is the number of cycles per second and is measured in units of hertz (Hz). The usual frequencies throughout the world are 50 Hz or 60 Hz and, in special applications, also 16.67 Hz and 400 Hz. The frequency customary in Israel is 50 Hz.

Power

Electrical power is the quantity of electrical energy per unit of time. It is usually measured in units of watts (W) and sometimes (mainly when speaking of motors) in units of horsepower (HP). The electrical capacity is proportional to the production of voltage and current. A given quantity of

power may be transferred at low voltage and high current or at high voltage and low current.

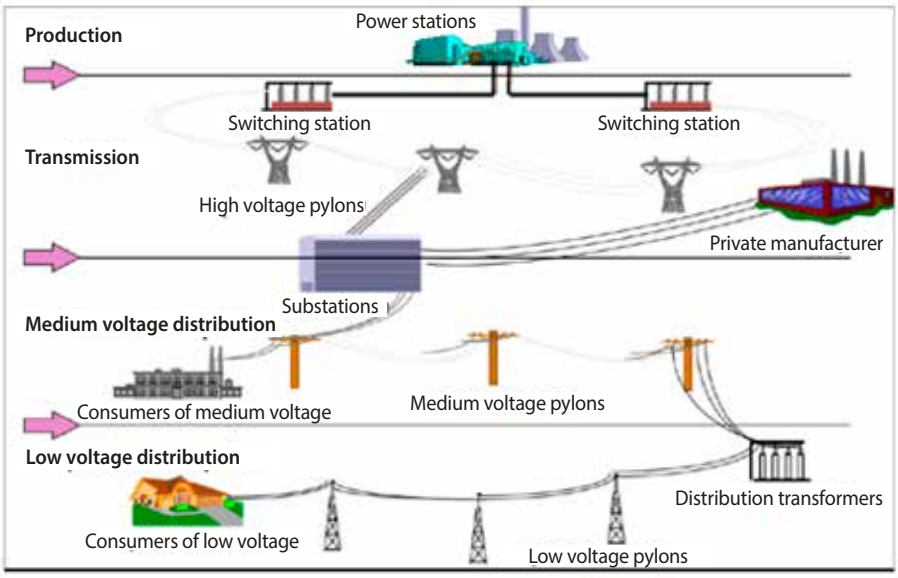

Fig. 1. The physical segments of the electrical system

The higher the voltage, the greater its danger and the larger the safety margins necessary to prevent injury. The higher the current, the greater the losses of the electrical grid. Consequently, electricity intended to travel long distances from the power stations to the proximity of the consumers is usually transmitted at high voltages and with a low current. The losses of the electrical grid are thus minimized and the necessary safety margins maintained with no particular difficulty. As electricity reaches the consumers, the voltage is lowered (which reduces the safety margins) and the current increased. While the increase of the current in the proximity of the consumers does increase the losses, this is acceptable due to the relatively short distances.

Transformers

A transformer is a device that enables changes in the voltages and currents. Transformers are usually defined according to the input and output voltages and the power that it can transform.

Segments of the Electrical System

It is customary to divide the electrical system into the following physical segments (fig. 1):

1. Generation – This segment includes the electricity production units.
2. Transmission – This segment includes the transmission grids with voltages of 400 KV, 161 KV, and 110 KV, switching stations that constitute intersections of the transmission grids, and substations that connect the 161 KV grids to the medium voltage grids of 33 KV, 22 KV, and 12.6 KV. In the transmission segment, electrical energy is transferred from the production units to the edges of the consumption centers. Only a small number of consumers (less than 50) or a particularly large number of consumers are connected to the transmission grid.
3. Distribution – This segment includes medium voltage distribution grids of 33 KV, 22 KV, and 12.6 KV, low voltage grids of 400 V, and the transformation stations that connect the medium voltage grids to the low voltage grids. In this segment the electrical energy is transmitted from the substations to the consumers. Some consumers (about 3000) use medium voltage, while most (about 2.5 million) use low voltage.

Notes

1 Consumption data in kWh per year are taken from the website of the World Bank. See http://data.worldbank.org/indicator/EG.USE.ELEC.KH.PC.

2 "Results of the Research Estimate the Cost of the Non-supply of Electricity," Ministry of National Infrastructures, November 2011, http://energy.gov.il/GxmsMniPublications/AlutHashmal.pdf.

3 In the opinion of the chair of the Israel Electric Corporation, the cyber threat is more significant than the kinetic threat. Cyber attacks are already regarded as being equivalent to seven accurate missiles a day. Conference: "Securing Israel's Electric Grid," Institute for National Security Studies, October 28, 2014.

