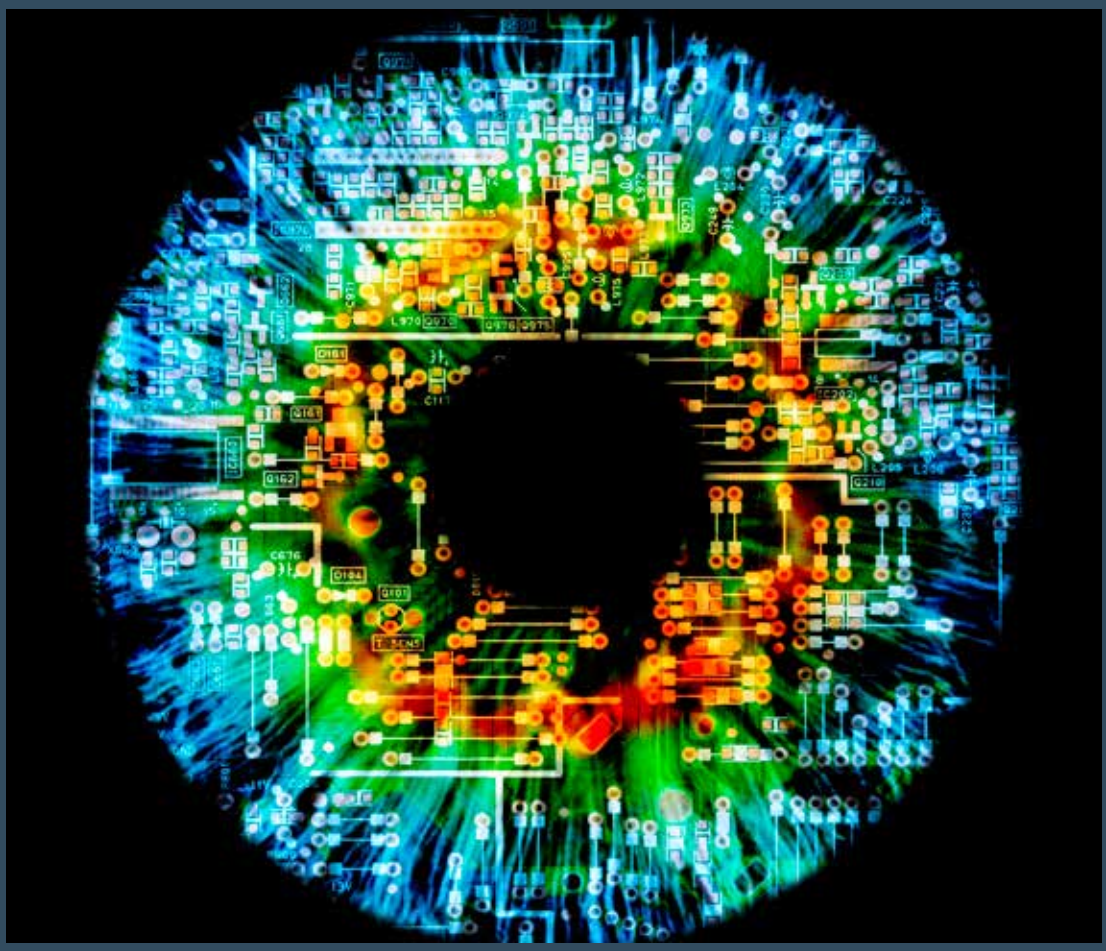

Guidelines for a National Cyber Strategy

Gabi Siboni and Ofer Assaf

Memorandum
153

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

Guidelines for a National Cyber Strategy

Gabi Siboni and Ofer Assaf

Guidelines for a National Cyber Strategy

Gabi Siboni and Ofer Assaf

Memorandum No. 153 March 2016

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

קווים מנחים לאסטרטגיה לאומית במרחב הסייבר

גבי סיבוני ועופר אסף

Editor: Ela Greenberg
Graphic design: Michal Semo-Kovetz, Yael Bieber
Cover photo: Science Photo Library / Getty Images
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

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

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

March 2016

ISBN: 978-965-7425-90-9

Table of Contents

Acknowledgments 7

Executive Summary 9

Introduction 15

The Cyber Challenge 19

Literature Review 23

Planning and Strategy 23

Israel 23

Force Build-Up 24

United States 25

United Kingdom 30

France 31

China 32

International Organizations (OECD, ENISA, European Union) 33

Defense and Deterrence 34

Facing Hardware Threats 36

Deterrence 36

Attack 37

Attack as Part of Overt Conflict 38

Cyber Attack as Part of the Operative Battle Plan 39

Defense 43

Response to Advanced Persistent Threat (APT) Attacks 44

Response to Rapid, Superficial Attacks (DDoS, Defacing) 49

Use of the "Cloud" by Security and Other Essential Organizations 50

Response to Hardware and Firmware Attacks 51

Preventing Attack through Deterrence 53

Recovery from Attack 54

Complementary Defense Issues 57

Culture of Cooperation and Transparency in Organizational Structure 57
Regulation in National Cyberspace 63
Professionalism of Employees and Responsibility of Business Managers 64
Summary 66

Attack 69
Overt and Hazy Cyberattacks 70
Attack as a Means of Delivering a Message 72
Attack as Part of a Covert Campaign 73
Summary 74

Insights and Recommendations 77
Main Recommendations 78
Recommendations for Defense 78
The Attack Field 79
The Organizational Field 79

Conclusion 83

Appendix: Glossary of Terms 87

Notes 91

List of Figures

Figure 1: Division of National Cyberspace According to Motivation for Activity 16
Figure 2: Boundaries of the Policy and Strategy Papers on a National Level 19
Figure 3: Concept for Handling APT Attacks 45
Figure 4: Defense Chain vs. Attack Chain 47
Figure 5: Visualization of Risk Management Process 55
Figure 6: Recovery from Attack as an Integral Part of Defense 56
Figure 7: Regulatory Status of Organizations in Israel 60
Figure 8: Proposed Responsibility for Operation in Cyberspace 62

Acknowledgments

First and foremost, we would like to thank Major General (ret.) Amos Yadlin, director of the Institute for National Security Studies, for his valuable and incisive comments. We would also like to thank all those who enlightened us with constructive criticism throughout the process of writing and review: Brigadier General (res.) Udi Dekel – deputy director of the Institute, Dr. Shmuel Even, Dudi Siman-Tov, Dr. Gallia Lindenstrauss, and Yoram Hacohen.

We thank Deborah Housen-Couriel for clarifying the breadth and analytical complexity of the cyber legal issue (which led us to conclude that we must dedicate a separate study and position paper to this issue); Corinne Berger, Simon Tsipis, and Yoel Kozak of INSS, who assisted in the collection of material.

We also express our sincere thanks to Moshe Grundman and Dr. Judith Rosen for their comments and work in publication of this memo, and we extend special thanks to Dr. Anat Kurz, director of research at INSS, for her extensive patience and valuable, informative advice throughout the process.

We would also like to thank those who helped us to comprehend the complex technological issue – Avi Shavit of the Office of the Chief Scientist, who referred us to relevant and fascinating industries, and the industry experts who hosted us and demonstrated their technologies: Gonen Fink and the staff of LightCyber Ltd., Nir Gaist and the staff of Nyotron Information Security Ltd., Ron Davidson of Check Point Software Technologies Ltd., Itzik Vager of Verint Systems Inc., the late Benny Rosenbaum of BioCatch Ltd., Elad Horn of enSilo Ltd., and Shimon Becker of CyberObserver Ltd. We also thank Major General (ret.) Prof. Isaac Ben-Israel for his scholarly comments.

Executive Summary

In the past few years, activity in cyberspace in the State of Israel has developed at a rapid and intense pace. In 2002, the government of Israel addressed this challenge by establishing the National Information Security Authority. Since then, Israel's functional continuity has become increasingly dependent on technology in general, as have other countries worldwide, and on cyberspace activity in particular. As a consequence of this dependence, the threats to Israel's functional continuity have intensified. Numerous states and enemies are systematically developing capabilities and acting against various systems and elements in Israel.

Several years ago, the Israeli government established the National Cyber Bureau to promote and regulate activity in cyberspace. The establishment of a National Cyber Defense Authority represents another step in this direction. In parallel, Israel must work to consolidate and outline a national strategy for activity in cyberspace, which will serve as the cornerstone of national growth in cyberspace. The document outlining the national strategy should be one of several documents. The primary document should be the national policy framework for cyberspace activity, which will define the overall national goals in the field of cyber activity and the methods for integrating them in the defense, economy, and other national efforts. Finally, each state entity operating in this space will be required to formulate its own organizational strategy for cyber activity.

Activity in cyberspace includes a number of components: one is defense, which is a fundamental element. The following entities in Israel require defense: institutions responsible for state security; institutions supplying essential services, and those responsible for administrative procedures and everyday life; and the institutions for which an attack would influence morale and the general sense of order, governance, and sovereignty. The sources of the cyber threat are multiple, and include hostile states, enemy states, terror organizations, hacktivists, and even private individuals. In parallel, the

State of Israel is also exposed to criminal activity in cyberspace, including business espionage and intellectual property theft, financial crime, and other types of crime that take advantage of the cybernetic space (drug dealing, pedophilia, arms dealing, and so forth).

In addition to the defense component, Israel also must address the offensive component on a national level. Naturally, the ability to cover these components in this paper is extremely limited. Rather, the goal of this document is to propose guidelines for formulating a national cyber strategy in the field of defense and offense. These guidelines do not encompass all aspects of the field; they do not relate to the legal features nor to issues relating to Israel's cyber industry.

The primary objective of a national cyber defense strategy is to maintain the state's functional continuity. A second goal is to enable the relevant Israeli authorities to decide upon and implement operations against enemies in the cybernetic and kinetic space, with confidence in the state's ability to withstand a cyberattack. In the defense strategy, we propose to differentiate between three types of attacks: 1) advanced persistent threat (APT) – penetration into the depth of an organization's computer system; 2) rapid, superficial attack, which has immediately recognizable results, and aims to change the site or prevent access to it and to the services it provides in the cybernetic space (Defacing, DDoS); 3) infrastructure attack – by damaging hardware components.

We suggest the following recommendations for preventing and defending against the three types of attacks:

1. Construct the system with a combination of tools and capabilities that do not require previous information and knowledge of attack components and methods, with an advanced capabilities system based on previous knowledge, specifically for defense against APT attacks.
2. Implement inter-organizational information exchange of reports on attacks.
3. Formulate a continuous and broad national cybernetic status assessment by organizations such as a national Computer Emergency Response Team (CERT).
4. Establish rapid response teams, using research and data on attack tools and attack groups.
5. Cooperate with commercial defense and intelligence organizations, as well as international bodies.

6. Develop ongoing intelligence collection about enemies and opponents for the purpose of warning.
7. Formulate a plan for cybernetic response as part of a possible means of deterrence.
8. Develop the ability to recover from an attack when possible, with the understanding that the line of defense is bound to be breached, and thus Israel must organize for rapid recovery following successful enemy attacks.
9. For superficial attacks – establish the ability to recover rapidly and provide the bandwidth that overcomes blocks, by integrating with internet suppliers in the civilian sector.
10. Use ability to rapidly transfer attacked sites to alternative, temporary host sites.
11. Establish a national capability for analyzing hardware attacks due to the technological difficulty of identifying hardware attacks. This should be done in parallel to the use of locally manufactured hardware in cases requiring an exceptional level of security.

We analyzed additional issues in the chapter on defense. The need to develop a national capability to recover from a cyberattack is critical, in the understanding that the "line of defense is bound to be breached" as a determined enemy will succeed in penetrating any defense, no matter how sophisticated. Therefore, Israel will need to construct appropriate mechanisms for recovery and return to routine as soon as possible. In addition, we examined the organizational issue, through an understanding that the State of Israel should be able to provide a response, both for the security sector and for civilian sector. The security organizations must continue to manage the cyber defense of the state's security sector, while cyber activity targeting the civilian sector will be handled by Israel's law enforcement bodies, headed by the Israel Police. The National Cyber Defense Authority will demand cooperation and synchronization between all entities and monitor the existence and enforcement of regulation in the civil arena, which is most exposed to cyberattacks. In this context, we recommend adopting a regulatory approach in the civil sector that will mandate the cyber defense field as a component integrated within existing statutory processes, both in the founding stages for business initiatives (licenses from the various statutory planning committees) and in their operational process (business licensing law). We suggest that in this framework, businesses should be required to issue a cyber resilience report. This document will serve as

the main statutory tool for identifying and analyzing the vulnerability of a business to a cyberattack, and for formulating processes of defense of these vulnerable points.

This document also relates briefly to cyberattacks and examines several attack scenarios, including attack in overt and obscure situations; attack as a method of communicating a message; and attack as part of a covert campaign. The main recommendations in this context are as follows:

1. Israel's security organizations should be required to integrate tools for cyberattacks in their operative plans and in the actual use of force in battle, in both emergency and routine situations.
2. Cyberattack should not stand alone. It must be part of a general plan in order to wield influence in a comprehensive, overt conflict.
3. An effective attack is not necessarily a sophisticated APT attack. We recommend to fully utilize the ability to implement an effective cyberattack on a specific target through superficial, rapid, broad attacks on targets, even if these are not so-called "gold targets" (military targets, national infrastructure).
4. An effective cyberattack can be implemented through proxies, without the need to take responsibility.
5. A significant cyberattack requires build-up of force, knowledge of the target, and advanced planning.
6. A cyberattack can represent a stage in "dialogue" between countries, when the goal of the attack is to communicate a message.
7. Attackers should be integrated within Israel's central cyber defense system, as part of the regular planning and operation of the defense system.

In conclusion, this document recommends leveraging the informality of Israeli culture. Israeli society enjoys inherent characteristics of broad personal connections through social networking, a casual manner of interaction, desire to help others, willingness to participate in activities of a national and patriotic nature, and a need to be "at the center of things" and to prove personal and professional relevance. These attributes enable recruitment of many individuals when needed, whether to assist friends or for a national goal, and all the more so in cases that combine these two motives. This type of informal activity is constant and occurs in a high percentage of cases that require it. Because it is voluntary, based on good will, and reinforced by Israeli culture, it is more intense and sometimes of even higher quality than cooperation due to structured, legal, or regulatory obligation. This type of

activity can make a significant contribution to cyber defense in Israel, and should be utilized.

Finally, a substantial part of the strategy document should remain open to the public. Such a document should also include sections for classified issues that should remain undisclosed and that will assist in coordination and synchronization of the defense organizations operating in Israel, as far as this is possible. Formulating the document is an important and achievable challenge that can determine Israel's status as a global leader in the cyber field.

Introduction

Given the growing use of cyberspace in promoting the interests of states and organizations, and the fact that Israel, a nation with developed technology, is very active in cyberspace, a number of guidelines for "a strategy for Israel's activity in cyberspace" should be discussed.[1] This document does not offer a comprehensive discussion of all the recommended guidelines for creating a national cyber strategy; rather, it focuses on guidelines needing clarification, given the increase in more varied cyberattacks, the greater awareness of the issue of cyber defense, and accelerated and creative technological development.

In this document, the term "cyberspace" follows the Israeli government's current definition as "the physical and non-physical area created or comprised from part or all of the following elements: mechanized computer systems, computer and communications networks, software, computerized data, content transferred by computer, traffic and control data, and the users of all of the above."[2] Cyberspace is one of five spheres of activity, the others being land, sea, air, and outer space. Although cyberspace is virtual and created by human beings, in many ways, it is the continuation of the kinetic world.[3] Cyberspace is thus another sphere in which Israel acts in order to ensure its goals of national and individual security, economic growth, and welfare for all its citizens.[4] Achievement of these goals requires efficient defense of Israel's citizens, organizations, and institutions in cyberspace, and educated use of this space.

In the context of national defense in cyberspace, the primary objective is to preserve the state's functional continuity. In order to implement this goal, determining the objects of defense is fundamental and must be regularly updated as cyber threats develop. Cyber threats can be divided into security and criminal threats, while the main difference between the two is the motivation to harm. The former is motivated by politics or security, while

the latter has criminal intentions, such as monetary profit, extortion by threat, theft, and fraud. These two types of threats are described in detail below:

a. Security – threats whose primary motivation is political and defense-related. This group includes enemy states and hostile organizations such as Iran, Hezbollah, and Hamas; rival states likely to act against Israel's security include China and Russia; and organizations, groups, and individuals with a political agenda such as Anonymous, various hacker groups, and individuals acting independently against Israel.
b. Criminal – this includes cyberattacks by criminal organizations and individuals for the purpose of financial fraud; theft and business and personal espionage by companies, private investigators acting illegally, and embittered employees who attempt to harm their employers for various reasons.

Figure 1 illustrates this division of cyberspace, including the existence of a mixed space in which threats are carried out with consequences for cyberspace relating to the state's national and civilian sectors.

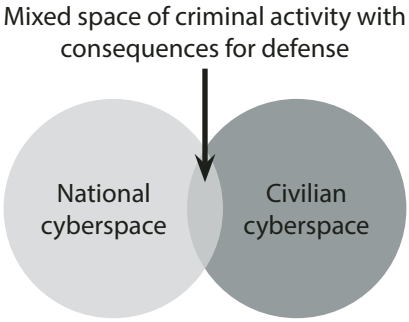

Figure 1: Division of National Cyberspace According to Motivation for Activity

The guidelines for defense offer a variety of operational concepts and tools that can serve both the cyberspace relating to the state's national government sector as well as the civilian sector, where entities addressing these spheres have their own unique attributes as part of its operational concept, and enable cooperation in cases where the threat crosses between spheres. In addition, the demarcation described in Figure 1 relates only to the sphere of threats. The operational sphere for cyber activity in the national sector encompasses the entire economy, including financial corporations and institutions, education, health, research and development, academic

institutions, and other areas. Organizations in these fields can also make use of some of the guidelines provided in this document.

A process of three stages can be defined – defining targets, strategic planning, and translating into tactics, so that defining targets influences the definition of the strategy, which in theory influences the choice of tactics to implement. In reality, the connections between levels are parallel and bidirectional, and the activity in each layer continuously influences the others. In this document, the examination of guidelines for national strategy has been carried out using this process, drawing from tactics in order to formulate realistic guidelines with a possibility for implementation. Addressing the more practical aspect of the guidelines represents a challenge, because activity in cyberspace is volatile, constantly updated, and forms new realities in the cyber world. In such a situation, deviating from the general, overall statements may lead to irrelevance, or the need for updates within a short time. Yet given the apparently real need, more concrete recommendations are offered herein.

In general, a strategy for cyberspace activity needs to be seen as an integral component of the state's engagement in the cybernetic field. In this framework, a process of force build-up for cyberspace must take place, and should include five key elements. The first element is formulating a strategy and doctrine for conduct in cyberspace. The second element is developing technology that supports achieving the goals and directions of the activity, as defined by the strategy. The third element relates to developing the human resources for the operation of the technological tools. The fourth complements the others, and relates to organizing personnel in relevant operational frameworks, based on relative advantages in operation. Finally, the fifth element addresses inculcation through drills and training exercises, with an emphasis on building operative programs and practicing them in reality.