4 According to Dr. Avi Shapira, chairman of the Inter-Ministerial Steering Committee for Earthquake Preparedness, there is a high probability of an earthquake occurring in Israel of between 6 and 7.5 on the Richter scale that will cause damage to infrastructures. including the electrical grid. This risk must be addressed, but no one is currently accepting responsibility. See conference "Securing Israel's Electric Grid," Institute for National Security Studies, October 28, 2014, https://goo.gl/KMtXZ7.

5 According to Shlomo Wald, former chief scientist of the Ministry of National Infrastructures, the current strategy in the energy sector does not address the subject of emergencies. See "Securing Israel's Electric Grid."

6 According to Wald, work in this field is not keeping up with the rapid developments around the world. All former drafts of plans have been found irrelevant to the developing security and economic reality.

7 According to Betzalel Treiber, head of the National Emergency Authority, "Securing Israel's Electric Grid."

8 According to the chair of the Israel Electric Corporation, "Securing Israel's Electric Grid."

9 Ibid.

10 "Is the Israeli Economy Prepared for a War with Iran?" *NRG*, August 24, 2012, http://www.nrg.co.il/online/16/ART2/398/054.html.

11 "Integrated Research on Disaster Risk (IRDR), Strategic Plan 2013-2017," IRDR, http://www.irdrinternational.org/wp-content/uploads/2013/04/IRDR-Strategic-Plan-2013-2017.pdf.

12 "The Sendai Report, Managing Disaster Risks for a Resilient Future," GFDRR and the World Bank, 2012, https://www.gfdrr.org/sites/gfdrr/files/publication/Sendai_Report_051012_0.pdf.
13 S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine* 21, no. 6 (2001): 11-25, http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.
14 S. M. Amin and B. F. Wollenberg, "Toward a Smart Grid: Power Delivery for the 21st Century," *IEEE Power and Energy Magazine* 3, no.5 (2005): 34-41.
15 An exceptional example is a recent book with several interesting articles on the subject. See V. Gurevich, *Cyber and Electromagnetic Threats in Modern Relay Protection* (Boca Raton, FL: CRC Press, 2014).
16 I. Sharkansky, "Local Autonomy, Non-Governmental Service Providers and Emergency Management: An Israeli Case," *Journal of Homeland Security and Emergency Management* 4, no. 4 (2007): 1-8; N. Laor, Z. Wiener, S. Spirman, and L. Wolmer, "Community Mental Health in Emergencies and Mass Disasters: The Tel-Aviv Model," in *The Trauma of Terrorism: Sharing Knowledge and Shared Care*, eds. Y. Danieli, D. Brom, and J. Sills (New York: Haworth Press, 2005), pp. 681-94.
17 M. Elran and A. Altshuler, "The Civilan Front in Israel: A Framework for Future Preparedness," in *Strategic Survey for Israel 2013-2014*, eds. S. Brom and A. Kurz (Tel Aviv: Institute for National Security Studies, 2014), pp. 145-87, http://www.inss.org.il/publication/the-civilian-front-in-israel-a-framework-for-future-preparedness/?offset=9&posts=13&outher=Alex%20Altshuler.
18 Sharkansky, "Local Autonomy, Non-Governmental Service Providers and Emergency Management"; E. Ben-Harush, "The Responsibility of the State with Regard to a Weakened Citizen in the Second Lebanon War: The Elderly and Invalids as a Case Study" (Graduation paper, Israel College of National Defense, 2007).
19 Since that time, various estimates have been made in public, with other numbers referring to between 100,000 and 140,000 missiles and rockets possessed by the two organizations.
20 Elran and Altshuler, "The Home Front in Israel."
21 Iron Beam is a new system under development in Rafael that aims to provide a laser-based response to mortar shells and short range rockets which are beneath the range of Iron Dome, *Israel Defense*, January 18, 2014.
22 M. Elran and A. Altshuler, "The Civilian Front in Operation Protective Edge," in *The Lessons of Operation Protective Edge*, eds. Anat Kurz and Shlomo Brom (Tel Aviv: the Institute for National Security Studies, 2014), pp. 121-27.
23 M. Elran and A. Altshuler, eds., *The Complex Mosaic of the Home Front in Israel*, Memorandum 120 (Tel Aviv: Institute for National Security Studies, June 2012). See the remarks of Giora Eiland (pp. 21-25) as presented in the conference "The Preparedness of the Civilian Front for War" held at the Institute for National Security

Studies on September 5, 2011. On the current topic Eiland said: "The most significant change is that the accuracy [of their missiles] has increased. This change has turned them from statistical to accurate weapons. The moment we are speaking of accurate weapons, they are no longer firing them at targets the size of Tel Aviv but at specific targets, be this a power station… a military HQ, or an airfield. These will be the targets. Our defense concept states that we are providing regional defense….The point is that even this regional defense, even in the best situation, will not stop all the missiles. If it is extremely successful, it will stop 60 percent, 70 percent, 80 percent of the missiles. 20 percent will penetrate. … This is not 20 percent falling statistically in some places but 20 percent aimed at very specific places. And now the question is whether these places…are properly protected, *and the answer is certainly not*. … If you look at the power stations in Israel, you will find that the major power station is in Hadera. It supplies most of Israel's electricity. If you take all this power station and ask what cannot suffer damage from the state's perspective, you end up with two relatively small buildings…if what is in these buildings is hit, it is not only a question of money, i.e., how much will it cost to repair it, but it is also a question of *how long it will take. The State of Israel may be six months in a situation in which it cannot supply its electricity needs*. Now the question is whether these two buildings, which stand just like two exposed buildings in the area, should be given the same protection as every neighborhood and residential building and every other site or whether you say…that there is priority for targets. …The same applies to defense: do you give priority to the defense of targets and protect specific places saying that even if the missile penetrates and hits, *at least it will not affect Israel's electricity supply*? The amazing issue in this question is not whether there is money or not but rather that there is an inconclusive debate around who bears responsibility for this matter" (emphasis added).

24 Analysis of Dr. Sinaia Netanyahu, chief scientist of the Israel Ministry of Environmental Protection, presented at "Securing Israel's Electric Grid."

25 Y. Rotstein, and E. Arieh, "Tectonic Implications of Recent Micro-Earthquake Data from Israel and Adjacent Areas," *Earth and Planetary Science Letters* 78, no. 2-3 (June 1986): 237-44, http://www.sciencedirect.com/science/article/pii/0012821X86900646.

26 Z. Ben-Avraham, M. Lazar, U. Schattner, and S. Marco, "The Dead Sea Fault and its Effect on Civilization," in *Perspectives in Modern Seismology*, ed. F. Wenzel (New York: Springer, 2005), pp.145-67, http://www.tau.ac.il/~zviba/uri/abs/ZBA_et_al_2005.pdf.

27 R. Avni, "Jericho 1927 Earthquake: A Macroseismic Research on the Basis of that Period's Sources," Ph.D. dissertation, Ben-Gurion University of the Negev, 1999; B. Z. Begin, "Destructive Earthquakes in the Jordan Valley and the Dead Sea – The Intervals of their Recurrence and the Possibility for their Occurrence," *Geological Survey of Israel*, Ministry of National Infrastructures, 2005; A. Salamon, "Natural Seismogenic Effects of the February 11, 2004 ML = 5.2 Dead Sea Earthquake," *Israel Journal of Earth Sciences* 54, no. 3 (2005): 145-69.

28 S. Zwebner, "The Preparedness of the State of Israel for Earthquakes," Knesset Information Center, October 2006, http://www.knesset.gov.il/mmm/data/pdf/m01582.pdf.
29 "The National Reference Scenario," ready.org.il: website for advancement of awareness and preparedness for emergencies, October 2012, http://ready.org.il/israel/nationalscenario/.
30 M. Elran and A. Altshuler, "How Prepared is Israel for Earthquakes?" *INSS Insight* No. 380, October 31, 2012, http://www.inss.org.il/publication/how-prepared-is-israel-for-an-earthquake/?offset=11&posts=13&outher=Alex%20Altshuler.
31 "Preparedness of the Local Authority for Coping with the Results of an Earthquake," National Emergency Management Authority, November 2007, p. 11.
32 See IS 413 on the website of the Israeli Standards Institution, https://portal.sii.org.il/heb/standardization/teken/?tid=7dc4df43-7c94-4326-8727-b2e656104b64.
33 Information from website of MIFAM, the system of training and development centers in local government, http://www.mifam.org.il/_Uploads/dbsAttachedFiles/adama.doc.
34 "The Fifth Assessment Report on Climate Change," IPCC – Intergovernmental Panel on Climate Change, 2014, http://www.ipcc.ch/activities/activities.shtml.
35 Report of the Information Center for Climate Change (report A, report B, and report of the local authorities), website of the Ministry of the Environment, www.sviva.gov.il.
36 IPCC – Intergovernmental Panel on Climate Change.
37 A. Salmon, "Map of the Regions Liable to be Flooded by a Tsunami along the Mediterranean Shores of Israel in Haifa Bay, the Dan Metropolitan Area, Ashdod, and Ashkelon," *Geological Survey of Israel*, September 2009.
38 Study day: "Tsunami on the Shores of Israel – Risks and Methods of Preparedness."
39 L. Vihul and M. N. Schmitt, "The Tallinn Manual on Cyber Warfare – A First Tool for Legal Practitioners," fifteen eightyfour, November 13, 2013, http://www.cambridgeblog.org/2013/11/the-tallinn-manual-on-cyber-warfare-a-first-tool-for-legal-practitioners-michael-schmitt-liis-vihul-nato/.
40 T. G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: John Wiley & Sons, 2006); G. N. Ericsson, "Cyber Security and Power System Communication: Essential Parts of a Smart Grid Infrastructure," *IEEE Transactions on Power Delivery* 25, no. 3 (2010): 1501-7.
41 G. Siboni, ed., *Cyberspace and National Security: Selected Articles* (Tel Aviv: Institute for National Security Studies, June 2013), http://www.inss.org.il/publication/cyberspace-and-national-security-selected-articles/?offset=6&posts=25&type=403.
42 Advancement of the National Capability in Cyber Space, Government Decision No. 3611, August 7, 2011, http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3611.aspx.
43 Adoption of the Recommendations of the Inter-ministerial Committee for Updating the National Program for the Development of the Negev in Light of the Implementation