This document is intended to assist in formulating the first key element in the force build-up (strategy and doctrine for activity in cyberspace), with the aim of targeting the national cyberspace activity. The national strategy should be an integral part of a hierarchy of binding documents, which together form an all-encompassing record of national policy for activity in cyberspace, and will define the overall goals of the state and method of integrating them in the national security and economy. The strategies for cyberspace activity that relate to all aspects of force build-up should be taken

from this document. Every relevant entity will be required to formulate its own internal strategy for action in cyberspace. A description of the proposed hierarchy of documents is given in Figure 2.

This document proposes guidelines for formulating Israel's national strategy for cyberspace, with the aim of assisting those individuals who bear the authority and responsibility for formulating and writing the document. In addition, as Figure 2 demonstrates, elements of this document can aid the relevant entities in formulating their own organizational strategy for cyberspace activity, and support other government and civilian sectors in attempting to regulate their cyberspace activity. The document, however, does not present a comprehensive strategy for Israel's cyberspace activity. There are other documents relating to various aspects of the strategy Israel must adopt when it chooses its path in the cyberspace arena.[5] Israel and other countries are engaging in a broad dialogue about the strategy for conduct in cyberspace, taking into consideration the characteristics of the cyberspace era, and the need to coordinate terms, laws, and professional and legal definitions, and for response and enforcement in the current era. Much has been written about the cyber age and the world of computers. Therefore, this paper will not reformulate the accurate and well-known statements of all those who work in the cyber field.[6]

General activity in the cyber field has expanded and intensified in recent years across all spheres, levels, and directions. It includes defensive and offensive activities, both governmental and non-governmental, motivated by national policy, ideology, technological challenge, crime or terror – both overt and covert – and information gathering or causing harm. This intensity enables study of policy and strategy that other states have adopted in relation to cyber activity. The proposals herein are based on the discussions primarily in the United States about cyber activity as described in numerous publications;[7] findings published about investigations of incidents by cyber intelligence and security companies;[8] technologies that are marketed in response to the needs of activity in cyberspace; and ideas suggested at conferences and meetings on the cyber issue.

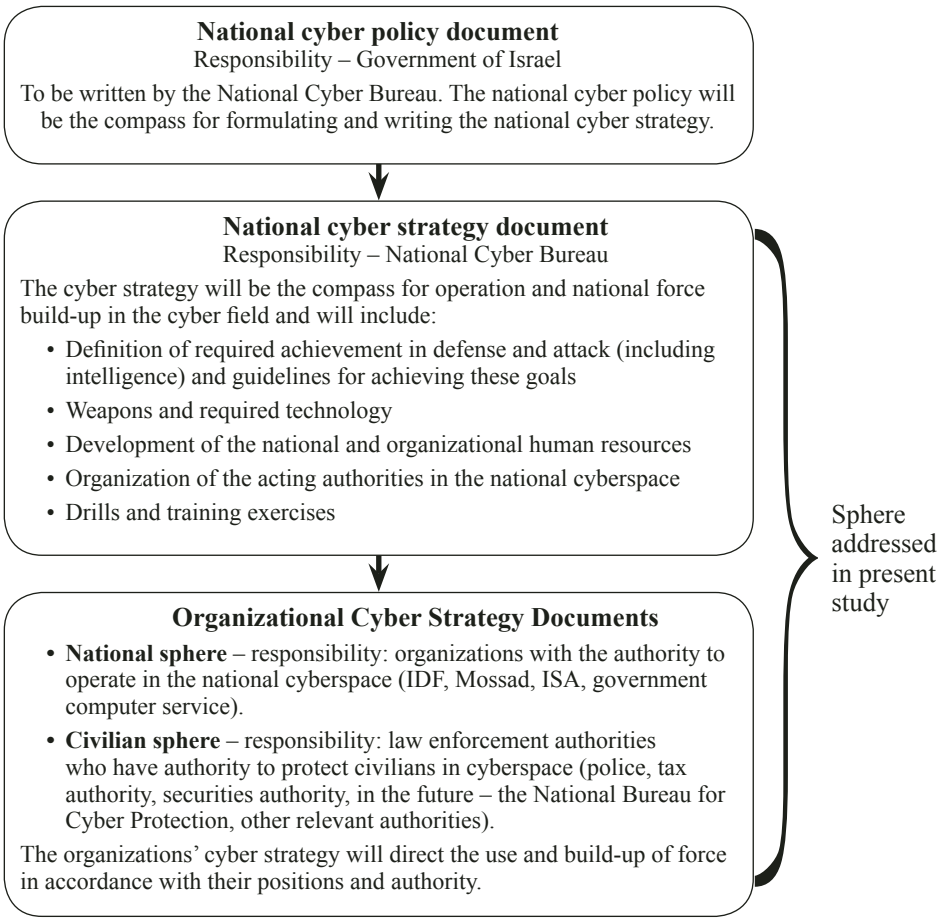

Figure 2: Boundaries of the Policy and Strategy Papers on a National Level

The Cyber Challenge

> *The essence of strategy is choosing to perform activities differently than rivals do.*
>
> Michael Porter[9]

Although Porter made this statement in the context of determining strategy for a business facing competition, it is relevant to formulating a national cyber strategy – defense against attacks. This is the main strategic challenge, with the overall goal being preservation of operational continuity on a national level.

Defense in cyberspace is a challenge for several reasons. First, the assailant has an advantage, which is amplified in cyberspace. At the core of this

advantage is the initiative, making absolute, hermetic defense impossible, and attack always possible. Second, an efficient and proven ability to defend against an attack based on unknown tools has yet to be implemented. As a result, continuous attempts are made to improve the existing methods and tools of defense. These improvements are useful, but they do not change the pattern of behavior between attacker and defender, and therefore do not offer a satisfactory solution. Third, solutions in the kinetic world for situations in which defense is not hermetic, such as "warning" and "balance of forces," have yet to be proven valid in cyberspace. The fact that an efficient defense method against a cyberattack has not been proven has created a reality in which cyber conflict is asymmetric in many dimensions. Symmetry does not exist between assailant and defender, between the required investment in defense and in the attack, and between a state with a strong technological infrastructure and a state without.

The discussion of formulating strategy also addresses attack in cyberspace. Naturally, discussion of a state's offensive capabilities is not open to public dialogue, due to the state's need to preserve technological advantages over time, and mainly because states tend to deny responsibility for attacks they carry out. Due to the lack of publications on the state's offensive strategies, treatment of the issue will be limited.

Recently, public dialogue in Israel and abroad has addressed two other significant issues. The first relates to the right to privacy in cyberspace. Due to the need to obtain information on cyber activity, mostly for defense purposes, information must be transferred to the government supervisory authorities responsible for national defense. Transferring extensive information to government authorities about citizens' activity in cyberspace raises questions such as which government organizations should be permitted to view this data and what use can be made of it. As these questions are subject to public and/or legal debate, we will not examine or address them here.[10] A second issue is possible harm to uninvolved civilians in a cyberattack, mainly due to the unified infrastructure and the connection between civilian networks and networks that are legitimate targets. This issue is not unique to the cyber sphere and is relevant in the context of physical battle in densely populated areas. Also worthy of public and/or legal discussion, this document will refrain from addressing this issue as well.

In order to analyze the strategic challenge and to create a "shared language," several questions can be raised: what are the threats and types of cyberattacks?

What are the objects of defense in Israel for which the defense strategy is formulated? Who are the enemies against which Israel must defend itself?

Cyberattacks – We can define three types of cyberattacks, differentiated by target and, consequentially, by design and tools:

1. Computer network attack (CNA): this attack aims to damage a computer/network and prevent continuation of normal operation. The damage includes stoppage for a limited amount of time, such as denial of service or defacing of site, and even deletion of data, halting operation of the computer, and paralyzing computer-supported processes in the organization under attack through an advanced persistent threat – APT.[11]
2. Computer network exploitation (CNE): this attack aims to collect data and/or spy. The data can be technological – about the structure of the network and the computers – for later perpetrating a CNA attack; data collection for the purpose of future active use (such as collection of credit card data or identity data of email users); or collection of content information (theft of commercial information, research and development or military and state secrets).
3. Computer network influence (CNI): this attack is designed to create a feeling of insecurity, lack of control, harm to sovereignty, and lack of ability to protect the normative way of life. Such attacks are generally limited in time, and do not cause real damage.

Israel's enemies – defining adversaries is a significant part of the process of force build-up and preparation of appropriate defense plans. In the field of cyberspace, adversaries may be defined in a broad manner, and defense abilities and plans may be based on other parameters. An adversary is anyone who carries out any kind of hostile activity against Israel in cyberspace for any reason. These are, of course, known and declared enemies such as Iran, Syria, Hezbollah, and Hamas, but may also include states attempting to engage in adversarial activity for a specific goal, such as espionage or theft of technological secrets, as well as organizations within states that have a specific interest in such activity.

The objects of defense in Israel – the objects of defense in Israel can be divided as follows:[12]

1. State security – all bodies dealing with state security, for which a cyberspace attack would damage state security, such as the foreign ministry, the defense ministry, the security organizations themselves, or parts of them, and all related organizations.

2. Essential services – a cyberattack (usually CNA) would halt these services and paralyze the state, causing extensive economic loss by affecting the monetary system, trade, and industrial production, and even endangering lives, by affecting food supplies, transportation, water, energy, and health services.
3. Government stability and daily life – a cyberattack would be disruptive, but not paralyze or endanger lives in the following: education; academia; research and development; justice; databases such as the population registry, ownership registry, land registry, patent registry; as well as various types of commercial businesses, and non-essential national and local government services.
4. Morale and authority – occasional damage to websites of government bodies; dissemination of damaging messages to civilians; interruption of communication sites for limited time periods; and any activity that creates an image of damage to governability, stability, and orderliness of the state.

Literature Review

In the framework of this research, a variety of sources were studied, including formal documents, articles, and statements of relevant organizations. Naturally, such a study is incomplete, and many sources were not surveyed. Alongside a survey of government publications, we also examined literature and research on these issues in Western democratic states, primarily the United States. The views of England and France are based on formal documents, while our analysis on China is based on research carried out by the Institute for National Security Studies. In addition, we examined documents of international organizations such as OECD, ENISA, and the European Union. The learning process also included surveying available publications and sources on the topics of defensive and offensive attacks.

Planning and Strategy

Israel

The government of Israel has not published a formal document detailing the state's strategy for activity in cyberspace. A government decision reveals the general direction and vision on this issue, mainly addressing the division of responsibility among the various bodies in Israel.[13] This decision is based on recommendations from the paper prepared in 2010-2011 by the Council for Research and Development under the direction of Isaac Ben-Israel. The Council's study was comprehensive, and its goal was "to present a working plan for a national initiative for facing the cyber threat, with emphasis on the response to security needs as well as the public and civilian systems."[14] The Council indicated the need to formulate a defense strategy for Israel's cyber field, and specified that the strategy should address defense of the State of Israel's national and civilian sectors in cyberspace. As part of this study, twelve recommendations were formulated, and the following recommendations were described in detail: establishment of the cyberspace bureau; broadening the authority of the Israel Security Agency (Shabak) or the Data Protection Authority as the body responsible for the civilian sector;

implementing a number of actions for policy and legislation to encourage the cyber industry, research and development in the cyber field and super-computing, as well as the establishment of a national center in the field of super-computing.[15] The Israeli government accepted the recommendations of the Council for Research and Development and charged the National Cyber Bureau with implementation. The Bureau has yet to publish a complete strategic approach regarding Israel's conduct in cyberspace. Since then, the only significant step taken has been another government decision to name the National Cyber Bureau as responsible for establishing a cyber authority that will be entrusted with defense of the civilian sector.[16]

The relative newness of the cyber field and the need for explanation and conceptualization, as well as the absence of a formal document that analyzes Israel's cyberspace strategy, has produced several papers relevant to the issue of strategy. In June 2011, Shmuel Even and David Siman-Tov published a memo on behalf of the Institute for National Security Studies that addressed the cyber issue in a comprehensive manner.[17] Even and Siman-Tov define the goal of Israel's strategy as securing Israeli cyberspace.[18] In their view, the aim of cyber defense is to preserve Israel's interests, and the method for achieving this aim is by formulating priorities in all fields related to objects of defense, and constructing a dynamic, integrative, and comprehensive defense system. Such a system will be based on integrating passive and active defense systems, integrating defense of essential targets and "territorial defense" components (traffic into the state, communications junctions), improving network architecture, and strengthening connections between physical and cyber defense mechanisms. Even and Siman-Tov base all activity on cooperative relationships between the government sector (defense and civilian) and the private sector, including sharing information and abilities, as well as close cooperation with foreign officials.

Force Build-Up

An essential component in formulating Israel's strategy in cyberspace relates to forming a methodical concept of force build-up.[19] Siboni analyzes the process of national force build-up in the cyber field as a product of many years of planning for strengthening in a methodical, directed manner. This process includes a number of fundamental elements, the first of which is formulating a strategy and theory of action for the entire process. The four additional components are investing in human resources and human

capital; developing technological tools; organizing personnel and tools in appropriate frameworks; holding training sessions, drills, and exercises in order to ensure that all systems function properly; and to improve and expand knowledge. In addition to formulating national strategy, Siboni proposes to relate to the implementation of forces of defense, intelligence, and attack in cyberspace. Operational theory in cyberspace must also relate to the national response in ordinary times, in emergency situations, and in the states where it is relevant – as well as in wartime – in order to properly define the ways in which the state must function not only during routine attacks, but also during wide-ranging cyberattacks carried out separately or in conjunction with physical attacks.

In addition, investment in human resources and human capital as well as development of technological tools and methods should be integrated and synchronized in a manner that utilizes the entire range of national resources in order to fortify the state's cyber defense ability. The existing technological and human resource systems should support the state's national targets, as will investing in technology as well as human capital in schools and academia. The organizational component relates to the responsibility and operational authority of individuals and means needed for implementing the national cyberspace strategy. For example, in Israel, defense organizations develop the ability to operate in cyberspace in order to support their basic objectives. Finally, an organized system of people and technological tools requires development of operative techniques, training modules, drills, and exercises, representing the pinnacle of the force build-up process. The security organizations hold regular training sessions, drills, and exercises. This field should be expanded to the civil sector, which is most exposed to damage in cyberspace, and efforts should be integrated with other organizations so that the national potential is maximized to its fullest extent.

United States

In recent years, the United States has worked intensively to formulate a strategy for cyberspace activity. The US Department of Defense views cyberspace as redefining the term "national security," because of its decisive influence on the ability of the Department of Defense to realize American objectives, both for defense and offense. In July 2011, the Department of Defense published an analysis of its basic strategy for action in cyberspace.[20] A description of the five principles of strategy is at the core of this analysis.[21]

They are as follows: (1) Cyberspace as a field of operation that requires organization, training, and equipment, enabling the Department of Defense to maximize its potential; (2) The adoption of a new operational defense concept with the goal of protecting its networks and system (3) Necessary cooperation with other government offices, agencies, and the private sector in order to implement a comprehensive, unified government cyber strategy; (4) Formation of a robust network of relationships with international allies and partners, to strengthen data collection for cyber defense purposes; and (5) Leveraging of the nation's creative ability through exceptional human resources and rapid technological advancements.

Two doctrinal documents define the work of the US military in cyber space. The first is the Joint Publication 3-12, Cyberspace Operations, which defines cyberspace and the objectives of the US military for operation in and/or through cyberspace in order to achieve its goals.[22] The second document defines information tactics in the US military. Here, the military once again relates to definitions of cyberspace operations – indicating that cyberspace occupies a significant position in information tactics – and to definitions of information defense, and thus creates a connection between implementing operations in cyberspace and protecting the information itself.[23] These two documents, written in a distinct military style, represent translation of the strategy and general directives of the US Ministry of Defense, and include the use of cyberspace for attacking targets in order to achieve the goals of the US military.

In a speech delivered on October 30, 2013, Keith Alexander, first commander of the United States Cyber Command and former director of the National Security Agency (NSA), summarized the cyber command strategy.[24] He listed the five principles underlying the strategy of the cyber command under his direction:

1. A force should be trained and ready for intervention during a cyberattack on an important entity. Alexander illustrated the need for such a force by describing a potential attack on the Wall Street stock market, using multiple DDoS attacks, similar to the attack on the Saudi company Aramco, which targeted some 30,000 computers. Alexander used this imaginary, but conceivable scenario in his speeches in order to explain to his listeners and convince them of the severity of the threat and of the fundamental need to implement the strategy formulated by the Cyber Command.

2. Clear division of authority and agreed command and control should be implemented. Alexander divides this job as follows: the FBI is responsible inside the borders of the United States, while areas outside the borders of the United States are the responsibility of the NSA and the Cyber Command, including intelligence cooperation with allies.
3. An architecture of networks at the Department of Defense, which is defensible, should be created rather than the present structure of 15,000 networks.
4. Intelligence evaluation in cyberspace should be shared both among government agencies and between government and the private sector. This cooperation must be based on legislation and take place between all government organizations working on cyber defense (Cyber Command, Homeland Security Department, NSA, FBI, and so forth) and private civilian organizations such as internet service providers. Alexander makes two important points – the issue of cooperation between the government and private sectors, and the regulation by law of transfer of information between sectors in the post-Snowden era.[25]
5. Division of authority: everyone operates under the direction of the president and according to the policy of the Department of Defense, but basic operational authority must be determined, so that action can take place.

Alexander's speech reflects the Department of Defense's interpretation of strategy as it is practically implemented. Ironically, the Department of Defense primarily has to deal with organizations that are not permitted to operate inside the United States, and which constitute the main threat. Alexander attempts to solve this anomaly by the method of transferring relevant data to organizations outside the FBI for defense purposes.[26]

One means of checking strategy is to understand the vision of those responsible for conduct in cyberspace. Speaking at a cyber seminar, Michael Rogers, Alexander's successor, related to the US military's expected functioning in cyberspace in 2025.[27] He said that the use of cyberattacks and cyber defense will be a natural and inseparable part of the commander's toolbox; he will operate and maneuver in cyberspace just as he maneuvers ground forces, in an integrated manner and with a broader concept of applying force. Rogers enumerates three significant points to achieve this situation. First is the understanding that cyber activity is operational activity in all aspects, and is part of the commander's responsibility and sphere of activity.

A commander must acquire and assimilate cyber abilities, and must be knowledgeable about the cyber abilities of the unit, its structure, and potential weaknesses. Second is the existence of a joint network for all Department of Defense forces, wherever they are located and in every medium they require, including cellular. The third and final point is people and partnerships that are the key to this work. In this context, Rogers relates to the need for quality personnel, emphasizing that the military cannot compete financially with the job offers of the civilian industry. Instead, the military will have to recruit personnel based on feelings of national obligation, participation in something significant, and the opportunity to do legally what they otherwise do illegally outside the system.

In April 2015, the Department of Defense published an updated cyber strategy document.[28] This document sets five goals for cyber strategy: (1) Build capabilities and maintain readiness of people for the purpose of activity in cyberspace; (2) Protect the Department of Defense's information network and databases and handle threats to these; (3) Defend the United States and US interests from destructive and significant cyberattacks; (4) Build and maintain options for cyber activity in order to manage and control conflicts; (5) Forge and preserve alliances and international cooperation in order to bolster the ability to handle cyber threats and reinforce stability.