of the Relocation of IDF Camps to the Negev, Government Decision No. 546, July 14, 2013, http://www.pmo.gov.il/Secretary/GovDecisions/2013/Pages/des546a.aspx.

44 Advancement of National Preparedness for Cyber Protection, Government Decision No. 2444, February 15, 2015, http://www.pmo.gov.il/Secretary/GovDecisions/2015/Pages/des2444.aspx.

45 Advancement of National Regulations and Government Leadership on Cyber Protection, Government Decision No. 2443, February 15, 2015, http://www.pmo.gov.il/Secretary/GovDecisions/2015/Pages/des2443.aspx

46 P. D. Allen and C. Demchak, "The Palestinian-Israeli Cyberwar," *Military Review* 83, no. 2 (2003): 52-59.

47 "Israel Electric Corporation Reveals Data about Cyber Activities Prior to the International Cyber Conference: Cybertech," Israel Electric Corporation, March 22, 2015, https://www.iec.co.il/spokesman/pages/220320151.aspx.

48 A. Teixeira, A. Saurabh, H. Sandberg, K.H. Johansson, and S.S. Shankar, "Cyber Security Analysis of State Estimators in Electric Power Systems," 49th IEEE Conference on Decisions and Control, December 15-17, 2010, pp. 5591-98, https://goo.gl/iZv532.

49 A. A. Cárdenas, A. Saurabh, L. Zong-Syun, H. Yu-Lun, H. Chi-Yen, and S. Shankar, "Attacks against Process Control Systems: Risk Assessment, Detection and Response," in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS, 2011, pp. 355-66.

50 D. Watts, "Security & Vulnerability in Electric Power Systems," 35th North American Power Symposium (NAPS 2003), University of Missouri-Rolla in Rolla, October 20-21, 2003, pp. 559-66.

51 G. Siboni, *The National Response for Civil Defense Against Cyber: Recommendations for Decision Makers*, position paper for the Institute for National Security Studies, August 2013.

52 EMP Commission 2004 Executive Report, as cited in A. Schnurr, "Vulnerability of National Power Grids to Electromagnetic Threats: Domestic and International Perspectives," *Energy Law Journal* 34, no. 1 (2013): 1-54.

53 V. Gurevich, "The Hazards of Electromagnetic Terrorism," *Public Utilities Fortnightly*, June 2005, http://www.fortnightly.com/fortnightly/2005/06/hazards-electromagnetic-terrorism.

54 Schnurr, "Vulnerability of National Power Grids to Electromagnetic Threats."

55 See the "Deployment of Electricity Generation Installations in Israel" on the website of the Ministry of National Infrastructures, http://energy.gov.il/Subjects/Electricity/Pages/GxmsMniElectricityProduction.aspx. See also the Israel Electric Corporation's report for 2012, https://www.iec.co.il/investors/DocLib1/isa_2012.pdf.

56 Statistical report of Israel Electric Corporation for 2010, https://www.iec.co.il/investors/DocLib/stat_2010.pdf.

57 "Preparedness for Emergencies," *Corporate Sustainability Report of the Israel Electric Corporation*, 2013, pp. 47-48, https://www.iec.co.il/Sustainability/Documents/annualReport2013HEB.pdf.

58 Y. Zeitun, "Before Iran? Tens of Millions for Protection of Infrastructure Installations," *Ynet*, July 31, 2012, http://www.ynet.co.il/articles/0,7340,L-4262517,00.html.

59 From Protocol No. 43 of the meeting of the Knesset State Control Committee, August 26, 2013.

60 U. Rubin, "The Active Defense of Israel During Operation Protective Edge," *Studies in the Security of the Middle East*, No. 111, Begin-Sadat Center for Strategic Studies, January 2015, http://besacenter.org/wp-content/uploads/2015/02/Hebrew-Booklet.pdf.