Most of the goals appearing in this document already appeared in previous documents of the Department of Defense. Two points are different. The first is the explicit understanding and statement that the United States does not have the real ability to defend hermetically all the networks of the Department of Defense, to close all their weak and vulnerable points, and to prevent successful attacks. In such a situation, the strategy is to map, identify, and defend the essential data and the most important networks and systems. The fourth task is also worded differently. The Department of Defense is determined to transform cyber activity into a tool in conflicts that will grant the president, as commander in chief of the US armed forces, the option of operating in cyberspace. The description of this task specifically states that its intention is to enable force commanders to integrate planning and to operate in both kinetic space and cyberspace. Although this was stated by commanders of the US military's Cyber Command, and appears worded differently in the documents, it is an explicit and sharply worded definition of the objective that the US government seeks to achieve in its cyber strategy. The other paragraphs relate to continuity of the Department of Defense's

activity – with the US infrastructure as a definite object of defense, because they serve the Department of Defense; cooperation with other government departments and agencies; cooperation with the private sector; build-up of technological force and adoption of advanced defense technologies; training people at the highest possible level; and international cooperation as an essential component in the ability to defend in cyberspace.

William J. Lynn III, a senior government official, shows how organized management of cyberspace challenges in the US government began as a direct result of a specific event, and explains the complexity of formulating a strategy considering the incompatibility of terms from the kinetic world with the cyber world.[29] Terms such as deterrence in Cold War parlance or hard defense of US cyberspace are not relevant. Lynn recommends deterrence on the basis of a strong and effective defense, causing potential assailants to conclude that they will use up their forces to no avail and fail to achieve their objectives; development of advanced risk-reduction strategy at the Pentagon as a more efficient response to threats of harmful components penetrating hardware and firmware; and operational and technological flexibility that enables maximum adaptation to the changing environment. Lynn describes an integrated defense system, comprised of a system that defends "the organization's cyber gateway" and a system that constantly searches for the harmful code that has passed the organization gateway and is located inside its network. Lynn also addresses the organizational issue that occupies a state in facing the challenges of cyberspace. He asserts that the Department of Defense's entry into the field of cyber defense within the United States, although not under his jurisdiction, is due to the high professional ability of his staff.

The FBI has the responsibility for defending cyberspace within the United States. The FBI has set itself the goal of preventing attacks on infrastructure, government authorities, organizations, private industry, and civilians in the United States. The FBI has formulated a strategy of preventative action through addressing the assailants' infrastructure, collecting intelligence, and cooperating with factors outside of the United States. Based on this strategy, the organization implements intelligence-based operations, establishes groups of experts who focus on specific threats, and promotes unique professional development of employees in the cyber field. For the FBI, as well as other US government authorities, cooperation among agencies and divisions that focus on cyber issues is a key point. Implementation is under the auspices

of the National Cyber Investigative Joint Task Force (NCIJTF) and other joint ventures, both inside and outside the United States.[30]

United Kingdom

The UK government defined its cyberspace strategy in 2009.[31] Although this document tends to be extremely general – as details would provide information to its assailants – it manages to convey the essence of the British government's strategy, particularly in the section addressing the organizational structure. The government states its intention to establish the national Cyber Security Operational Center (CSOC), and to include all organizations involved in cyberspace activity. In addition, the British government intends to establish an Office of Cyber Security (OCS) in the Cabinet. Through these two organizations, the government plans all activities in all areas, preserving the necessary principles such as individual freedom, freedom of information flow, and balance between the necessity to ensure this freedom and the need to defend the United Kingdom from cyberattacks; international and internal cooperation; research and development; education, and other fields relevant to activity in cyberspace. The document represents a framework for conduct in cyberspace in the United Kingdom, and emphasizes that a detailed plan is needed for the various organizations in order to transform it into operation.

In November 2011, the Cabinet Office published a document addressing the United Kingdom's strategy for cyber defense, defending the United Kingdom and promoting it in the digital world.[32] The plan set four targets for Great Britain's conduct in cyberspace, emphasizing the fields of defense for 2015: battle against cybercrime with the aim of becoming one of the safest places in the world to conduct cyberspace commerce; stronger resistance against cyberattacks and better defense of British interests in cyberspace; assistance in building a cyberspace that is open, stable, and vibrant, which will safely serve the British public; and the construction of a database that will include knowledge, skills, and abilities needed to achieve the national cyber security goals. The document details the public part of the government plan to achieve these goals, including citizens' awareness of cyber threats and protection abilities; government cooperation with the private business sector; improvement of enforcement against cybercrime; international cooperation with states and organizations; education at all levels; strengthening abilities of defense organizations in handling high-level threats; helping consumers to determine parameters for efficient cyber defense tools; determining one

qualified entity to handle cyberattacks and crises; and encouraging local police forces to respond to civilian complaints of attack. To achieve these goals, the UK government budgeted GBP 650 million in 2011. In December 2014, the Cabinet Office published a report on the implementation of the 2011 program.[33] The document describes broad-ranging, detailed government activity in all four areas that were defined as targets in 2011.

France

The government of France determined its general strategy for conduct in cyberspace in 2009.[34] The core of the strategy is data defense, aspects of data transfer security (mainly sensitive government information), and prevention of data theft. The threats defined by the French government are spy operations and data theft by foreign governments, propaganda, dissemination of ideology and operational directives by terror organizations, and in the future, attacks on government infrastructure by terror organizations as well as enemy states. The French government defined international cooperation with allies as vital for managing cyber threats due to the "borderless" character of cyberspace; as well as the protection of data in fields of government, defense, technology, commerce, and finance relating to French sovereignty; and of sensitive communications of national organizations by means of encryption strong enough to resist deciphering.

In the view of the French government, recovery from a cyberattack on infrastructure is limited, and thus France considers defense of infrastructure as critical, with infrastructure referring to sectors vital to the population and to sectors related to government operation, the economy, and national defense and security capabilities. The French government holds the public administration responsible for the protection of data regularly exchanged between the administration and civilians. In 2010, the French government published directives for increasing the security of this data, and set priorities for implementing these directives. The government considers itself obliged to warn civilians and civilian institutions about cyber threats and to give them instructions to defend themselves. In the long term, the government intends to instill awareness of cyber security through the French educational system.

The method of achieving these targets is through the following steps:

1. Monitoring, analysis, full understanding, and prediction of technological developments, and the ways in which the public will utilize them;

2. Government development of detection capability of attacks on information systems, mainly operating on government networks. The French government has equipped the Data Protection Authority with an operations room for the purpose of formulating a national status report and, if needed, to plan for emergency situations. Based on directives from 2009 and 2011, the government determined that the French Network and Information Security Agency (ANSSI) was the national entity responsible for protecting information systems. Founded in July 2007, it is attached to the General Secretary for National Security and Defense, and is under the prime minister's authority;
3. Continuous improvement of technological, scientific, industrial, and human abilities in the cyber field;
4. Defense of the national data systems and operation of national infrastructure. In this section, the French government gives concrete steps such as encryption systems for government offices and organizations and an identity verification system based on smart cards;
5. Strengthening French legislation relevant to the cyber issue;
6. Development of international cooperation in the field;
7. Distribution of information. The ANSSI is responsible for giving specific assistance and consultation to decision-makers so that they may defend the vital information systems of their organizations as well as the technological, scientific, commercial, and financial systems.

China

The strategy formulated by China for cyberspace activity is vastly different than that described above for the United States, Great Britain, and France. In their article on Chinese cyber tactics, Siboni and Y.R. conclude that the Chinese have implemented a strategy that views cyberspace and kinetic space (land, sea, air, and space) as part of a unified space, and have identified cyberspace as a place in which they can make up for weakness in kinetic space and tip the balance of power between them and their Western enemies, primarily the United States.[35] The United States follows a similar principle in its developing strategy. Cyberspace activity in China is seen as an integral part of the other fields of operation. The Chinese cyber units, both military and informal, operate in broad infrastructural operations so that they can achieve access to communications systems and infrastructures, and obtain information and take control of possible targets for attacks as

needed. The primary targets are located in the United States, and the type of activity analyzed (activity that was discovered and reported openly) led the authors to conclude that the Chinese have internalized military and political weakness in kinetic confrontation with the United States. They recognize the American reliance on its advanced cyberspace system and have identified it as a potential target, which, during confrontation, will enable China to compensate for its weakness in the overall balance of powers against the Americans. In the detailed description of the Chinese attacks, it is clear that the Chinese objectives are infrastructural – for example, an attack on Google can achieve access to the password system and control of the development of the different versions of Google; an attack on the RSA Security company is designed to obtain access to the SecureID database, which would enable the Chinese to easily attack all companies served by RSA; in addition to the wave of attacks that took place in 2006-2011 on Western targets, including government systems, oil and gas infrastructures, communications infrastructures, security industries, computer and electronics companies, and financial institutions.

International Organizations (OECD, ENISA, European Union)

The Organization for Economic Cooperation and Development (OECD) has addressed issues of information security and cyber security for over twenty years. In 2012, this organization published a report on the new cyber security strategy of ten of the OECD's member states.[36] The core of the new strategy is defense of the developed member-states, which are dependent on cyberspace, without harming the freedom of initiative and growth that the internet enables. The strategies formulated by these countries encourages cooperation between governments on the political and operative levels, and clarifies the roles and responsibilities of various authorities; strengthens cooperation between the private and government sectors; and emphasizes the need to respect values such as privacy, freedom of speech, and free flow of information. Some of the strategies adopt a more flexible and rapid approach due to the character of the field, with emphasis on the economic aspect as dominating cyber defense policy. Others include dialogue with parties interested in the cyber field, both for the purpose of policy-making and for implementing this policy. The framework of the new strategies reveals greater investment in research and development; monitoring of national infrastructures; identification of attacks in real time; harnessing the relevant

industry and economic motivation as engines for creating cyber security systems; encouraged cooperation with internet suppliers, and initiating cyber security drills.

In May 2012, the European Network and Information Security Agency (ENISA) also published a report on the status of cyber security among some of its member states. This report relied on data collection for the purpose of creating a practical guide to cyber security for the organization's states.[37] The organization determined that an agreed definition of cyber security does not exist, neither within the European Union nor outside it – and this fact threatens international cooperation, a necessity upon which all agree. The report details topics, known and trivial, that can be found in most of the cyber security strategies. As of the date of publication of the report, the ENISA determined that the EU did not have any cyber security strategy, but it intended to create a study with guidelines for such a strategy. The report recommends that member states create a national strategy for cyber security.

In February 2013, the European Union published a document on the issue of cyber security strategy for EU member states.[38] This document lists the values according to which the strategy must be constructed. The values that the European Union upholds in the kinetic world, such as protection of basic rights, freedom of expression, the right to personal and private information, free access to information and the internet, effective and democratic management by parties of interest (not governmental), and shared responsibility for achieving and ensuring security, also applies to the cyber world. The commission determined five priorities for strategy: achievement of cyber resilience; significant reduction of cybercrime; development of policy and cyber defense abilities, which relate to the general security and defense policy; and formulation of a coherent international cyber policy that will advance the values of the EU. The commission determined that implementation of strategy must be performed mainly by individual governments, and that the EU cannot take responsibility for focused implementation of this strategy. Still, due to the cross-border character of cyberspace and cyber threats, the document defines responsibility of the EU organizations as part of implementing the strategy.

Defense and Deterrence

As in the article by Even and Siman-Tov, Averbuch and Siboni agree that the effectiveness of the classic defense system, based on prior knowledge

of a harmful code, has become increasingly obsolete because the assailants have learned to bypass the signature of the various anti-virus systems. Thus they recommend anomaly-based discovery systems.[39] The technique involves various methods of learning the normative behavior of code known as positive or a representative sampling of it, and writing algorithm that identifies the exception to this normative behavior. Anomaly-based systems may be used for identification and prevention in real time at the entry to the protected network and for identification of a sleeping harmful code, which is introduced into the network and awakened for operation at a later date. The second manner of using an anomaly-based system requires a system that processes information and data logs of activity on computers and servers in a protected system for long periods of time, and enables research of the unusual phenomena (security information and event management – SIEM). The scope of the treated and studied material is big data, and tools and methods enable the identification of anomalies. The weakness of this method is many false positive warnings, which threaten to destroy the credibility and effectivity of the system, and false negative warnings from partial learning of routine or incorrect processing of data. The strong point of this technology is that it is disconnected and independent of recognition and early signature of any specific type of harmful code.

Ben-Israel and Tabansky presented the challenges that the cyber age poses to the accepted views of kinetic security.[40] The ability to identify the assailant and to view his cyber activity as an act of war, followed by a response according to the rules of war, is highly problematic. The ability to defend is also precarious, due to the difficulty of distinguishing between cyberattack and computer malfunction, and the need to maintain an expensive and updated defense system over time. The concept of deterrence is also dubious, because it depends on identification of the attacking factor. This is a very difficult act, due to the structure and attributes of global cyberspace. If the source of the attack is identified and results in retaliatory damage to the computers from which the attack was generated – without the ability to check and verify the damage done to these computers – the ability to deter as a component in the cyber security concept is significantly diminished.[41]

In his study, Cohen describes the threat as similar to the one facing Israel by states such as China, Iran, and Russia, and potentially by terror organizations as well. [42] Similarly to Even and Siman-Tov, Cohen also distinguishes between defense that is applied to objects of defense in various

categories, and broad defense, based on fighting cybercrimes, obtaining intelligence by the intelligence community, and a central authority for operations management, which he recommends establishing under the auspices of the IDF.[43]

Facing Hardware Threats

According to Pierluigi Paganini, combatting hardware/firmware threats is possible, albeit partial, through the use of disruptive and deceptive steps designed to prevent the launch of an attack.[44] He recommends considering "power reset" technology, which prevents problematic components from calculating their time of operation in order to prevent timer-based attacks; "data obfuscation" technology, which encrypts data and values fed to problematic components so that they cannot receive special codes; or to employ data identification or "sequence breaking," which breaks or mixes a chain of messages in a random manner, to prevent problematic components from identifying data patterns and activating an attack on the basis of these patterns.

Deterrence

Amir Lupovici claims that the issue of deterrence in cyberspace is a challenge, mainly because the three main elements of the Cold War model of deterrence do not exist in cyberspace.[45] The author differentiates between deterrence through punishment, which has the role of exacting a high price from the assailant following the attack, and deterrence through prevention, intended to make the assailant feel that the defense is too strong and that his attack will fail, leading him to refrain from implementing the attack in the first place. In deterrence through punishment, the main element of being able to exact a price from the assailant is not guaranteed in the cyber world. This is due to the difficulty in identifying the adversary, and also because some, whether individuals or organizations/states, may have computer systems or information that are not advanced enough to be harmed by a deterrent attack. In this context, Lupovici proposes using non-cyber deterrence against cyberattacks, thus overcoming this specific obstacle. A second element is the reliability of the defender. In order to create deterrence, the defender must implement its response threat. If the defender suspects a chain of responses that will counteract its own response, it is liable to avoid action and thus compromise its reliability. In addition, an imbalanced response is likely

to lead to an international outcry that will lead the defender to moderate its response, thus harming its deterrence reliability. The third element is the ability to remove the threat through a reliable communication channel agreed upon by the adversaries. The weakness of this point is the inability to identify the assailant certainly prior to the attack, which is relevant to creating deterrence. Deterrence through prevention requires an effective defense system. The adversary must be aware of its existence and realize the difficulty in implementing an attack against it.

Attack

Ralph Langner's analysis of the Stuxnet attack is worthy of examination here.[46] Langner divides the attack into two parts. The first part of the attack was covert, and its method of implementation was designed to achieve a specific objective – not the massive and immediate destruction of the Iranian centrifuge system.[47] During the attack, a decision was made to switch from this operational tactic to one designed to destroy a large number of centrifuges, even at the price of exposing the attack.[48] Langner describes the possible use of contractors who had connections with the system at Natanz, in order to introduce the malware into the relevant computers.[49] In addition to the damage by the malware, Langner describes the attack as designed to collect information as well. The fact that Stuxnet skipped over to other systems enabled the assailants to test these systems as possible sources of information on contractors connected to Natanz, and perhaps even those connected to Iran's secret nuclear facilities.[50]

As opposed to the innovation that Langner identifies in the method of the Stuxnet attack, James Lewis criticizes those who view the Flame and Stuxnet tools as novelties in the field of cyber warfare.[51] Lewis analyzes the "noise" created as a result of the exposure of these tools within the context of a political battle with Russia – a battle that aims to diminish the US advantage in cyber technology. Lewis does not find any fundamental difference between attack tools used for espionage and data collection, and those designed to sow destruction. The basic operations required for espionage or destruction are the same acts of gathering intelligence and securing a foothold within a computer network. The view that a cyber operation can have a destructive kinetic consequence is also not new, according to Lewis' analysis. Russia's attacks on Estonia and Georgia are examples of implementation of this strategy, and they also were carried out through proxies. According to

Lewis, the use of Stuxnet does not represent a new age as it will not lead to a sophisticated and destructive cyberattack on the United States, due to the fear that an attack causing serious kinetic damage may lead to a powerful kinetic response by the Americans. In this analysis, Lewis also contributes to the discussion on deterrence, and argues that deterrence integrates both worlds – cyber and kinetic – into one equation of the balance of power.

Attack as Part of Overt Conflict

As opposed to the covert attack, a cyberattack can be part of an overt conflict between powers, such as in the 2008 war between Georgia and Russia. In analyzing the Russian attack on Georgia, Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata point to the Russian strategy of using cyberspace in the battle over national awareness, public narrative, information, morale, and public opinion – all part of the kinetic battle they waged over the national Russian interest in an area steeped in controversy.[52] The use of cyberspace was part of a broad battle of awareness, which, in turn, was part of the overall kinetic battle to obliterate Georgian sovereignty in the Ostian territories. According to the authors of this study, the Russians had realized the importance of the battle over national awareness in the information age at an earlier stage, during the first war in Chechnya (1994) when they lost the battle of narrative. Applying the lessons learned then can be perceived in all battles that the Russians have since waged. In the Georgian war, the Russians' battle tactics included paralyzing the physical systems (disconnecting the optical fibers that served Georgia's international internet traffic); taking control of Georgian internet traffic (traffic rerouted through Russia); blocking Georgian broadcasts to prevent heads of state from communicating with the public; broadcasting Russian propaganda messages on Georgian sites, throughout the Former Soviet Union, and to Western countries; and finally paralyzing the Georgian internet servers through a massive DDoS attack, which led to paralysis of the foreign ministry, the president's office, and various essential services, including the banking system, for several hours. The Georgian attempts to fight this battle were only partially successful. The Russians did not hesitate to broaden their cyberattack to other sites outside Georgia, including attacking an American host site that supplied services to the Georgian government. In implementing this strategy, the authors imply that proxy organizations were utilized, including Russian crime organizations (there is no direct evidence of Russian government

involvement in these attacks), as well as civilian supporters of Russia who launched cyber interventions on their own initiative.

Attack as Part of the Operative Battle Plan

States are preparing to implement cyberattacks as a structured part of their operative military plans. The examples given here demonstrate that at least three global superpowers (United States, Russia, and China) view this as part of their operational strategy in cyberspace. As noted above, China is apparently preparing an infrastructure for such an operation in an emergency situation. During the war with Georgia, Russia implemented this strategy as part of its battle tactics in the fields of public awareness and information.

In this context, we once again turn our attention to the American concept. According to US cyber command directors Alexander and Rogers, the cyber command is building power and pushing for cyber operation to become an integral part of every operative plan of the US military command staff, exactly as in land, sea, or air maneuvers, even though there is not any documentation that this strategy should be implemented. Cyber activity will be integral to the command/operations decisions that each commander will be required to make. Each commander will have to understand the power he holds, the consequences of the actions he orders or authorizes to perform, the ability of the general staff to assist and the manner in which cyber operations can aid in achieving battle objectives. The commander will have to understand the dangers faced from enemy cyber operations, and the methods of defense against such operations. In their testimonies, Alexander and Rogers speak of cyberattack groups as integral components of the battle command staffs. They also mention the concept of command and control in the context of the command's cyber status report and between battle command and cyber command.[53] Rogers' vision is that the use of cyber tools – for defense and offense – will be an integral, inseparable part of the commander's toolbox, managed and maneuvered just as ground forces are maneuvered in an integrated manner and with a broader view of applying force. This will be carried out through a joint-network resolve shared by all forces.[54] At another opportunity, Rogers explained that development of an operational concept and command as well as control structure must be ensured, and this will transform cyber battles into an operational reality.[55]

Table 1: Comparison of State Strategy Documents

This comparison is based on access to unrestricted publications studied for the purpose of writing this document.

	Defense	Attack	Deterrence	Force Build-Up	Organizations and Processes	Legal Regularization	International Cooperation
Israel	The government accepted recommendations for an initiative	No mention or treatment. Israel is considered to have attack abilities, and together with the United States – the Stuxnet attack.	No mention or treatment of this issue.	Broad treatment in summary of initiative for technological and human force build-up.	Open discussion alongside several government decisions on division of responsibility among organizations on the cyber issue. The National Cyber Bureau was established, and a decision was made to establish the National Cyber Defense Authority. Recently, the decision was made to establish the Cyber Command in the IDF.	No mention or treatment of this issue.	No mention or treatment of this issue.
United States	Intensive treatment at government level.	Cyberspace is understood as part of the kinetic world and a continuation of it. There is a plan for assimilating cyberattack abilities in the military commands as part of every operative plan, and setting up attack groups within these commands. The United States is assumed to have been part of the cyberattack in the covert operation against Iranian nuclear capabilities (Stuxnet).	Broad discussion of the issue – whether deterrence in cyberspace can be carried out without evidence of attempts to deter, with the exception of the case of the cyberattack on North Korea, following the attack on Sony.	A broad process of force build-up led by the DoD, together with government offices and relevant agencies. Force build-up includes commitment of financial resources, human capital, training, combat doctrine, and tools.	A plethora of organizations operate in US cyberspace, with areas of overlap. The structure of responsibility and authority appears still unstable, but dialogue is taking place. Processes are in stages of being regularized, both in security and military organizations, and in the government and civil sector.	Not yet implemented. Under discussion: the tension between defense of right to privacy in the post-Snowden era and the understanding that without data on the private/civilian sector, it will be difficult to protect the vital assets of the United States.	A significant component is present in the concept.

	Defense	Attack	Deterrence	Force Build-Up	Organizations and Processes	Legal Regularization	International Cooperation
France	The core of the strategy documents is defense. Definition of relative threat and guidelines for a defense plan exists at government level. Explicit reference to encryption as a significant component of defense.	No mention or treatment of this issue.	No explicit mention or treatment of this issue. Implicitly understood that strong encryption should deter attack.	Planning and specific description of force build-up in the technological field and human capital. Investment in incorporating the issue of cyber defense and its dangers into the educational system.	Establishment of a national status command center, definition of responsibility of ANSSI for cyber defense of the state, and definition of government responsibility toward the various sectors.	No mention.	Appears as a significant component of strategy, including the need to avoid falling behind in investments, relative to European counterparts (Great Britain and Germany).
International Organizations[56]	Broad treatment.	No mention or treatment.	No mention or treatment.	Reference in principle.	Reference in principle.	Reference.	Broad reference.
China	No mention or treatment.	Like the United States, China considers cyberspace as a continuation and complementary part of the kinetic world. It carries out cyberattacks as part of a comprehensive plan whose goal is coverage and compensation for its kinetic military weakness in comparison to the United States, and as part of a strategy of economic development based on new initiatives and invention in other countries.	No mention or treatment.	No mention or treatment.	Organizations exist within the Chinese military and proxy organizations for carrying out attacks.	No mention or treatment.	No mention or treatment.

	Defense	Attack	Deterrence	Force Build-Up	Organizations and Processes	Legal Regularization	International Cooperation
Russia[57]	Lacks combat doctrine, documents, and open discussion – no mention.	Analysis of cyber activity in the Georgia-Russia war and the attack on Estonia indicate Russian use of cyberspace for attack operations, although via proxies and without proof of government responsibility for the attacks.	No mention.	Lacks combat doctrine, documents, and open discussion – no mention.	Lacks combat doctrine documents and open discussion – no mention.	Lacks combat doctrine documents and open discussion – no mention.	Several mentions of Russian desire for international law to regulate cyber battle.

Defense

The main goal of a national cyber defense strategy is to preserve the basic functioning of the state, which can be harmed by a cyberattack. Another important objective is to enable the relevant factors in the State of Israel to determine and execute operations in cyber and kinetic space against its adversaries, in the recognition that cyberspace can be defended against potential actions. Still, implementing any strategy will not lead to the thwarting of every cyberattack against every target or against every object of defense. Hermetic defense results are impossible to achieve, and thus some cyberattacks will succeed despite the guidelines for a defense strategy proposed herein.

This document proposes that deterring a cyberattack means preventing the attacker from achieving their objective. The goal of thwarting a cyberattack is not protection of computers or networks, nor does it necessarily mean blocking the attack. This distinction is significant because it can provide the defense with a wider field for maneuvering when it comes to planning and choosing tools for defense strategy. For purposes of defense strategy, this document proposes to differentiate among three types of attacks. The first type is an advanced persistent threat (APT), an attack planned to penetrate the depth of an organization's computer system for a relatively long period of time, with an attempt to hide the attack. The second type is a rapid, superficial attack, whose results are immediately noticeable. Usually, its aims are to cause changes to the site or prevent access to it and the cyberspace services it offers (defacing, DDoS). Although such an attack seems superficial and its results are usually limited in time and in its effects on the public morale, intensive use of such tools over time against a number of targets in a single state will significantly disrupt daily routine, and is liable to cause damage to aspects beyond public morale. Finally, an infrastructure attack is an attack on hardware or firmware elements,[58] for the purposes of stopping operation (CNA) or for enabling future access to the computer/network.

For APT attacks, the strategy should be based on a combination of tools and abilities that do not require prior information or knowledge of attack components and methods, along with existing tools and methods whose development should be continued. This guideline is essential, but does not stand alone. Efficient cyber defense must be based on additional guidelines, including transparency in reports on inter-organizational attacks; forming an up-to-date, comprehensive evaluation of national cyber status; constructing rapid response factors; using research and learning data on attack tools and groups; cooperation with commercial defense and intelligence organizations; international cooperation wherever possible and worthwhile; development of continuous intelligence collection on enemies and opponents for deterrence purposes; formulation of a cyber response plan as part of a possible deterrence dimension; and development of the ability to recover from an attack when possible, with the understanding that the line of defense will always be breached, and thus Israel must organize for rapid recovery as a result of successful enemy attacks.

Response to Advanced Persistent Threat (APT) Attacks

Handling this type of attack is based on a number of assumptions. The first of these is that most organizations require connection to the public cyberspace, and thus all networks are threatened with attack, including those declared as supposedly disconnected from external cyberspace. The second is that the assailant will attack the point that is most convenient – meaning the least defended point. The attack point can be a factor in "the supply chain" – in other words, an external organization that is in contact with the defended entity, but not protected like it. Another assumption is that the assailant is liable to carry out the attack through tools embedded into computer products at an earlier time, even as part of the production process. Later, the assailant will prefer to initiate attacks different from those already identified and researched, both in choice of attack tool and implementation of attack method. Finally, it is assumed that the defense will not have the necessary intelligence about the attack – identity of the assailant, physical location, motivation and goals, attack tools, method, and date of the attack.

In planning the defense system, a response must be given to the implications of the above-mentioned assumptions. In general, the defense must be planned along a continuum, from the end point at the defended organizations' network to the last of the organizations that are related in some way to its computer

system. The methods of defending a sensitive organization in the field of state security must be identical to those used to defend the computer network of organizations that are in cyber contact with the organization attacked. Another guideline is to discover the attack at the earliest possible point, and use a system for handling attacks in a calculated, intelligent, and responsive manner. This differs from immediate, automatic cessation of the attack. In the overt system, this document proposes to enhance the methods of conduct and the tools based on existing intelligence and statistical analysis, and to integrate the ability based on the identity of attack without prior signature, or any other intelligence.

As a guideline for the preferred treatment for an attack, this document proposes to contain the attack as much as possible, at the point at which the assailant is likely to achieve his goal. Containment enables the defense to learn about the attack, the tools, the objectives, and if possible – the identity of the attackers. In this context, it is possible to examine thwarting the attack by a number of means, and not just by immediate destruction of the tools of the attack. This approach is relevant mainly when the purpose of the attack is data theft. It must be executed in such a way that the attack will be under control and the defender can perform follow-up, without the assailant being aware. In this context, see Figure 3:

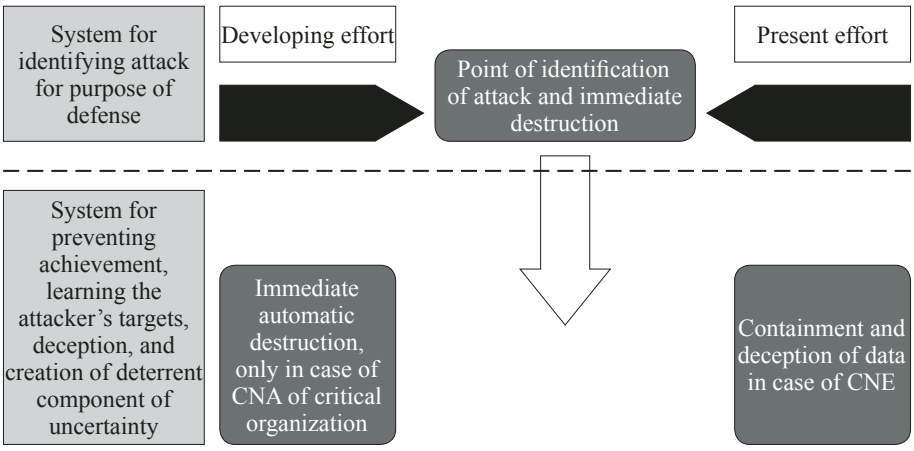

Figure 3: Concept for Handling APT Attacks

The upper part of Figure 3, above the dotted line, describes the system of attack discovery, a critical point for all that is related to APT attacks in

cyberspace. The assailant will undertake significant efforts to avoid early discovery, while the defender will attempt to discover the attack as early as possible. Early discovery and identification of the attack provides the defender with a true advantage, but is not essential. One developing concept of defense assumes that the attacker has succeeded in his mission, and the organization's network contains a harmful code. The defense must adopt patterns of operation and technological abilities that enable it to disrupt and thwart the attacker from achieving their objective at various points, even without identifying the attack at an early stage.[59]

The ability to discover and identify an attack depends considerably on prior information in the mode of "know your enemy." This information includes knowledge of the code of the tool of the attacker or part of it, and/or knowledge of the operational patterns of an attack group or a specific assailant. For the most part, this information derives from analysis of the tool of the assailant, attack groups, and individual attackers by cyber defense and intelligence companies, and cooperation between these companies and the organizations that are being defended. At a higher level, this information includes statistical analysis and behavioral algorithms for finding attributes of attacks without having any firm indication of an attack.[60] This is a broad and strong foundation, based on existing and developing abilities to implement the first discovery component in the discovery system proposed here. In organizations targeted for defense in Israel, this component should be enhanced by having information embedded in it, which is held by the Israeli intelligence services, and the detailed and extensive intelligence maintained by commercial defense and intelligence companies worldwide. This information must be updated as close to real time as possible, and it must issue a warning each time suspicious activity is identified.

Figure 4 also shows a graphic representation of the defense concept. It shows the defense process as it relates to various components on the attack chain axis. This representation divides the process of attack into seven stages.[61] Four components of defense are activated during the process of the attack: early warning actions to prevent attack; detection of attack as soon as it takes place; reaction to prevent damages of the attack; and finally, recovery operations with the goal of returning to full operation, if actions fail to prevent the damage caused by the attack.

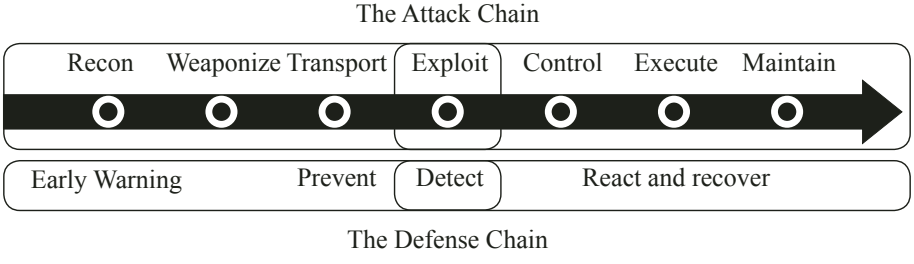

Figure 4: Defense Chain vs. Attack Chain

This line of defense requires a supportive structure such as a Computer Emergency Response Team (CERT), organizational Cyber Security Operation Center (CSOC), and appropriate work processes. Optimization of various components of defense at the level of tools, intelligence, cooperation, transparency, time, quality of reaction, and professionalism of CERT/organizational CSOC are not luxuries or options. The efficacy of this defense line should not be taken for granted, and it is not guaranteed. It is conditional on continuous updating and improvement, because the ongoing chase after attack tools stems from a position of structural weakness, and only the best and most efficient functioning, or close to that, will grant this line of defense relevance over time and justify the investment.

In order to ensure that a system can identify a planned and focused attack for which prior information does not exist, it must use technology that does not require prior knowledge and signature of the attack tool or the attackers.[62] An example of this type was given in the description of a product based on monitoring and checking the exit points in the organization's network.[63] Technology that is not based on knowing the attacker, their tools, and methods requires in-depth knowledge of the "legal" processes of the protected organization's computers, and checking of each command/process against a previously known routine. With the assumption that an attack code will have difficulty imitating the "legal" operation, it will be identified as a code performing an "illegal" operation, without connection to the defender's previous knowledge of the attack code. The power of a solution of this type is in its theoretical disconnection of the dependence between the detection ability and the existence of specific or generic/conclusive prior intelligence. The significant weakness of this connection undermines an important advantage of the assailant – the ability to surprise with a new

tool or skill or with an already identified and signed attack tool, in which a minor change has been made, enabling the assailant to circumvent the defense mechanisms.[64]

The proposed guidelines for designing the detection stage are the ongoing provision of information by the intelligence community and leading intelligence companies to the intelligence-based defense system; the addition of a detection component not based on prior intelligence (such as the examples given here); and integration of all these into a complete detection system. This act is likely to enhance and upgrade the efficiency of this detection system so that one component feeds the next with data, improving its ability to detect and identify an attack. The existence of a professional organizational entity responsible for managing the detection system and making the decisions is essential for this technology to be really effective.

The next stage is to prevent the assailant from achieving his goal. This is the stage described in Figure 3, and the concept of handling an APT attack is depicted under the dashed line. Based on the definition chosen (obstructing the attacker's goal and not the attack itself), there is the potential to change the situation at this stage since the default action upon discovery is the decision to immediately stop the attack. At this stage, the proposed procedure is to distinguish between an attack whose goal is destruction (CNA) and an attack whose goal is espionage and data theft (CNE). In addition, a distinction must be made between attacks on sensitive and essential entities for purposes of destruction and halting operation of infrastructure, such as the electric company or the water company, and attacks on other, non-essential bodies, for the purposes of destruction and halting operation, but also for espionage and data theft. The guideline is to immediately halt the attack on essential and sensitive entities when discovered for which the explicit goal of the attack is most likely destruction and halting operation. For all other entities, the guideline is to contain the attack in order to learn about the attack; the technological aspects of the tools used; the fields of interest of the attacker; and if possible, the attacker's identity. In order to reduce the ability to cause harm or steal data, processes are needed to show constant change and to deceive the attacker. For example, after identifying the attacker's interest, the location of the data on the network or of the network to be defended should be changed. Such changes will make it very difficult for the assailant to carry out data theft.[65]

After identifying the assailant's fields of interest, additional actions may be considered, such as feeding the assailant incorrect information. This mode of action can thwart the attacker's objective.[66] Furthermore, data deception can be part of deterrence. Placing an uncertain component in relation to the reliable data stolen from the organization can have significant weight in whether or not it is profitable to carry out an attacks. The guideline for containing and disrupting/deceiving an attack can turn the tables from a situation in which the attacker initiates, learns the weaknesses of the defender, and secretly carries out its attack without the defender's knowledge – to a situation in which the defender learns the attack, analyzes it, and responds in a sophisticated and covert manner without the attacker's knowledge.

The combined defense system is relevant to APT attacks. Two additional types of attack require a response that completes the proposed defense strategy: rapid and superficial attacks, whose results are immediately visible and usually designed to change or prevent access to sites or cyberspace services (DDoS, defacing); and attacks that take place by treating the hardware or firmware components during the serial production stage or by individuals after having acquired the product.

Response to Rapid, Superficial Attacks (DDoS, Defacing)

The most common attacks on the network are those characterized as relatively rapid and superficial. For these, the attacker does not need much prior intelligence; the intelligence can be obtained rapidly, and mostly, it does not require a sophisticated attack or special attack tools. Usually, this kind of attack results in prevention of service (DDoS – Distribute Denial of Service) of a site, and their actual damage is limited in time and scope.[67] A line of defense is needed against such attacks, not only to prevent their effect on morale and image, but mainly because a DDoS attack, when planned as part of broader activity, can cause real damage. This kind of threat should not only be characterized as only affecting public morale and the sense of sovereignty and governability, but, as in the Georgian case, should be considered a real CNA attack, with the attacker's goal being to thwart communication and transfer of information.[68] The guidelines for preparing defense against service prevention attacks or site change is to rely on the internet service and cloud information providers to broaden bandwidth for an organization; monitoring, locating the attack, and blocking it; and constant

monitoring of organizations' data centers in order to withstand an attack by the application intended to prevent service.[69]

Another risk relates to the possibility of creating a large number of superficial attacks. A broad-range DDoS attack assumes that even though each individual attack is superficial and has only limited, local potential for damage, synchronizing a large number of DDoS attacks could produce grave results. The suggested guideline is to provide bandwidth that can override blockage to sites relaying information to the public or serving as symbols of government and sovereignty. This will prevent the sites from communicating with addresses connected to the attack and when needed, they will be transferred to alternate host sites.