61 A. Harel, "GOC Home Front Command: Iron Dome for Protection of Power Stations and IAF Bases Prior to the Big Cities," March 29, 2013.

62 Nonetheless, the special report of the State Comptroller from 2011 on the subject of preparedness in Israel for earthquakes stated that: "In the decade that has elapsed since the date of publication of the report from 2001…a long period of time in which it was possible to achieve significant progress on the subject of preparedness for earthquakes, no significant improvement has occurred in this field, and no budget for preparedness has been fixed, not even spreading it over a few years in order to alleviate the economic burden of building reinforcements," in "Resistance of Buildings and Infrastructures to Earthquakes – Situation Assessment," State Comptroller's Report, March 23, 2011, http://www.mevaker.gov.il/he/Reports/Pages/116.aspx?AspxAutoDetectCookieSupport=1#.

63 The national reference scenario was formulated under the guidance of the National Steering Committee for Earthquakes and has been accepted by all relevant response bodies in Israel as the basis for assumptions regarding preparedness for earthquakes. In accordance with the reference scenario, in an earthquake of 7.5 on the Richter scale in the region of Beit She'an, there are expected to be about 16,000 fatalities, 6,000 seriously injured, 83,000 lightly injured, and about 377,000 evacuated from their homes. It is likewise expected that the casualties will be dispersed throughout most of the country. See "File of Questions and Answers for the Turning Point 6 Drill, Home Front Command, population department, September 2011," http://www.herzliya.muni.il/_Uploads/dbsAttachedFiles/earthquake-QA-sep2012.pdf.

64 *Earthquake Damage Scenarios in Israel as the Basis for Turning Point 6 National Emergency Drill*, Geological Survey of Israel Report No. GSI/21/2012, October 2012. The report does not specifically address damage to electrical installations.

65 See the website of the Home Front Command, http://www.oref.org.il/.

66 L. Gutman, "How will the State Cope with Earthquake Damage to Infrastructures from an Earthquake?" *Calcalist*, July 21, 2011, http://cordis.europa.eu/fp7/home_en.html.

67 Information regarding FP7 (Seventh Framework Programme for Research and Technological Development) from the website of the European Council, http://cordis.europa.eu/fp7/home_en.html.
68 Information regarding Horizon 2020 from the website of the European Council, http://ec.europa.eu/programmes/horizon2020/en.
69 "The Israel Electric Corporation reveals cyber activities data prior to the international cyber conference, Cybertech," Israel Electric Cooperation, March 22, 2015, https://www.iec.co.il/spokesman/pages/220320151.aspx.
70 Schnurr, "Vulnerability of National Power Grids to Electromagnetic Threats."
71 J. Kappenman, "A Perfect Storm of Planetary Proportions," *IEEE Spectrum*, January 24, 2012, http://spectrum.ieee.org/energy/the-smarter-grid/a-perfect-storm-of-planetary-proportions.
72 For example: GE, Power World Corp., Mitsubishi.
73 P. Pry, *Apocalypse Unknown: The Struggle to Protect America from an Electromagnetic Pulse* (CreateSpace Independent Publishing Platform, 2013).
74 *Protection of Infrastructures from Electromagnetic Pulses: Review of the Sensitivity of the Electrical Grid to Electromagnetic Pulse and the Derivatives from Electromagnetic Threats*, Ministry of National Infrastructures, Energy, and Water Resources, in cooperation with the Electric Infrastructure Security Council, EIS, 2013; not circulated to the public.
75 S. A. Boyer, *SCADA: Supervisory Control and Data Acquisition* (North Carolina: International Society of Automation, 2009), http://dl.acm.org/citation.cfm?id=1717879.
76 "EMP Commission 2004 Executive Report," as cited in J. Kappenman, *Low-Frequency Protection Concepts for the Electric Power Grid: Geomagnetically Induced Current (GIC) and E3 HEMP Mitigation (Meta-R-322)*, Metatech Corporation, January 2010, note 228, at 3-1, 3-4.
77 Pry, *Apocalypse Unknown*.
78 Ibid.
79 S. Masood, "Rebels Tied to Blackout across Most of Pakistan," *New York Times*, January 25, 2015, http://www.nytimes.com/2015/01/26/world/asia/widespread-blackout-in-pakistan-deals-another-blow-to-government.html?_r=0.
80 D. Melvin, "Power Outage Hits Much of Turkey; Officials Won't Rule Out Terrorism," *CNN*, March 31, 2015, http://www.cnn.com/2015/03/31/middleeast/turkey-power-outage/.
81 *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, Homeland Security, https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.
82 "Presidential Policy Directive – Critical Infrastructure Security and Resilience," The White House, February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

83 T. F. McLarty and T. G. Ridge, *Securing the U.S. Electrical Grid*, Center for the Study of the Presidency and Congress (CSPC), October 2014, https://www.thepresidency.org/sites/default/files/Final%20Grid%20Report_0.pdf.

84 *Federal Resource Guide for Infrastructure Planning and Design*, Build America Investment Initiative, May 2015, http://portal.hud.gov/hudportal/documents/huddoc?id=BAInfraResGuideMay2015.pdf.

85 S. E. Flynn, *Bolstering Critical Infrastructure Resilience After Superstorm Sandy: Lessons for New York and the Nation*, G. J. Kostas Research Institute for Homeland Security at Northeastern University, April 2015, https://globalresilience.northeastern.edu/resource/bolstering-critical-infrastructure-resilience-superstorm-sandy-lessons-new-york-nation/.

86 "Information of Community Resilience Planning Guide," National Institute of Standards and Technology, http://www.nist.gov/el/building_materials/resilience/guide.cfm.

87 State Comptroller's Annual Report No. 65(b), Jerusalem, December 2014, http://www.mevaker.gov.il/he/Reports/Report_270/ReportFiles/fullreport_2.pdf.

88 E.J. Fitch, "Delay, Deny, Delete and Destroy: American Conservatism and Environmental Protection," *Interdisciplinary Environmental Review* 7, no. 2 (2005): 34-42.

89 S.D. Smith, *Inter-Agency Collaboration and Consequence Management: An All-Hazard Approach to Emergency Incident Response*, Public Entity Risk Institute, 2003.

90 See the outstanding events since the beginning of the 21st century and the extent of their financial damage: Fukushima, Japan 2011 – $300 billion; earthquake in Sichuan, China, 2008 – $148 billion; oil leak in the Gulf of Mexico, 2010 – $60-100 billion; floods in Thailand, 2011 – $45 billion; earthquake in Christchurch, New Zealand, 2011 – $40 billion; the cumulative damage of the attack on September 11, 2001 on the US has reached almost $2 trillion. See Institute for the Analysis of Global Security at http://www.iags.org/costof911.html.

91 "Resilience in Society: Infrastructure, Communities and Businesses," Cabinet Office, February 20, 2013, https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses.

92 *Disaster Resilience: A National Imperative* (Washington, D.C.: National Academies Press, 2012), http://www.nap.edu/openbook.php?record_id=13457.

93 The many varied definitions and interpretations of the term "disaster" demonstrate its subjective nature. See E. L. Quarantelli, "What is Disaster? The Need for Clarification in Definition and Conceptualization," in *Disaster and Mental Health Selected Contemporary Perspectives*, ed. B. Sowder (Washington, D.C.: Government Printing Office, 1985), pp. 41-73.

94 C. S. Holling, "Resilience and Stability of Ecological Systems," *Annual Review of Ecology and Systematics* 4 (1973): 1-23.

95 P. E. Roege, Z.A. Collier, J. Mancillas, J. A McDonagh, and I. Linkov, "Metrics for Energy Resilience," *Energy Policy* 72 (2014): 249-56, http://www.sciencedirect.com/science/article/pii/S0301421514002237.

96 Government Decision No. 4450 (2009), http://www.pmo.gov.il/Secretary/GovDecisions/2009/Pages/des4450.aspx; Government Decision No. 3484 (2011). http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3484.aspx.

Authors and Contributors

Dan Weinstock served as the director of the Electricity Administration in the Ministry of National Infrastructures, Energy, and Water in the period 2005-2008. He received a BSc cum laude in electricity capacity systems from the Faculty of Electrical Engineering at the Technion in 1992. He completed his MSc in 1994, and his research thesis, under the supervision of Prof. Avraham Alexandrovitz and Dr. Adrian Zukerberger, dealt with matrix convertors. He was awarded a PhD by the Faculty of Engineering at Tel Aviv University in 2008 under the direction of Prof. Yosef Elbaum. The subject of his doctorate was the optimal design of solar fields. In 2014 Dr. Weinstock was awarded an additional MSc in natural gas and oil engineering by the Technion. His thesis was on the subject of natural gas for transportation.

Dr. Weinstock is a faculty member of the Holon Technological Institute's Faculty of Engineering and an external lecturer at the Azrieli Academic College for Engineering in Jerusalem and the Sammy Shimon Academic College for Engineering in Ashdod.

He served for some 10 years as a technical officer in the IAF in various positions in the field of electricity. He subsequently worked as an electrical engineer in the light railway project in the Greater Tel Aviv area and as chief electrical engineer in Better Place (company for electrical vehicles). He is currently a consultant in the energy sector in the following fields: renewable energy, natural gas, improved energy efficiency, smart grid, and electrical transportation.