Use of the "Cloud" by Security and Other Essential Organizations

Work on the "cloud" is divided between the external, internal, and hybrid clouds (integrating internal and external clouds according to need and the organization's policy), and also based on use of the cloud as a software service (Software as a Service – SaaS), as a platform (Platform as a Service – PaaS), and as infrastructure (Infrastructure as a Service – IaaS).[70]

Although all agree on the efficiency and savings when working on an external cloud, defending the entity's information is disconcerting. Aside from the sense of discomfort when the information is placed in an external location, and technological concerns (availability of applications in emergencies, durability of the cloud supplier under heavy usage), organizations must ask how their information is protected in the cloud. How can an organization ensure that its information will not be stolen by a CNE attack? How can it ensure that its organizational information will not be damaged by a CNA attack? The problem exists for those entities fearing industrial espionage, as well as financial institutions that must demonstrate reliability and discretion, and government and security organizations concerned about damage and theft of information.[71]

Use of the cloud raises additional concerns beyond the risk posed to information security. The issue of service availability is crucial for certain sectors, such as finance. The risk relates not only to technological availability of service, but also to political aspects. For example, a state may decide to block cloud service or partial cloud service to a country (as in the case of Israel) due to political decisions. This leads to a very high level of risk, but the probability that it will occur must be examined. Israel, like many countries,

relies on services originating in other countries. A key example is the use of Global Positioning System (GPS). Many essential security systems rely on these location services. Here as well, the level of risk is high, but experience shows that the likelihood of this risk is negligible. Here, a direct comparison can be made with the use of the cloud for essential civilian services, such as the financial sector. These sectors should perform an organized and comprehensive process of risk management when transferring to cloud services. The location of cloud servers and the risk of service prevention due to political considerations must be considered, and the servers preferably should be located in states with an appropriate Western political culture.[72]

The use of the cloud by security organizations or organizations defined as providing essential government services is still in its inception. Organizations based on information that is exclusive, sensitive, reliable, and protected, such as banks and even security organizations such as the US Defense Department, have begun partial and preliminary use of the cloud, subject to detailed defense directives.[73] Handling an organization's information security for cloud use has led suppliers to provide varying levels of defense services on the cloud.[74] In addition, organizations are determining directives, standards, and procedures for cloud use. In parallel, the cyber industry is developing products designed to effectively confront the existing threats to cloud use.[75]

It is recommended that security entities and essential bodies in Israel wait as long as possible and not rush into using the external cloud. The use of the cloud is still in its infancy, as is the analysis of threats realized to the information stored on the cloud, and of the most efficient ways of defending against these threats. If the decision is made to use and rely upon the cloud, its use must be measured and gradual. The model should be hybrid (leaving information and processes on the organizational network as well) and accompanied by detailed, stringent directives for cloud use.

Response to Hardware and Firmware Attacks

Hardware-based attacks[76] are possible and are implemented in two ways. One is by penetrating the attack component during the production stage of the device. Examples are "back door" capability, enabling the assailant to obtain secret access to the device's communications or memory, and penetration of a sleeping software agent (BOT) that can be operated by the attacker or when predetermined conditions are realized. For the most part, an attack during production stages will be executed by a state or manufacturer,

which has access to these stages.[77] The second way is by the use of ordinary commercial equipment, which has the ability embedded within it to enable access to the memory or to the device's communication ability.[78]

The field of hardware and firmware attacks has great potential for damage for three main reasons: The attack components cannot be removed through conventional methods (anti-virus, formatting); they can circumvent security mechanisms (such as passwords, encrypted system files); and it is extremely difficult to locate attack components that have been embedded during the production process.[79] It is very challenging to identify these attacks and treat them.[80] The extent of the threat and its seriousness is even greater due to the fact that China, a state that has carried out cyberattacks in any way possible, manufactures a significant amount of the computer hardware and computer products.[81]

Handling attacks on hardware and/or firmware is complex and worrisome to the superpowers as well. Similar to the proposal for confronting APT attacks, the guidelines for a strategy to handle these attacks also integrates a number of methods. The first method is to use hardware built in Israel in a safe, authorized location. This solution only partially neutralizes the problem, because construction of the components required is very complex and expensive, and sometimes even impossible from a practical point of view. Therefore, this approach cannot be implemented everywhere and for every purpose. If possible, we recommend implementing it in the most sensitive fields, in which Israel requires the highest level of confidence and trust in the information security and production processes.

A second approach confronts attack by using the most thorough examination and inspection of hardware components. The hardware can be checked in depth, in the form of "reverse engineering," to reveal components or code embedded during post-production. This process is also expensive and delays production and installation. Reverse engineering that reveals components embedded during component production is even more difficult and expensive. Still, the proposal is to examine the possibility of performing reverse engineering on computers related to the production system and in sensitive work processes, and for which a computer system based on secure hardware cannot be manufactured.

The situation is somewhat different for hardware attacks embedded in existing devices produced in serial manufacturing. In this case, one of the possible treatment approaches is the ability to compare components in

the serial device – assuming it can be determined that one is an operative device that was not handled by the attacker – and a device under suspicion of handling. This comparison is not immediate and requires advanced professional abilities.

Finally, similar to the proposal for handling ATP attacks, the handling of hardware attacks also must be based on understanding the potential damage. It is proposed to take steps that mislead and disrupt, thus preventing execution of the attack. In this framework, it is worthwhile to examine implementation of proposals such as "power resets" – a technique that prevents damaging components from computing how long they have been operating in order to deter timer-based attacks; "data obfuscation," which encrypts data and values entered into problematic components so that they cannot receive special codes or be operated on the basis of data identification; and "sequence breaking," which breaks or mixes randomly a series of messages, thus preventing damaging components from identifying data patterns and executing a subsequent attack.[82]

We recommend adopting a complex strategy comprised of a variety of solutions described here. Secure hardware and firmware manufactured in Israel may be used in a protected manner, but this is possible only for individual objects of defense, for which there is a high motivation to attack through hardware and firmware. Physical tests of hardware can be conducted in order to ensure the absence of components that should not be present. The core of the defense needs to be very sophisticated, and changes should be made in the information entered into some of the components, in order to eliminate the basis for executing the attack. Given the high level of sensitivity and professionalism required in this field, it is recommended to establish a national center for testing hardware and firmware. Such a center can meet all the needs of the relevant factors in Israel, and can be integrated into the national laboratory that exists today at Rafael, or in another framework.

Preventing Attack through Deterrence

The proposed defense strategy is not hermetic, and we must assume that sometimes, attacks will be successful. The success of a cyberattack usually raises two issues – the question of response (usually for deterrence) and the question of recovery from attack. The popular, rational justification for responding to an attack is the desire to deter and prevent additional attacks. This viewpoint is based on the assumption that the attacker will think

rationally and weigh the cost of the attack and profit if successful. As long as the cost of the attack is higher than the profit, the assailant will choose not to execute the attack, thus creating deterrence. The validity of this process has not yet been proven in cyberspace. A real obstacle is determining the identity of the attacker. Such identification is not possible in many cases. States and bodies with cyber handicaps have an advantage here, as they can carry out cyberattacks against developed nations without fearing any anticipated cyber or physical response,[83] as the ability to react in a manner that hurts the assailant is limited due to the cyber handicaps of the assailant. At the same time, in cases when it seemed that a cyber or physical response could be used for the purpose of deterrence, such a response attack was not carried out.[84]

Alongside the classic definition of deterrence, a strong defense ability can also serve as deterrence, leading the attacker to conclude that it is not worthwhile for him to invest in an attack because his chances of breaking through the defense system are very low.[85] Furthermore, we may also consider, as proposed above, deterrence based on the attacker's uncertainty about whether the information he steals is an amalgamation of real and false information, and his inability to distinguish between the two.

Recovery from Attack

"Recovery from attack" is a broad term covering preparation, processes, tools, and methods whose goal is to reduce the damage of a successful attack and return rapidly to normal operation. Recovery from attack may be described in technological terms as return of the computer network and computer-based work processes to operation after they were neutralized by the attack. Technological recovery is mostly based on backup of systems and databases, under the title of a disaster recovery plan (DRP). Such a backup system is usually needed and planned for rapid dealing with physical damage (earthquake, flooding, fire, and explosions) or malfunction of the computer system, or by accidentally deleting information at the location of the organization's central computer system, resulting in irreversible damage. A backup system is also relevant for recovery from destructive cyberattacks, as long as the attack has not damaged the backup systems as well.

The concept of recovery from an event is taken from the field of risk management. This field is an integral part of planning defense in general and in cyberspace in particular, and it is designed to determine priorities for

defense methods while considering the general risk framework. The overall risks are analyzed through a survey, and then they are prioritized. Alongside the defense solution for these risks, the organization must consider the steps to be taken in order to minimize the extent of damage and its duration, if the defense does not succeed and the risk occurs.

In the theoretical context, the concept of recovery from attack is related to the field of national or organizational resilience. This resilience reflects the organization's ability to confront expected or unexpected extreme situations, and to return to a level of functioning, at least to that which preceded the event, and sometimes to an even higher level. In order to constantly improve national resilience in the cyber field, these processes should be incorporated as an integral part of the risk management process, and tools and methods must be developed that will enable rapid and effective recovery from cyberattacks. Figure 5 describes the general risk management process and recovery as an integral par of it.

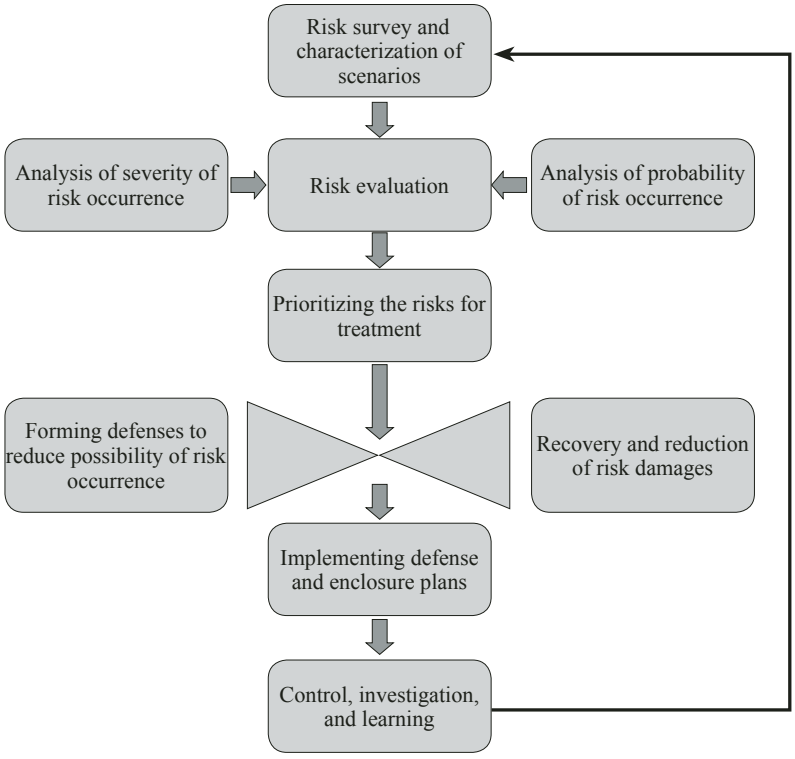

Figure 5: Visualization of Risk Management Process

The relationship between defense of cyberspace and recovery from attack can be seen in the Figure 6. The left side of Figure 6 shows the system of defenses employed in order to prevent occurrence of an attack. These defenses are multi-layered, and their goal is to hinder the assailant from executing the attack. The attack vector pictured on the left is the process of the attacker attempting to penetrate the defense in order to execute the attack. Because it is clear to all that every defense, as resolute and sophisticated as it might be, is likely to be breached by a determined assailant with advanced abilities, we may assume that sooner or later, the attacker will achieve his goal. The recovery process is designed to plan in advance the steps that can reduce the damage and return the system to normal functioning as rapidly as possible. In this, recovery can also prevent the assailant's desired achievement. In Figure 6, the risk management theory developed in 1979 and known as the "Bowtie" – due to its resemblance to the eponymous knot – was adapted to the cyber field.[86]

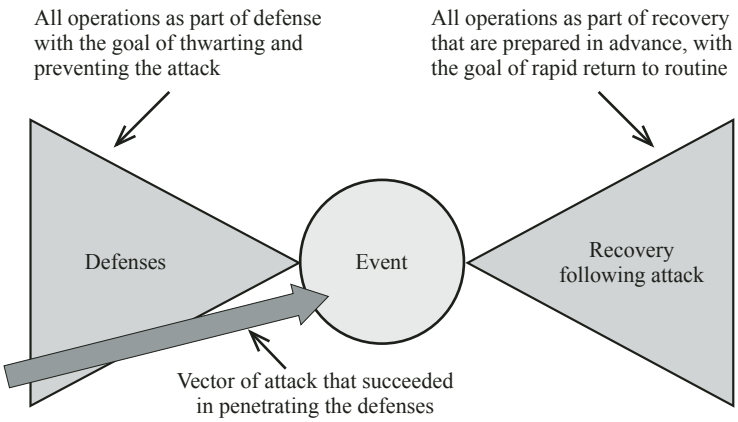

Figure 6: Recovery from Attack as an Integral Part of Defense

Recovery from an attack is not only limited to the technological viewpoint. For example, in the successful attack on the databases of the Sony Corporation, North Korea, the main suspect in the attack, did not achieve its desired result of preventing the screening of a specific film because the American government was able to convince Sony to screen the film. This is an excellent example of a successful cyberattack, which integrated a kinetic threat to physically attack viewers in the cinemas that screened the film; this attack was prevented, however, through determined leadership.[87]

Complementary Defense Issues

Culture of Cooperation and Transparency in Organizational Structure

Two issues, worth exploring, complement the strategy detailed above – the organizational structure and a culture of transparency and cooperation. The defense strategy described here cannot be implemented optimally without a guiding hand that actively supervises the relevant organizations, or at least those related to national security and essential to the functioning of the state, and their entire "supply chain." Active supervision means determining a responsible entity in every supervised organization (or at the sectorial level) that must implement defense at the required level and ensure that its entire supply chain implements the same level of defense. This supervising entity will be required to report every irregular incident. It must exchange information with other organizations in a transparent manner, both regarding attack and effective defense mechanisms. In addition, it must coordinate its response to attacks with the security organizations that are responsible for such on behalf of the state.[88]

A division of responsibility for cyber defense exists in Israel. The division reflects the general responsibility for security in Israel, in addition to significant corrections and changes over the years, born out of the character and attributes of cyberspace and inter-organizational struggles. Although not the focus of this document, some explanation is necessary about the organizational development in Israel in the field of cyber defense responsibility.

The Regulation of Security in Public Entities Act of 1998 determines authorities and responsibilities for information security and security of essential computer systems of various public entities. Appendices to the act have determined that the Israel Security Agency (ISA; in Hebrew, Shabak) is responsible for information security of the Prime Minister's Office, the Defense Ministry, defense systems factories, the President's Office, and the Foreign Ministry. Despite this decision, some of the organizations have deviated from this framework. The Defense Ministry is supervised by the Director of Security of the Defense Establishment, while the Mossad and the IDF are independent in cyber defense.[89] The appendices to the law define the organizations that represent essential infrastructure in Israel, and are supervised by the ISA in the fields of information security and computer systems security.[90] In 2002, the government issued decision 84B of the Ministerial Committee for Security Issues, establishing two dedicated entities: a supreme steering committee, to regularly study the identity of the public

and private entities essential for the functioning of the state; and a national unit for defense of computer systems.[91] The goal of the steering committee, directed by the head of the National Security Council, is to formulate steps for defending the state's critical computer systems. This committee served as the steering committee that supervised the national unit for computer infrastructure security of the ISA.[92]

In 2011, the government decided to establish a national cyber bureau, "a bureau for the prime minister, the government and its committees, which recommends national policy and promotes its implementation in the field of cyberspace, subject to all law and government decisions."[93] In addition to serving as a central entity, the cyber bureau is charged with implementing the recommendations of Isaac Ben-Israel the chairman of the National Council for Research and Development, namely, to advance and develop knowledge infrastructure; engage in research and development related to cyber technology; develop "tools for emergencies in the cyber field"; establish "a national cyber security framework" and "solutions for local defense." This should be accomplished "without damaging the authority invested in any other entity by law and the government's decisions."[94] Some three years later, the prime minister charged the head of the cyber bureau to establish "a national authority for operative defense in cyberspace," to operate alongside the bureau and accept authority and responsibility for the issue of defending the civilian space from cyber threats. The authority will be an operative entity.[95]

In 2011, the chief of general staff of the IDF granted responsibility for cyberspace operation to two entities – the 8200 unit of the military intelligence for the field of offense, and Teleprocessing Corps, the defense unit of the IDF computer division for the field of defense.[96] In an interview, the head of the Teleprocessing Corps reported that the IDF had established a center that integrates representatives of military intelligence forces and members of the computer division, whose job is to defend against cyberattacks.[97] On June 15, 2015, the chief of staff publicized his decision to establish a cyber command within the IDF, which would address all fields of cyber activity; this process should take about two years to establish.[98]

Other entities in Israel do not have specific responsibility for defense against cyberattacks, but their activity touches on the field: the National Computer Division of the Ministry of Finance, which is responsible for supplying secure internet services to government offices, and defending

government networks in their connection to the internet; the Israel Police Unit for Prevention of Cybercrime, which operates as part of the Lahav 433 unit, and investigates cybercrime and "initiated activity related to online threat scenarios";[99] and the Authority for Law, Technology and Information, founded within the Ministry of Justice – whose role is "advancing awareness of the individual to the issues of privacy and protection of personal information on the internet."[100] In the context of defense against cyberattacks, Israel may be divided into several groups (see Figure 7):

1. Defense organizations – IDF, intelligence community organizations, Israel Police, and similar entities. These organizations decide on their own defense concept and implement it in accordance with their operational needs and operating authorities.
2. Defense industry – defense companies and organizations with defense sensitivity. The Director of Security of the Defense Establishment (DSDE) determines the requirements in the field of cyber defense, and confirms that these demands are met.
3. Critical national infrastructure – sectors whose activity is essential for the functioning of the state, for example: supply of electricity, water, and so forth. These operate under the guidance and control of the Israel Security Agency.
4. Government offices – defense of most government offices and government authorities is carried out under the direction of the national computer division, which has a unit operating in the field of cyber security. The Ministry of Defense is guided by the DSDE.
5. The civil sector – all other civilian users of the internet, including organizations, businesses, and private individuals. This is the most vulnerable group, whose defense capability is determined by business considerations. As a result, assailants may prefer to act against this sector whose defense is deficient. This group must operate under appropriate regulation to be determined by the National Bureau of Cyber Defense that was recently established.

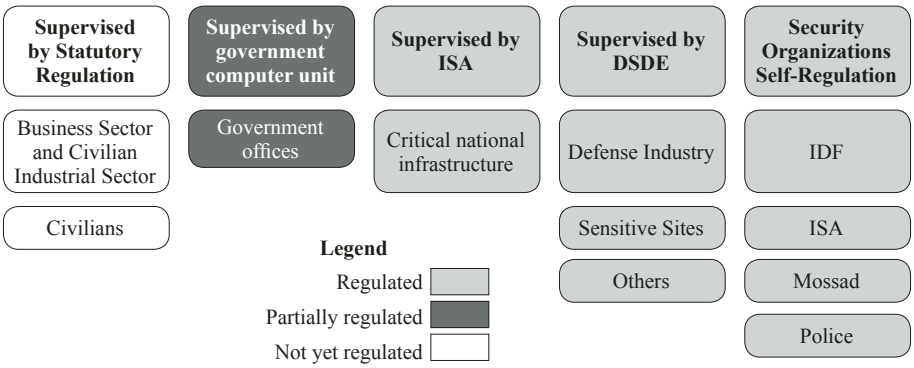

Figure 7: Regulatory Status of Organizations in Israel

The organizational structure and entities responsible for cyber defense or that have a role in cyber defense – in one or another division of responsibility – require full regulation. We discuss regulation below, as it relates to security of the civil sector. Based on the description of the transition and changing responsibility for protection in cyberspace, adequate consideration has not been given to threats, their consequences, and the need to formulate a coherent strategy for cyber protection in the broadest sense – including intelligence – with the possibility of kinetic attack and response. In order to implement such a strategy so that the defense will be effective, appropriate work processes and an organizational structure are needed. Until the work processes have been finalized, the structure in Israel stabilized, and government decisions implemented, we should at least ensure an ongoing, thorough, and professional dialogue among all these organizations, at all levels, with an emphasis on work levels. Whether the structure will become stable and a cyber defense authority will be established to protect the entire civilian sector[101] – or in another framework[102] – it is critical that dialogue take place and lead to a structured process for the methodical and rapid treatment of major cyberattacks against Israel.

Israel needs a body that can comprehensively evaluate the status of cyberattacks against the country. This body should formulate a policy in relation to these attacks, and be responsible for providing guidance about cyber protection. It should evaluate the national cyber status, using the organizational reports of CERT/CSOC, reports of Israeli suppliers and open publications, reports of the intelligence community, and data flow from commercial defense and intelligence companies. It should provide

protection against a broad attack on a variety of targets in Israel. This entity should determine the following: a strategy according to which the supervised organizations operate; a series of tools and products that all organizations should be required to install in order to implement the strategy; the commercial defense and intelligence organizations that will provide intelligence on internet threats; the types of intelligence transferred from the intelligence community to the supervised organizations; and ensuring that information transfer is anchored in law. In addition, the supervising entity should have a broad reporting obligation, which includes information on every attack attempt; development of handling methods; and successful experiments with new tools for protection. Sharing information among the supervised organizations is critical. The desired dialogue is direct, of the type managed directly between the organizational CERT/CSOC at all times (certainly among organizations in the same sector), while informing the sector's regulator and/or the national CERT center. The information to be shared must be broad and varied, starting with data on attack attempts in real time, findings of investigation of tools found at the time of attack, and new methods and tools for protection. Reporting on damages of the attack can be sent only to the regulator, if it exists, or to the national supervising entity and the national center for cyber defense management, due to the commercial sensitivity of such reporting, and this is beyond the report required by law from public and government companies today. Transparency and cooperation must be anchored in law, but more importantly – they must be part of training, and founded upon the understanding that only cooperation based on transparent reporting can significantly support the asymmetric battle of the defender against the attacker in cyberspace.

Although a decision has already been made to establish a national authority for cyber defense, the difficulty of separating the physical space from cyberspace raises the need to create a unified framework for defense against security threats. The distribution of threats in cyberspace and the assailants' ability to identify weaknesses and act accordingly require an extensive examination of current national security. The state's exposure to cyberattacks stems not only from the exposure of computer systems to internet threats, but also from a broad range of breaches. In order to comprehend what takes place in cyberspace, an integrative status report must be produced about attacks both in the national cyber and physical space. Israel's attackers do not differentiate between these spaces; rather, they create an integrated system

between them. Therefore, the defender must avoid artificially separating the defense of these two spaces, which can cause harm.[103] For this reason, we suggest that the cyber defense system be part of the ISA. Every broad attack or APT attack – both for the purposes of stealing information and spying and for purposes of destruction – is a security issue, and therefore the defense system must be under the responsibility of a security entity. In addition, defense requires examination and research of databases located in Israeli cyberspace, and sometimes even of details and content. The only security entity authorized by law to implement such activity among Israeli citizens is the ISA, in addition to the Israel Police, which is entrusted with investigating cybercrime.

The proposal approved by the Israel government allows the specialized government entities in the field of cyber defense to continue operating, but mandates the creation of a central authority for directing and managing cyber protection. At present in Israel, when more than one entity deals with the issue, a continuous, overt, and transparent dialogue needs to be managed among the supervising entities. In addition, organizing activity in cyberspace requires regulation within the context of the division between the security and criminal threats. Significant cyber activity is criminal, and the entities responsible for cybercrime are the various law enforcement agencies, including the Israel Police, the tax authority, the securities authority, and other relevant organizations. Figure 8 depicts the organizational responsibility proposed in Israel's cyberspace.

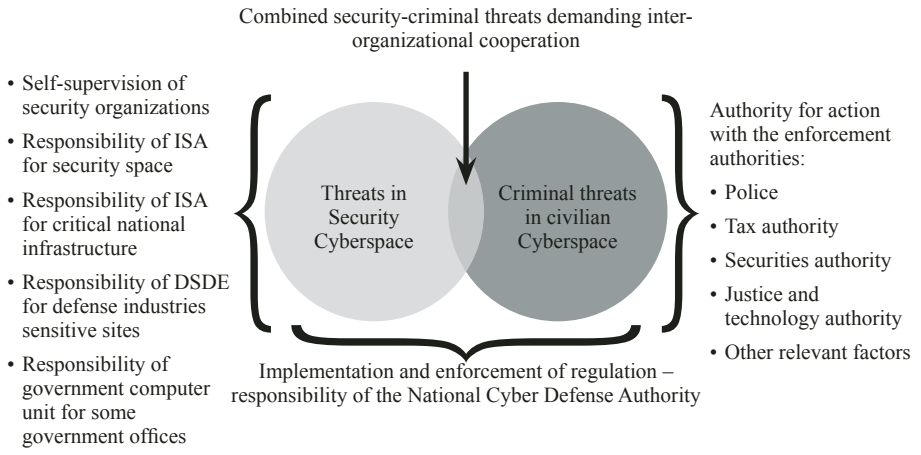

Figure 8: Proposed Responsibility for Operation in Cyberspace

The National Cyber Defense Authority will be required to act as the national regulatory entity, which will supervise civilian cyberspace, including the business sector and the other entities operating in this space. We propose differentiating between these spaces, enabling the defense entities to concentrate on the threats to Israel's security, and the enforcement authorities to focus on the criminal threats to civilian cyberspace. At the same time, infrastructure for inter-organizational cooperation must be constructed for cases where the threat traverses the two spaces. One example is when a cybercrime organization sets goals that are political as well as terrorist.[104] The Israel Police and other enforcement authorities will formulate the strategy for action in the civilian space so that they can cope efficiently with crimes such as cyber fraud, fraud in securities commerce, intellectual property theft, business espionage, internet pedophilia, and the sale of prohibited substances.

Regulation in National Cyberspace

The national cyberspace also includes organizations and businesses that if harmed, could cause damage to the economy and even national security. The fragility of the civilian environment demands an appropriate response. One of the tools that can improve defense of the civilian space is regulation in the field of cyber security. The main points of the proposal for improving the situation described below are to include the cyber defense field as a structured component of existing statutory processes, at the stages of establishing new business initiatives (authorization in the various planning committees) and in their operational processes (business licensing law).[105]

The establishment of any business initiative in the State of Israel requires compliance with statutory planning processes, and the entrepreneur must obtain the authorization of planning committees for a number of areas, including fire and rescue services, public health, environmental protection, dangerous materials, and home-front protection. We propose that within this framework, every entrepreneur be required to relate to the relevant cyber defense issue through a survey or report. This document will serve as the main tool for determining the exposure of new initiatives to the possibility of cyberattack, and for formulating defense against this likelihood. In addition to new initiatives, we also propose using the business licensing process, which requires periodic renewal, to ensure that the business' activity over time meets obligatory criteria in various fields, including protection and

defense against cyberattack. In this manner, the regulator will have another tool for legal control.

From a statutory point of view, the survey or report must be comprehensive, and must apply to all applicants, unless an exemption is given by the authorized entity. But from a practical point of view, standards need to be determined. These standards can relate to a number of components, such as the size of the initiative or the sector to which is belongs, such as energy, food, medicine, or transportation. Once it is decided that the entity must present a cyber survey, the process will function according to the following milestones: 1) Directives: the regulatory entity will be responsible for preparing directives for implementing the above-mentioned survey; 2) Preparation: the survey will be prepared under the responsibility and funding of the entrepreneur, through authorized consultants; 3) Inspection: the regulator will be responsible for inspection, using external consultants who will be trained and authorized for checking the surveys; 4) Authorization: the regulator will examine and authorize the response and will also determine whether the initiative will continue to receive guidance.

As for the identity of the regulator in the cyber field, two options exist. The first is to establish regulation by sector, with the regulator from the relevant sectors. For example, regulation in the field of cyber defense of the health system will be determined by the Ministry of Health; regulation of water corporations will be determined by the Ministry of Infrastructure; and so forth. The other option is regulation through a central regulator, based in the cyber bureau and the National Defense Authority still to be established. Due to the technological complexity of the defense means and the need to preserve a uniform level of security, as well as the concern that sectorial regulation may create a "Tower of Babel" of security instructions throughout the various sectors, the most efficient manner is to determine a uniform professional framework for defense in the civilian sector. This would be similar to other central regulators such as the Fire and Rescue Services, Home-Front Command, and storage of dangerous substances.

Professionalism of Employees and Responsibility of Business Managers

In order to operate a multi-layered defense system in an efficient and comprehensive manner, professional employees are needed, especially those with high-level technical knowledge and skills. The knowledge to be embedded in the systems must be the result of professional analysis and

comprehension of the employees who occupy positions of monitoring and forensic analysis (in places where it exists). Such employees require constant training, professional updates, engagement in inter-organizational dialogue, participation in conferences, continuing education, and above all – training. Skill is acquired partially through daily work. They acquire an organized and broad process of learning from errors, assimilation of knowledge acquired in other locations, and more comprehensive skill through practice and exercise. We propose that all employees in the defense system of an organization, a sector, and of the state benefit from continuous learning through every possible method, and above all, that they receive periodic training with updated insights and more advanced work concepts. Israel has companies that train workers in cyber defense systems to identify and react to warnings correctly (from a professional viewpoint and according to the organization's policy). Their decisions can determine the path for handling the warning. As this decision can be fateful for the attacked organization, investment in this area is critical.

The one responsible for an organization's cyber defense, the Chief Information Security Officer (CISO), is the organization's highest professional decision-maker who recommends the necessary steps in defense processes beyond the everyday handling of warnings. Clearly, the person occupying this position must have a high level of professionalism. He must have managerial skills and leadership determined by the pace of work and changes in the field, by managing employees at a high professional level, and by pressure in cases of serious attacks. He must also exhibit patience and level-headedness, due to false alarms and "noise" that the security system creates. At the same time, and more importantly, the CISO in an organization must be task-oriented, and must constantly consider his organization's weaknesses and methods of handling them. This individual must focus on the nature of attacks – the unidentified breach and in what creative way the attack will arrive – and less on the issue of the visibility of defense, adherence to rules, and proving that he operated in a reasonable manner when an attack is discovered. For example, such an officer must initiate regular penetration tests by an internal staff, if one exists, or by external staff, who have unique ways of thinking and can reveal the weaknesses of his organization's IT system. He must train himself and his staff to function in situations when an attack is discovered inside the organization's network, and when restraint, professionality, and patience are required in order to respond in a sophisticated and successful

manner to thwart the assailant's goal, not just the attack itself. A CISO with such a demeanor can make the difference between a successful attack and one that is foiled.[106]

The managers of organizations must view investing in cyber security as an integral part of their organizational infrastructure and as an essential professional ability, upon which the organization is dependent. The cyber defense of an organization is the responsibility of the manager no less than making profits, initiating new business deals, and finding ways to grow the company. The issue of defending information and computer support of work processes in the organization must be part of the character of the organization, not a topic for technological, tactical management by the IT manager or a cyber security manager. One of the major difficulties of managers of companies and organizations is that the resources and investments required by a cyber security system are problematic; they are comparable to investment in the defense budget. In a speech given at the INSS yearly conference, David Brodet attempted to explain the difficulty in measuring the benefit of investing in a defense budget. Such a budget is designed "to prevent an incident so that it will not actually happen in the future" and for which "the probability of occurrence is an unknown."[107] Similarly, investment in cyber security is supposed to prevent an attack so that they will not happen in the future, even though it is not at all clear that such an incident is about to occur. This investment does not have direct and immediate profit, and not even anticipated profit in the future. It is only likely to prevent a possible and uncertain "disaster" to the organization. Despite this recognized difficulty, managers must invest in cyber security with the intention to prevent a future attack from achieving its goals. This target is neither intuitively evident nor clear to all managers. Sometimes, we have the feeling that managers act in order to fulfill their duty and show that they have acted in a reasonable manner when a harmful attack is discovered. The actions of managers in the cyber security field who are not fully committed to preventing an attack from achieving its goal have an impact upon the other employees in the field, and are highly likely to cause the cyber defense to fail.

Summary

The discussion of the proposed principles for a cyber defense strategy for Israel began with a description of an integrated defense system against APT attacks. This type of attack is the most disruptive to defense systems around

the world. It is challenging and constantly being renewed, and if successful, it can cause severe damage to the organization it attacks. In our evaluation, developing technology in cyber security offers new, creative possibilities for defense, and with proper management, can lead to "turning the tables," by monitoring, analyzing, and reacting to the attack in a sophisticated manner and preventing the attack from achieving its goals – sometimes without the assailant even being aware. Although an important part of the integrated defense system is the ability to identify an attack without prior intelligence, we recommend trying to obtain intelligence of every type and from every source. Intelligence can help significantly in confronting all kinds of cyberattacks. Intelligence is available for attacks that demonstrate a declared ideological position.[108] Other intelligence is based more on infrastructure, focusing on attack tools, characterization of attack groups, and/or attack methods.[109] This intelligence, as well as information from other sources, can facilitate the handling of attacks. We propose integrating intelligence as a component of the defense system, while constantly developing and investing in it, because in the game between attacker and defender, intelligence can locate and foil an attack. We recommend implementing an integrated, graded defense against hardware/firmware attacks, while employing existing methods and tools to defend against rapid, superficial attacks. We propose to implement all of these defense abilities as a directive within the organizations in the state, according to level of importance and indispensability.

An entity whose entire purpose is cyber defense (organizational CERT/CSOC) is needed in order to implement this defense in organizations, in addition to the integrated technological ability. At the state level, an entity must be established to actively supervise implementation of the cyber defense strategy; analyze and determine the state's cyber situation; and manage the policy of response to attacks on organizations that are protected at the national level. Ideally, only one such organization is needed; currently in Israel, the government has given responsibility of this issue to more than one entity, requiring constant dialogue at all levels among the various supervisory organizations. Beyond regulating the state organizational structure, action must be taken to assimilate a culture of maximum reporting and transparency regarding attacks, defense methods, defense tools, and relevant findings from investigations.

The highest level of professionalism must exist among cyber security system employees in all organizations and at all levels. Professionalization

must be encouraged for cyber security managers in organizations, and they must constantly search for the weak points and breaches in their computer systems, networks, and organizational data with the goal of providing a response. Managers must be encouraged to view the issue of cyber security as a significant area of their responsibility; and should invest the necessary resources in order to implement effective cyber security.

Attack

Cyberspace attacks have various motivations, executors, and objectives. We have detailed above the three known types of attacks (CNA, CNE, and CNI). These attacks are executed by various entities, states, non-governmental groups, and individuals. Some of the attacks are carried out by hired assailants, mainly when the state does not wish to be associated with the attacks.[110] Motivations for all types of attacks can be ideological, criminal (mostly monetary theft), commercial or technological theft (of commercial secrets, patents, information protected under inventors' rights), espionage (theft of state secrets), embedded in power struggles or policy realization. Cyberattacks are part of a plan for a state to gain interests. Yet there is no evidence that a state has ever realized its interest through only cyberattacks. Still, we should note that no state has taken credit for a cyberattack, and has been able to measure the attack's success.

We may differentiate between the three states of attack – overt, hazy, and covert. In the overt state, the attack is identified and known, and a state/organization has formally accepted responsibility, or else legal proof of responsibility is present. In the "hazy" state, the attack is identified and known, but no entity has formally accepted responsibility, although sometimes we may guess or assume the identity of the perpetrator. The attacker hopes that investigation, if carried out, will not lead to legal proof of the state's responsibility for the attack. In the "covert" state, the attack is hidden, so that the victim (and preferably, all others except the assailant) is unaware of it. As soon as the attack is identified and known to the attacker or other entities (whether publicized or not), it moves to "hazy" status, even without any clear assessment of the identity of a responsible state.

Because we view cyberspace as a direct continuation and inseparable part of the kinetic world, a state's cyberattack targets are as broad as its interests, and represent only part of a broad range of operations intended to achieve its goals. Cyberattack can empower and leverage kinetic effects, and

thus contribute to limiting the duration of the battle or clarifying its result. Of course, cyberattack does not replace physical battle; in the immediately foreseeable future, achieving battle objectives through cyber activity alone is unrealistic.

Overt and Hazy Cyberattacks

In order to consolidate guidelines for Israel's cyber strategy, we must understand how this field is perceived and implemented by states around the world. For this purpose, we may focus on several points in the American concept, and on a number of conclusions from the cyber battle between Russia and Georgia in 2008. A state's cyberattack as part of an overt, declared conflict is designed to aid in achieving an objective or clarifying a result, and it must be part of an overall plan for security, politics, economy, public consciousness and morale, or a combination of these.

Cyberattack as part of an overt, declared battle can be characterized by CNA, CNE, or CNI attacks, and they can be overt, hazy, or covert attacks. From the public dialogue in the United States, we learn that a cyberattack can serve as the rationale for a US counterattack either in cyberspace or in the kinetic space. The Americans view cyberspace as an operational space just like the other four spaces, and do not limit themselves to operating only in cyberspace. American involvement in a conflict can also be expressed only by their cyberspace activity. Clearly, in order to establish such a strategy, the state must form a preliminary force whose purpose is to build attack ability in cyberspace.[111]

For this reason, the US Department of Defense systematically has organized to implement cyberattack operations as an integral part of its warfare theory. The survey above demonstrates that the United States perceives cyber defense and offense as an integral part of the commander's toolbox. The commander will manage and maneuver cyberspace just as ground forces are maneuvered in an integrated manner and with a broad concept of applying force.[112] The Obama administration is reputed to have tested the ability of a cyberattack to solve the issue of Syrian air force attacks on civilians during the Syrian civil war without accompanying military activity. The test concluded that such an achievement is not possible through cyberattack alone.[113] Similarly, the establishment of the cyber arm planned for the IDF also underlines the understanding that cyberattack abilities must be integrated into the toolbox of the Israeli commander, as well as into the IDF's operational plans.

As of this writing, there is no evidence that the United States has used cyber warfare as part of an overall systemic conflict. On the contrary, the evidence points toward avoiding the use of cyberattack. Examples are the Syrian case noted above, and the United States' refraining from a cyberattack, which was intended to destroy Saddam Hussein's economic power on the eve of the 2003 invasion of Iraq and prevent him from funding the battle and paying his armed forces. Such an event (assuming it took place in this manner) reflects the US position of self-deterrence regarding the use of cyberattack as part of warfare. The basis of this fear is the indirect consequences for entities other than the attack target and the inability to meet international legal standards, mainly the principle of proportionality.[114]

An example of implementing a cyberattack during an overt conflict is the cyberattack against Georgia in the August 2008 war with Russia, described above. The core of the attacks were DDoS and defacing operations. The attacks targeted Georgian news sites and government offices. Executed in batches over several hours' duration, the attacks were effective in integrating kinetic and electronic operations to paralyze the Georgian communications system. As a result, the Georgian government's communications with its citizens and the world was significantly disrupted, and the Georgian central bank halted electronic trade. The perpetrators of the attacks focused on their objective – to significantly disrupt Georgian communications – and were knowledgeable of their methods, as the August attack was preceded by earlier attacks on the same sites. The Georgians realized that they were under cyberattack and tried to defend themselves. They blocked internet communications entering from Russia to prevent attacks and propaganda. When the Georgian government tried to receive service from infrastructure companies in various countries, this infrastructure was attacked as well, including that of an American provider. The attacks were attributed to informal groups, crime organizations, and mercenary cyberattack groups, with most of the cyberattacks originating from sites in Europe and the United States. Still, the timing of the cyberattack on August 8, together with the invasion of Russian forces into Georgia, raises the possible connection between the assailants and the Russian establishment, although it cannot be proved. Even in the absence of such a connection, and even if we attribute responsibility to citizens acting out of ideological motivations, the phenomenon of informal entities easily and effectively interfering with a military conflict is impressive.[115]

Similar to strategies in several countries, especially the United States, Israel's national strategy in the cyber field should include a combination of cyberattack efforts in all relevant systems, together with kinetic efforts. To do so, we will be required to internalize the international law that will apply to cyberspace. The assumption is that the laws of conventional warfare will also be valid in cyberspace, and those who work in the field of cyberattack will be required to meet these demands.[116]

Attack as a Means of Delivering a Message

An overt conflict between two sides does not obligate direct kinetic conflict between them. "Dialogue" between two sides exists in various forms, and cyber tools can serve as a "language" in a conflict. Such activity will be defined as an attack for purposes of influence (CNI). One example is the August 2012 attack against the Saudi company Aramco and RasGas of Qatar. The Aramco attack destroyed data in some 30,000 company computers. At the time, senior US officials attributed this attack to Iran.[117] We may assume that the purpose of the attack was to deliver a message of warning to the United States regarding sanctions against Iran.

Another possible example is the conflict between the United States and North Korea. North Korea carried out a cyberattack against the Sony network as part of a battle designed to prevent the screening of a feature film about the North Korean leader. The cyberattack was accompanied by threats of terror attacks against movie theater chains, with the goal of preventing the screening. Sony Pictures initially capitulated under pressure, but eventually permitted the screening after the American government intervened and asked it to stand firm. The incident ended after the United States apparently initiated a cyberattack response, during which North Korea was cut off from the internet.[118] This incident can be seen as an inter-state "dialogue" that takes place in cyber language and is part of an overall, broader battle.

From the descriptions above, several conclusions may be drawn and used as guidelines for formulating an attack strategy:

1. Cyberattack ability should not stand alone, but rather should be part of a general plan in order to influence a comprehensive, overt conflict.
2. If integrated within a general plan, an effective cyberattack may be implemented against a focused target – such as disrupting a government's communications as in the Georgian case – through a superficial, rapid,

broad attack of objectives other than "gold targets" (military targets, state infrastructure).

3. An effective attack need not be a sophisticated ATP. In the above incident, DDoS and Defacing attacks achieved their objectives. A cyberattack can significantly harm a target that is not "cyber rich" and technologically developed. Furthermore, a highly developed technological state may be more vulnerable to cyberattack than an underdeveloped one because it has fewer defense abilities.[119]
4. A state can implement effective cyberattacks through proxies without taking responsibility as part of an overt war, while the state accepts responsibility for the kinetic aspect. Cyberattack requires build-up of force, knowing the target, and advance planning.
5. A cyberattack can serve as a layer in inter-state dialogue, with the goal of the attack being to send a message, usually a warning.

Attack as Part of a Covert Campaign

A covert campaign is a conflict using hidden means; use of these means and responsibility for the results – if they are discovered – can be denied. A state wages a covert campaign with the goal of achieving interests or preserving them. In handling central, complex issues, states can act through overt as well as covert campaigns, which help manage overt aspects of the campaign, and contribute to achieving the goal (for example, theft of information/ espionage). Naturally, no proven examples exist of covert cyber operation, mainly because no group will assume formal responsibility for such attacks even after being exposed. For the purpose of illustrating a covert attack and formulating a strategy recommendation in this field, we can rely on analysis of the most well-known example of a covert cyber operation – the Stuxnet attack on the Iranian nuclear facilities at Natanz.[120] As mentioned above in the literature survey, Langner's analysis points to a two-pronged attack. The first part of the attack was covert, and its method of implementation was intended to achieve a focused goal.[121] During the attack, a decision was made to switch from this operational tactic of mass and immediate destruction of the centrifuge system to one designed to disrupt a large number of centrifuges, even at the price of exposing the attack.[122] To introduce the malware into the relevant computers, Langner describes the possible use of contractors who were connected to the Natanz system.[123] In addition to the damage that the malware was to cause at Natanz, Langner describes

the attack as designed to obtain information. The fact that Stuxnet skipped over to additional systems enabled the attackers to test these systems for information on Natanz contractors, and possibly even connection to Iran's secret nuclear facilities.[124]

In Langner's analysis, the covert attack identified the weak points in the target's system in order to circumvent defense mechanisms and penetrate the relevant computers, using the example of exploiting the supply chain. According to Langner, the attack's objective was destructive, and this determined its tactics as exemplified in the differences between the first and second versions of Stuxnet. Furthermore an attack for destructive purposes can be exploited in order to gather information. Changing objectives in the middle of a covert attack is a process that can lead to changing attack tools and tactics, as Langner relates regarding the change in Stuxnet's objective. Even after discovery, the attacker must avoid proof of connection to the attack, particularly legal proof. In this case, the attack is attributed to the United States, and sometimes to a joint US-Israel operation, but there is no real proof connecting the attack to these countries.

Summary

Cyberattack as a tool in the service of the state forms part of a wider battle, and does not stand alone. Cyberattack ability is an additional way in which the state acts to achieve its objectives and preserve its interests. The main recommendation is to assimilate cyberattack in all programs and levels as a supporting tool, as part of a broader program for the state to achieve its objectives. The table below presents a summary of the entire issue of attack:

	Overt Conflict	Covert Conflict
Type of attack	Overt or hazy (including use of proxy) All types of attacks are relevant: short and superficial, APT, hardware/ firmware prepared in advance	Covert, and after discovery – hazy. Relevant types of attack: APT, hardware/firmware
Types of objective	Targeted (military/ government) or civilian	Targeted (military/ government) or civilian
Desired achievement	Collection / influence (including delivering messages) / destruction	Collection and destruction
Status	Part of battle	Part of battle
Attributes	Immediate, overt results (of influence and destruction attacks); possibility of achieving overt cyber conflict in real time; reaction can be in the kinetic plane; can serve as an additional language for delivering messages between rivals	Results depend on planning and do not always appear immediately at full strength

Insights and Recommendations

The discussion of formulating a strategy for Israel's conduct in cyberspace is no different in substance than determining a state strategy in any other field. The desired objective must be defined, and a plan must guide the manner in which it is achieved. Defining strategy is always challenging and complex, and in Israel it is sometimes even more complex given the tendency to respond to a specific situation, and then define that response as strategy. The discussion of cyberspace involves several additional complex challenges. First, the rules of cyberspace conduct have not yet been formulated in the system of global relationships. Therefore, every state attempts to cloak its strategy in a secretive shroud, particularly for attack, and to maintain deniability. An additional challenge is that the nucleus of cyberspace activity is technological. Technological ability is what enables a state to formulate a strategic plan for cyberspace and achieve the state's objectives. This technology is constantly being developed and aggressively promoted, although only a small percentage of the technology has been proven effective. Paradoxically, the latest technology designed to solve gaps in cyberspace defense ability has not yet demonstrated maturity. Therefore, the proposed strategy must be based on promising technological concepts and directions, even if they have not yet reached the status of established solutions. Finally, as in every new and developing field that is both essential and rich in resources, organizations struggle over responsibility, authority, and mainly, control of resources. The tendency to handle the organizational issue at the state level is understandable, but this process is like putting the cart before the horse. Ideally, a state should first determine objectives, plans, tactics for implementation, and a culture for operation in cyberspace; only then can it adapt the organizational structure to the plan as well as to the work processes so the strategy can be implemented. Lacking the proper order for action, we had to relate to the organizational reality in Israel – that the

government has already decided upon – as a constraint – and we have tried to recommend how Israel should act within this framework.

For any state, the formulation of strategy in the cyber field begins with defense. The main challenge today is the state's ability to protect its property and civilians from damage that begins in cyber operation, but has kinetic consequences that are even more destructive. States fear espionage and the theft of large amounts of secret information stored today in national computer systems. This fear is not new, but cyberspace greatly exacerbates it. In addition, cyberattack can harm states in areas essential to their existence – this is a new field, not entirely understood and therefore very frightening. States are awakening to the new reality of cyberattack that could impair a state's energy systems or paralyze the monetary system. Furthermore, preemptive cyber activity may damage military capabilities. These fears, in addition to the structural advantage possessed by the assailant and the constantly improved quality of attacks, have led to the need to determine an effective solution for the challenge of defending cyberspace at both the level of concept and operational methods, as well as at the technological level.

Main Recommendations

The State of Israel must implement both defensive and offensive activity in cyberspace. The goal of the strategy we propose is to enable this activity so that it will achieve the objectives when needed, and protect state property at a relatively high security level over time. This document has analyzed various components and has provided recommendations for operation of aspects of Israel's defense and offense in cyberspace. In addition, we will emphasize additional angles of some of the fundamental components that form the foundations of the national strategy, upon which the recommended directions of operation are based.

Recommendations for Defense

Use of technology for defense

The technological system used should integrate a number of appropriate methodologies, and defense tools. We propose utilizing the relative advantage of Israeli industry in the field, and to examine the integration and assimilation of new defense tools in the organizational defense system in an easy, positive, and persistent manner. A large number of organizations

in the relevant industry in Israel and globally should hold regular dialogue for continued, organized analysis of products.

Choosing the right response for defense
We recommend formulating an approach based on active defense. This process begins with preventing immediate attack by means of technological disruption, followed by containing the attack and implementing deception, which not only prevents the attacker from achieving his objective, but also will prevent him from realizing that he has been discovered, at least until a very late stage.

International and internal cooperation
We recommend implementing and expanding cooperation at all levels for the purposes of cyber defense, both between Israel and friendly nations, and within Israel – between the government and private sectors. In addition, we recommend that Israel broaden its activity in relevant international forums.

The Attack Field
We propose making cyberattack an integral part of plans for achieving national objectives and preserving national interests. We must act to implement cyberattack only in consideration of a defined objective. Regarding integration between offensive and defensive attack, we propose integrating "attackers" within Israel's central defense system for the purpose of planning and everyday operation of the defense system.

The Organizational Field
Integration of cyberspace and kinetic space
We propose that cyberspace be viewed as part of the physical, real life in kinetic space, instead of as a space on its own. This concept should be implemented in relevant decisions, such as the state's organizational structure for handling the cyber issue, or in issues regarding methods of operation in cyberspace.

People and nature of the mission
For individuals in cyber occupations (even the auto-didactic ones), we recommend continuous professional training and in computer science, and regular practice and drills. We also recommend training the managers of

cyber organizations to choose the proper combination of expertise for their group, and to formulate the appropriate nature of the mission.

Connection between government organizations and cyber industry in Israel
Israel's national organizations operating in cyberspace should be cognizant of new directions of thinking and development, at least those existing in the Israeli cyber industry. To achieve this, we recommend implementing bi-directional transfer of information in a careful and controlled manner between state organizations and civil groups representing the public/private market in Israel. The bi-directional relationship should be grounded in law, without harm to the state's security and intelligence sources, and with minimal detriment to individual's rights to privacy.

Organizational structure

A single entity should have responsibility for managing the entire system of national cyber defense. In every sector and government organization or group working with government organizations, we must ensure that an organizational body is responsible for cyber activity. This body will be under the supervision of the central government's organization responsible for cyber defense, and will be required to report every incident or new development in the field. Because cyberspace must be part of managing any kinetic battle, and because the character of defense in cyberspace is primarily security-related, we recommend that a security organization be responsible for cyber defense on behalf of the state.

Israel's informal mode of operation
Israel's informal mode of operation has a place in cyberspace as well. Broad social networks, a culture of social interaction, a willingness to help, an interest in activities of national importance, the desire to be at the center of things, and to prove personal and professional relevance enable large numbers of individuals to be recruited when needed, whether to help friends or for a national purpose, and certainly in a situation that combines these two reasons. This informal activity is almost constant, and we can rely on it in many cases when needed. Because it is voluntary, based on goodwill, and anchored in Israeli culture, it is stronger and sometimes of higher quality than cooperation deriving from structural, legal, or procedural obligation. It enables ad-hoc cooperation; recruitment of high-quality professionals from various fields; streamlined and open channels for information transfer;

efficient problem-solving; and the ability to surmount challenges, which in ordinary circumstances would be time-consuming and might not even be resolved. Operating in Israel can mean either finding creative, rapid, and real solutions through informal channels and reliance on flexible interpretations of law and rules; or a sluggish process of foot-dragging that might not even produce solutions, even though it is based on clear definitions of law, procedure, and organizational responsibility.

We therefore propose formulating laws and procedures, defining organizational and structural responsibility, forming flowcharts and work procedures, while simultaneously enabling this informal activity to continue. Such activity should exist alongside the rules and procedures. Leaders should not hesitate to take advantage of it in times of need or distress, even when not fully congruent with rules, organizational structure, and formal responsibility.

Conclusion

Although addressed here, a number of issues in the field of cyber operations still remain undeveloped and insufficiently treated. These issues have been applied to cyber activity using a system of terms and conduct originating in and defined by the kinetic world. These issues are presently being redefined and adapted to the cyber world. Some are legal – such as how to prove legal responsibility for damage caused by cyber activity. Others are ethical – such as whether it is right to implement a cyberattack when it cannot be restricted only to its defined target, and may affect other targets, and thereby damage civilian systems and endanger lives. In addition, civil issues address the question of how to defend citizens' right to privacy, when authorities need information about civilians in order to protect them.

As for approaches to deterrence, the question arises as to whether states, organizations, or individuals can be deterred from hostile cyber activity to a state, or to private entities and individuals within it? Should deterrence remain solely in the cyber field, or can kinetic tools be used against cyberattacks? The issue of recovery from attack (namely, national cyber resilience) relates to tactics for recovery, as well as to these questions: can we make an equal comparison between recovery from natural disasters such as earthquakes, fires, or incidents caused by humans, and recovery from cyberattacks? What role should the state take in such recovery? This document has addressed such questions, but because they are still incipient, at least partially, we cannot always offer a clear recommendation for how Israel should act with regard to these issues. We must allow these issues to develop, while we gain some experience and engage in thinking about these matters before we can define conclusive policy in these fields.

Another point that deserves attention is the transparency required in organizations, sectors, and states for their cyber defense systems. Naturally, organizations tend to hide their weak points or potentially harmful issues. For this reason, they have a tendency to avoid reporting cyberattacks – or at

least to refrain from giving the necessary detail. This is particularly true for organizations that operate with a high level of trust; without, they would face the danger of collapse and closure. A primary example of this is the banking system. Account information must remain between bank and customer alone – this is the entire basis for the client's trust in the bank, and the fundamental reason for his willingness to deposit his financial assets there. The revelation that a foreign entity penetrated the bank system and operated within it, and that the bank failed to react in a timely manner and to protect information will cause the clients to feel that their money is insecure. This will make the collapse of the bank, and even the entire banking system a real and tangible risk. Even if the bank understands this risk, the ability to engage in active defense requires the bank to quickly share details of the attack and the damage caused in a transparent manner. In sensitive sectors such as the monetary system, reporting and transparency may need to be limited to individuals in relevant positions, the regulator, and bodies responsible for cyber defense in Israel, and not made available to the entire public. Either way, reporting and transparency are clearly essential. Implementing this principle is the basis for quality cyber defense.

Alongside the process of formulating strategy in cyberspace, we must relate to critical support tools for implementing this strategy. These tools include building a relative technological advantage and maintaining it over time; an organized and agreed-upon work process; positive, professional, and regular dialogue among all national entities addressing cyber defense, and between these entities and the objects of defense; professional cooperation between government and external entities such as Israel's civil cyber industry, government entities of allied states – subject to national interests – and the global cyber industry, as needed; and finally, adapting Israeli law as required for effective defense, along with high-level legal support in the field of international law.

Israel is unique on two points, and this uniqueness is worth preserving. One characteristic, which is well-known and has served as a relative advantage for a long time, is that Israel is highly skilled in invention and initiative, particularly in the high-tech industry, on which cyberspace is based. Most Israeli startups that are developing products for cyberspace offer impressive ideas, providing creative responses with substantial potential for surprising, innovative solutions for cyber issues. Israel has a real need to maintain and expand this relative advantage, primarily through continued formal training

of a talented population, as well as through continued private and public investment in the Israeli high-tech market. The second point is the ability of Israeli society to create ad-hoc solutions for challenges. Because social networking has a strong basis for activity in Israel, abilities, products, and operational methods can be connected within a short time and in an informal manner in order to create real solutions for challenges in the cyber field. This reality, which may appear chaotic at times, enables rapid response, circumvents bureaucratic obstructions, and overcomes a lack of legal definitions or excessive definitions of authority and organizational struggles. This advantage, which is an integral part of Israeli culture, must be preserved, alongside the need to implement proper conduct that is institutionalized and based on legal principles.

In order to harness all interested parties into synchronized, synergetic operation, a large portion of the strategy formulated should be open to the public, who should be able to access and employ relevant sections. Of course, such a document should also have classified sections, addressing topics better left unmentioned, which will aid in coordination and synchronization among all defense organizations operating in Israel. This synchronization is an essential and achievable goal that can establish Israel's position as a global leader in the field of cyber activity.

Appendix: Glossary of Terms

Term	Meaning
General	
Strategy	Basic components in the plan for achieving state objectives, while harnessing national resources in order to attain targets for action in cyberspace. The terms "operation" and "tactics," which mainly appear along with "strategy," detail the concrete manner of operation (each space at its own level), the method, and the means of implementing the strategy for cyberspace operation.
Cyberspace	The physical and non-physical area created or comprised of part or all of the following factors: mechanized and computerized systems, computer and communications networks, software computerized information, content transferred in a computerized manner, data on traffic and control, and the users of these.
Cyberattack	Illegal penetration, mostly covert, of a computer, computer network, or any device connected to a network controlled by computer for various purposes. Attacks are divided by goal, type, method of attack, and sometimes by attack tool.
Cyber defense	Preventing the attacker from attaining the objective in cyberspace. This does not necessarily mean preventing the attacker from reaching the computers or network.
Goals of cyberattack	
CNE – Computer Network Exploitation	Attack for purposes of exploiting the information on the computer/network and the information stored in the computer/network.
CNA – Computer Network Attack	Attack for purposes of destruction. The expression of destruction will be in the kinetic world (for example – deleting essential information, turning off electricity, stopping water flow, disrupting weapons systems).
CNI - Computer Network Influence	Attack for purposes of psychological influence, hurting morale, influencing public awareness.

Term	Meaning
Main types of attack	
DDoS – Distributed Denial of Service	Flooding a service provider site with a large amount of false queries, in such a way that blocks it and causes it to collapse, thus preventing service to users.
Defacing / change of appearance	Changing a site's appearance and embedding messages that serve the attacker.
Advanced Persistent Threat - APT	Usually covert, sophisticated attack for the purpose of remaining as long as possible in the depth of a system or computer network, mostly for the purposes of collecting information and espionage, sometimes as a phase before an attack for purposes of destruction.
Tools and methods of attack	
Malware, malicious software	Software / code used by an unauthorized / illegal user of the computer, for any purpose.
Zero-day attack	Attack that exploits a weakness / software breach that is known to the attacker but unknown to the defender, to intelligence and defense companies, and to the software manufacturer.
Trojan horse	Damaging code / program that attempts to penetrate a computer through camouflage of a harmless program.
Back door	Code granting the attacker permission to enter a computer at a distance.
Botnet	Network of software agents installed in a computer (usually without the knowledge of the computer owner) in order to exploit a network's computer resources for shared performance of a task, based on a legal software system installed in them. In the cyberattack context, this term relates to illegal and covert overpowering of a computer from a distance, and using it to perform tasks that the attacker defines.
Phishing	Illegal attempt to obtain information from a computer, such as username, password, or other identification details about people. Usually, the attempt is based on email communications, instant messaging, or social networks (e.g., Facebook), and refers the user to a site that seems trustworthy and sometimes familiar.
Hardware / firmware attacks	Attacks based on changes in hardware (usually at the manufacturing stage) or changes in the software located in hardware components for the purpose of preliminary / basic use of the computer.

Term	Meaning
Types of cyber defense	
Defense based on prior information / intelligence	Defense against cyberattack in which the attack code is known and recognized, and/or the target and date of attack are known. For example, known, limited malware, such as a known attack code that has been fully or partially identified by a defense system (anti-virus tools are mostly based on such prior knowledge). Another example is defense against service-prevention attack, for which an open warning is given regarding target and date.
Defense independent of prior information / intelligence	Use of technology that is independent of information collection on attack codes or intentions, but is based on the best possible knowledge of the defended environment.
Tools for cyber defense	
Security information and event management - SIEM	A combination of two terms: security information management, meaning information security based on accumulation of data and saving logs of computer operations, deep analysis of them, and professional understanding of events; security event management – management of information security events, relating to the ability to locate, understand, and respond in real time or very close to real time, to cyberattacks on computer networks.
Computer forensic science	Branch of digital scientific investigation that relates to legal evidence (sometimes for purpose of presenting in court) found in a computer or in digital storage methods. The goal is to test digital media using scientific investigation for the purpose of identification, preservation, reconstruction, analysis, and presentation of facts.
Anti-virus	Software designed to identify computer viruses and to protect the computer from their operation.

Notes

1 The term "strategy for cyber activity" refers to achieving the government targets in cyberspace by harnessing government resources to achieve these goals. The terms "operation" and "tactics," which usually appear after "strategy," describe the concrete methods of operation (each field at its own level), and the means of implementing the strategy for conduct in cyberspace.

2 Israel Government Decision no. 3611 of August 7, 2011, http://www.pmo.gov.il/secretary/ govdecisions/2011/pages/des3611.aspx.

3 Nati Cohen, "The Fifth Dimension," *Ma'arachot*, no. 452 (December 2013), p. 10, http://maarachot.idf.il/PDF/FILES/4/113334.pdf.

4 See Guidelines for Government Policy on the Knesset website. These may be summarized under the general definition of security and economic welfare, http://www.knesset.gov.il/docs/heb/coalition2013_3.pdf.

5 Isaac Ben-Israel and Lior Tabanksy, "An Interdisciplinary Look at Security Challenges in the Information Age," *Military and Strategic Affairs* 3, no. 3 (December 2011): 21-37, http://heb.inss.org.il/index.aspx?id=4354&articleid=1126.

6 Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Memorandum, no. 109 (Tel Aviv: Institute for National Security Studies, June 2011), http://heb.inss.org.il/index.aspx?id=4354&articleid=1043.

7 Tyrone C. Marshall Jr., "Cybercom Commander Calls Cybersecurity Order First Step," *DoD News*, February 13, 2013; William J. Lynn III, "Defending a New Domain, The Pentagon's Cyber Strategy," *Foreign Affairs* (September/October 2010), http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain; Claudette Roulo, "Alexander: Laws, Policies Lag Behind Changes in Cyber Threats," *DoDNews*, February 27, 2014.

8 For example, see analysis of the "Red October" attack, Kaspersky Security Bulletin, Kaspersky Lab Global Research and Analysis Team, 2013, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf. See also an example of a characterizing attack trends and analysis based on broad collection, Symantec, "Internet Security Threat Report," vol. 19, 2014, http://www.symantec.com/en/uk/security_response/publications/threatreport.jsp?inid=il_ghp_hero3_istr-2014-V19.

9 Michael Porter, "What is Strategy?" *Harvard Business Review*, November 1996, https://hbr.org/1996/11/what-is-strategy.

10 See, for example, the discussion on legal regularization of NSA activity within the United States, as reflected in the statement of Keith Alexander, commander

of US Cyber Command and director of NSA, before the Senate Armed Services Committee. Alexander is aware of the conflict between cyber defense and the right to privacy, yet believes that these goals may be achieved simultaneously. He asks to receive data without content from internet providers and in return give them classified information on attributes of malware, so that they can find them and report in real time. For details, see *Hearing to receive testimony on U.S. strategic command and U.S. cyber command interview of the defense authorization request for fiscal year 2014 and the future years defense program*, pp. 8-10 (March 12, 2013) (testimony of Keith Alexander, commander of US Cyber Command and director of NSA and C. Robert Kehler, commander of US Strategic Command), http://www.armed-services.senate.gov/imo/media/doc/13-09%20-%203-12-13.pdf.

11 A definition of the term "advanced persistent threat" (APT) appears in the glossary of this document.

12 The actual division in Israel partially fits the proposal suggested here. The discussion on objects of defense in Israel's cyberspace focuses on issues of structure and inter-organizational division of aspects of authority, responsibility, and resources. For details on the objects of defense in Israel's cyberspace, see Roi Goldstein, *Cyberspace and Defense of Essential Infrastructure*, Knesset – Center for Research and Information, May 12, 2013. This document was written for a discussion in the Knesset Committee on Science and Technology on "Promoting Israel as a Leader in the Cyber Field," pp. 6-7, and footnote 19, www.knesset.gov.il/committees/heb/material/data/mada2013-05-13.doc.

13 Following is the text of the Israeli government's decision from August 7, 2011, on establishment of the National Cyber Bureau, centering on the organizational issue: "In consideration of this, following the decision of the Ministerial Committee on National Defense No. 84B of December 11, 2002 (below, Decision 84B), and without detriment to the authority given to another factor according to any government law and decision: To establish a National Cyber Bureau (below, the Bureau) within the Prime Minister's Office, as detailed in Appendix A below. To regularize the responsibility for handling the cyber field, as detailed in Appendix B below. To promote the ability to defend cyberspace in Israel and to promote research and development in the cyber field and super-computing, as detailed in Appendix A. The budget for implementing this decision will be decided by the Prime Minister, in consultation with the Minister of Finance, and will be presented for government authorization two months from the date of this decision. Despite the text of this decision, and to remove any doubt, it is hereby clarified that this decision will not apply to the special organizations, to which special arrangements will apply, as determined by agreement between them and the Bureau no more than 120 days from the date of its establishment." From the website of the Prime Minister of Israel, http://www.pmo.gov.il/secretary/govdecisions/2011/pages/des3611.aspx.

14 Council for Research and Development, "Report of the Council for Research and Development for the years 2010-2011," p. 10, http://most.gov.il/Molmop/Reports/Documents/AnnualReport2010-11.pdf.
15 Ibid., pp. 39-40.
16 Announcement of the chief secretary regarding the prime minister's declaration of September 21, 2014, http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokerashot210914.aspx, and announcement of the Chief Secretary regarding the government's decision on the issue of the "decision-makers' proposal" of February 14, 2015.
17 Even and Siman-Tov, *Cyber Warfare,* pp. 70-73.
18 Ibid., p.70.
19 Gabi Siboni, "Wanted: A National Policy – Force Build-Up in Cyberspace," *Haaretz*, January 2014.
20 US Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011.
21 Ibid., pp. 5-10.
22 Joint Chief of Staffs, "Cyberspace Operations," US Army Joint Publication 3-12, February 5, 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
23 Joint Chief of Staffs, "Cyberspace Operations," Joint Publication 3-13, Information Operations, Chapter II, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
24 Cheryl Pellerin, "Alexander: Defending Against Cyberattacks Requires Collaboration," US Department of Defense, October 30, 2013.
25 After the Snowden affair broke, public debate in the United States centered on the violation of individual rights by the NSA on behalf of defense and security. In this atmosphere, General Alexander was unable to convince others that entities such as the NSA and the Cyber Command should be permitted to receive data on US citizens, even though it was vital to their defense.
26 Pellerin, "Alexander: Defending Against Cyberattacks Requires Collaboration."
27 Cheryl Pellerin, "Cybercom Chief: Cyberspace Operations Key to Future Warfare," US Department of Defense, June 16, 2014.
28 The Department of Defense Cyber Strategy," The Department of Defense, April 2015, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
29 Lynn "Defending a New Domain: The Pentagon's Cyber Strategy."
30 The Federal Bureau of Investigation, "Ten Years after: The FBI since 9/11 – Cyber," http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/cyber-1.
31 "Cyber Security Strategy of the United Kingdom - Safety, Security and Resilience in Cyber Space,"Presented to Parliament by the Prime Minister, by Command of Her Majesty, June 2009, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf.

32 Cabinet Office, "The UK Cyber Security Strategy - Protecting and Promoting the UK in a Digital World," November 2011.
33 Cabinet Office, "The UK Cyber Security Strategy Report on Progress and Forward Plans,"December 2014.
34 French Network and Information Security Agency, "Information Systems Defense and Security – France's Strategy," https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf.
35 Gabi Siboni and Y.R., "What Lies behind Chinese Cyber Warfare," *Military and Strategic Affairs* 4, no. 2 (September 2012): 49-64, http://heb.inss.org.il/index.aspx?id=4354&articleid=1185.
36 OECD, "Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy," 2012, http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.
37 ENISA, "National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace" May 8, 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategiesncsss/cyber-security-strategies-paper.
38 European Commission High Representative of the European Union for Foreign Affairs and Security Policy, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," Brussels, February 7, 2013, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.
39 Amir Averbuch and Gabi Siboni, "The Classic Cyber Defense Methods Have Failed – What Comes Next?" *Military and Strategic Affairs* 5, no. 1 (April 2013): 37-48, http://www.inss.org.il/uploadImages/systemFiles/MASA5-1Eng5_Averbuch%20and%20Siboni.pdf.
40 Isaac Ben-Israel and Lior Tabansky, "An Inter-Disciplinary Look at Security Challenges in the Information Age," *Military and Strategic Affairs* 3, no. 1 (December 2011): 21-37, http://heb.inss.org.il/index.aspx?id=4354&articleid=1126.
41 Ibid.
42 Nati Cohen, "Preparation and Organization of the State of Israel for an Extensive Cyberattack," National Security College, Fortieth graduating class, and the Department of Political Science, Haifa University, May 2013. See also, Nati Cohen, "The Fifth Dimension," *Ma'arachot* 452 (December 2013), p. 15, http://maarachot.idf.il/72194-he/Maarachot.aspx.
43 Cohen, "Fifth Dimension," pp. 15-16.
44 Pierluigi Paganini, "Hardware Attacks, Backdoors and Electronic Component Qualification," InfoSec Institute, October 11, 2013, http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-componentqualification/.
45 Amir Lupovici, "Cyber Strategy and Deterrence: Trends and Challenges in Research," *Military and Strategic Affairs* 3, no. 3 (December 2011): 41-52.

46 Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, November 19, 2013, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin.

47 According to Langner, the goal of the attackers was to cause the Iranians to lack trust in their ability to operate the centrifuge control system – and not to cause mass damage to the centrifuges themselves. Accordingly, the attack was planned to cause lasting damage, not extensive immediate damage, which would signal to the Iranians that the problem was not their technological knowledge, but rather a cyberattack. As Langner wrote, "If catastrophic damage had been caused by Stuxnet that would have been by accident rather than on purpose. The attackers were in a position where they could have broken the victim's neck, but they chose continuous periodical choking instead. Stuxnet is a low-yield weapon with the overall intention of reducing the lifetime of Iran's centrifuges and making the Iranians' fancy control systems appear beyond their understanding." Ibid., p. 7.

48 In Langner's words "The results of the overpressure attack are unknown. Whatever they were, the attackers decided to try something different in 2009. This new Stuxnet variant was almost entirely different from the old one. For one thing, it was much simpler and much less stealthy than its predecessor. It also attacked a completely different component of the Natanz facility: the centrifuge drive system that controls rotor speeds." Ibid, p. 5. Langner also wrote that, "At some point the attacks should have been recognizable by plant floor staff just by the old eardrum . . . It's another sign that the makers of this second Stuxnet variant had decided to accept the risk that the attack would be detected by operators." Ibid., p. 7.

49 Ibid., p. 9.

50 Ibid.

51 James A. Lewis, "In Defense of Stuxnet," *Military and Strategic Affairs* 4, no. 3 (December 2012): 65-76, http://www.inss.org.il/uploadImages/systemFiles/MASA4-3_Lewis.pdf.

52 Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue* 43, no. 1 (February 2012): 3-24, http://sdi.sagepub.com/search/results?fulltext=cyclones+in+cyberspace&submit=yes&journal_set=spsdi&src=selected&andorexactfulltext=and&x=0&y=0.

53 Cheryl Pellerin, "Cybercom Builds Teams for Offense, Defense in Cyberspace," *DoD News*, March 12, 2013. See also, *Hearing to receive testimony on US strategic command and US cyber command in review of the defense authorization request for fiscal year 2014 and the future years' defense program,* March 12, 2013, http://www.armed-services.senate.gov/imo/media/doc/13-09%20-%203-12-13.pdf.

54 Rogers' statement on June 12, 2014 at a cyber seminar hosted by the Association of the US Army's Institute of Land Warfare.

55 Rogers' statement on May 28, 2014 at the 2014 Cyber Summit, http://www.defense.gov/news/newsarticle.aspx?id=122384.

56 OECD and the European Union.

57 The analysis of the Russian case relies on actual findings from the conduct ascribed to Russia in cyberspace.

58 "Firmware" is software that is positioned in a hardware device and handles the functioning of the component. As for its flexibility for changes, firmware is the intermediate state between software (which is very easy to change) and hardware, which cannot be changed. In most cases, the firmware of an electronic element is saved in ROM memory. Sometimes the firmware is saved on the flash drive, and then it can be updated by the end user. Common reasons for updating firmware are fixing bugs or adding content to a component.

59 See, for example, the products of enSilo Ltd., which test only the exit point of the organizational network and handle suspicious data only at this point. See also, the products of Secure Islands Ltd., which ensure that the files on the network are protected at a high level based on the company's security policy, without relation to their origin or nature of use. See Raphael Kahan, "Cyber out of the box: Security companies that think differently," *Calcalist*, March 25, 2015, following the exhibition of the two companies at the CyberTec conference, and the websites of Secure Islands and enSilo respectively at http://www.secureislands.com/product/technology/ and https://www.ensilo.com/.

60 Some commercial products exist. See, for example, the description on the VERINT website: http://www.verint.com/solutions/communications-cyber-intelligence/solutions/cyber-security/index.

61 Giora Engel, "Deconstructing the Cyber Kill Chain," *LightCyber*, November 26, 2014, http://lightcyber.com/deconstructing-the-cyber-kill-chain.

62 For a description of a fundamental solution based on anomaly, see Averbuch and Siboni, "The Classic Cyber Defense Methods Have Failed."

63 See reference to enSilo website: https://www.ensilo.com.

64 For example, see the solution proposed by Nyotron: http://www.nyotron.com. Another example is the solution proposed by Light Cyber: http://lightcyber.com/products and the data-based solution on characterization of the individual user proposed by BioCatch: http://www.biocatch.com/#!products/c5rw.

65 For example, as Keith Alexander stated at the Fourth Annual Cybersecurity Summit, September 25, 2013: "We can break down each system we see being scanned by an adversary and put it in a new place. You can jump networks, you can jump databases, and you can jump your phone system, [making] it very difficult for adversaries to exploit them." See http://www.defense.gov/news/newsarticle.aspx?id=120854.

66 The thought of handling information or a product stolen from a computer or network is based on the story of the strike on the Siberian gas line. Supposedly, the CIA had realized that the Soviets had stolen a plan for a control component from computers of a Canadian company in order to use in a similar component they were planning to design. The information in the programs had been corrupted in advance and caused an explosion in the Siberian gas line. Whether or not the story is true, it raises the possibility that manipulation of stolen data need not allow

the thief to use the stolen information successfully. The result need not be kinetic and overt as described in this story. Details of the story can be found in, "War in the Fifth Domain," *Economist* July 1, 2010, based on a book by Thomas Care Reed, who served as Air Force Secretary in the Ford and Carter administrations and as a consultant in the Reagan administration. See http://www.economist.com/node/16478792.

67 A full analysis of the main issues of DDoS attacks is located on the website of Arbor Networks: http://www.arbornetworks.com/ddos-attacks.

68 Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace."

69 See, for example, Sean Leach, "Four ways to defend against DDoS attacks," *Network World*, September 17, 2013, http://www.networkworld.com/article/2170051/tech-primers/four-ways-to-defend-against-ddos-attacks.html; George V. Hulme, "7 essentials for defending against DDoS attacks," *CSO*, January 14, 2013, http://www.csoonline.com/article/2133613/malware-cybercrime/7-essentials-for-defendingagainst-ddos-attacks.html.

70 Benedikt Martens and Frank Teuteberg, "Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model," University of Osnabrueck, Association for Information Systems AIS Electronic Library, May 2011, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.231.6718&rep=rep1&type=pdf.

71 "Experimental transfer of Bank Hapoalim to Amazon cloud," *TechTime*, September 18, 2014, http://techtime.co.il/2014/09/18/aws/; "Bank of Israel regulates use of cloud," *Israel Defense*, February 3, 2015, http://www.nrg.co.il/online/1/ART2/625/607.html; "USA: Commercial suppliers of cloud services in the service of the Defense Department," *iHLS*, December