Meir Elran is a senior research fellow at the Institute for National Security Studies (INSS), where he is head of the program for research on the home front and the program on socio-military relations.

Dr. Brig. Gen. (ret.) Meir Elran is a former senior officer in the intelligence branch of the IDF. He served in a variety of positions in the research division and as a staff officer (intelligence) of the Southern Command,

deputy commander of the National Security College, and deputy head of the intelligence branch. After leaving the IDF, he served as deputy CEO of Tel Aviv Municipality, director of the Brookdale Research Institute of the JDC, and a consultant for strategic planning in government ministries and in various government branches (among them, the Ministry of Defense, IDF, Israel Police, and National Security Council).

Dr. Elran holds a BA from the Hebrew University of Jerusalem in political science and Middle East studies and an MA in international relations and Russian studies from the University of Indiana. He completed his PhD at the University of Haifa in the political science department in the field of societal resilience. He teaches at the Inter-Disciplinary Center (IDC) in Herzliya.

Alex Altshuler is a research fellow at the Institute for National Security Studies and a postdoctoral researcher in the Fulbright program at the Kennedy School of Administration at Harvard University. His research focuses on preparedness for emergencies from the level of the individual, through the level of the organization and the community, and up to strategic preparedness at the national and international level. As part of his research he has developed a number of innovative research models relating to emergencies.

Dr. Altshuler has published 26 scientific papers and presented his research at 23 scientific and professional conferences.

Ehud Ganani is deputy CEO of the Electric Infrastructure Security (EIS) Council. He coordinates and develops EIS Council activities in Israel that aim to increase awareness and preparedness for a protracted blackout. He is a member of the Spectrum Group of consultants from Virginia that provides aid to companies engaged in security and transactions with the federal government.

During 2005-2012 Dr. Ganani served as CEO and chairman of a number of Israeli companies in the field of technology, development, and supply of security products including: Rabintex Industries, which engages in means for personal protection and protection of vehicles; Traceguard Technologies, which engages in the detection of explosives in airports and in border crossings; Bird Aerosystems, which engages in the protection of aircraft against missiles; and Defensoft, which engages in the design of protection systems for borders and installations.

In 2005-2011 he served as a member of the board of directors of Gilat Satellite Telecommunications and served voluntarily as the chairman of the Public Committee for Security and Homeland Protection in the Export Institute. In 2002-2005 he served as CEO of IMI. From 1974 until 2002 he worked at Rafael in a number of positions, including the representative in Washington (1991-1996) and VP for marketing and business development (1997-2002).

Dr. Ganani is a chemical engineer and has a BSc from the Technion and a PhD from Washington University, Saint Louis. He was a guest lecturer at the University of California, Davis.

Sinaia Netanyahu, who studied the economics of natural resources and agriculture, serves as chief scientist in the Ministry of the Environment. As part of the advancement of the Ministry's scientific activities, Dr. Netanyahu initiates and supports research and the development of knowledge about preparedness for climate change, the environment and health, environmental and water technologies, prevention of forest fires, oil alternatives for transportation, energy production, green construction, spatial planning, biological diversity, and many other subjects.

Eitan Parness is the founder and CEO of the Association of Green Energy Companies in Israel. He is an expert in policy and regulation in the field of green energy and the reduction of greenhouse gas emissions. He is a member of the Green Growth Round Table. During 2008-2014, he was a member of many official committees in the field of energy, planning, and policy in Israel. He is a member of groups of experts in renewable energy and increased energy efficiency in the economic organization of the UN for Europe (UNECE 2014) and was part of the Israeli delegation to the fourth conference of the international energy agency IRENA 2014. He is a member of the founding team of the World Council for Photovoltaic Solar Energy (GSPVA). He has extensive experience in the advancement of public processes in emergency management and lectures on the subject in a number of academic institutions and professional courses.

Eitan Parness is a founder and the Israeli chairman of the German-Israeli Renewable Energy Committee: AHK. He was awarded the title Man of the Year in the Global Cleantech Awards for 2012 and received the Brian Medved Award at the 2014 Eilat Eilot Green Energy Conference. He has served as

a member of the public management of the Israeli Society for Solar Energy (ISES), Melitz, and Friends of the Jerusalem Botanical Gardens. In 2015 he was elected secretary of the Global Solar Council.

He holds a BA and MA in law and is a graduate of Warwick University and of the Hebrew University of Jerusalem.

Amir Steiner was a member of the Institute for National Security Studies cyber security program in 2012. He has a BA in telecommunications from Sapir College. He trained in information security management (CISO), network managers (MCITP), and information security implementation (ISSI) at the See Security – Information Security & Cyber Warfare College.

Amir Steiner has researched the subject of the Dark Net and the world of virology, and published online articles, including "The Fine Distinction between Freedom and Privacy for the Misuse of Technology," and "Protection of the Financial Sector Against Cybernetic Fraud."

He served as a battery commander in the artillery corps with the rank of major.

Shai Toledano joined the Institute for National Security Studies in 2013 as an intern working on the project on the delegitimacy of Israel. He took part in interviews with senior persons and decision makers in the Israeli economy with the aim of mapping threats to the Israeli economy as a result of the threats of delegitimacy. He has a BA in economics and language studies from Oxford Brookes University, England where he served as vice president of the Foreign Students Union. He is a business development director at Forma-Tech Systems and is responsible for cooperation in the US and the Far East.

INSS Memoranda, December 2015–Present

No. 165, June 2017, Dan Weinstock and Meir Elran, *Securing the Electrical System in Israel: Proposing a Grand Strategy.*

No. 164, February 2017, Einav Yogev and Gallia Lindenstrauss, *The Delegitimization Phenomenon:Challenges and Responses* [Hebrew].

No. 163, February 2017, Nizan Feldman, *In the Shadow of Delegitimization: Israel's Sensitivity to Economic Sanctions*.

No. 162, November 2016, Yoel Guzansky, *Between Resilience and Revolution: The stability of the Gulf Monarchies* [Hebrew].

No.161, November 2016, Udi Dekel, Gabi Siboni, and Omer Einav, eds., *The Quiet Decade: In the Aftermath of the Second Lebanon War, 2006–2016* [Hebrew].

No. 160, November 2016, Pnina Sharvit Baruch, *The Report of the Human Rights Council Commission of Inquiry of the 2014 Operation in the Gaza Strip – A Critical Analysis* [Hebrew].

No. 159, September 2016, Meir Elran and Gabi Sheffer, eds., *Military Service in Israel: Challenges and Ramifications.*

No. 158, September 2016, Doron Matza, *Patterns of Resistance among Israel's Arab-Palestinian Minority: A Historical Review and a Look to the Future* [Hebrew].

No. 157, August 2016, Emily B. Landau and Anat Kurz, eds., *Arms Control and Strategic Stability in the Middle East and Europe* [Hebrew].

No. 156, August 2016, Udi Dekel, Nir Boms, and Ofir Winter, *Syria's New Map and New Actors: Challenges and Opportunities for Israel.*

No. 155, June 2016, Emily B. Landau and Anat Kurz, eds., *Arms Control and Strategic Stability in the Middle East and Europe.*

No. 154, June 2016, Nizan Feldman, *In the Shadow of Delegitimization: Israel's Sensitivity to Economic Sanctions* [Hebrew].

No. 153, March 2016, Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy*.

No. 152, March 2016, Dan Weinstock and Meir Elran, *Securing the Electrical System in Israel: Proposing a Grand Strategy* [Hebrew].

No. 151, December 2015, Udi Dekel, Nir Boms, and Ofir Winter, *Syria: New Map, New Actors – Challenges and Opportunities for Israel* [Hebrew].

Many countries in the West, including Israel, have realized that their national security depends in part on the resilience of the home front. This resilience relies largely on the reasonable and continuous functioning of the various systems that serve it, first and foremost the orderly provision of the basic products of critical national infrastructures. The electrical system has a major place among these infrastructures because of the potential risk of a protracted blackout over large parts of the country and the paralysis of vital national systems.

Securing the Electrical System in Israel: Proposing a Grand Strategy examines the major external threats facing Israel's electrical system and the current responses to these threats. It offers an assessment of the Israeli situation and looks at tools that have been implemented abroad, particularly in the United States, that might be useful models for Israel. This analysis provides a basis for recommendations regarding what should be done in order to improve the preparedness of the electrical system to cope with significant risks to Israeli national security. The study contends that the security of the electrical system ultimately depends on a comprehensive strategy – which does not currently exist in Israel – that will ensure the secure supply of cheap and available energy to meet Israel's civilian and military needs.

Dan Weinstock served as the director of the Electricity Administration in the Ministry of National Infrastructures, Energy, and Water in the period 2005-2008. Dr. Weinstock is currently a consultant in the energy sector in numerous fields, including renewable energy, natural gas, improved energy efficiency, smart grid, and electrical transportation.

Meir Elran, a senior research fellow at INSS, heads the INSS program on Israel's civilian front and the program on socio-military relations. A former senior officer in the IDF Intelligence Corps, Dr. Elran served as a consultant for strategic planning in government ministries and in various government branches, among them, the Ministry of Defense, IDF, Israel Police, and National Security Council.

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב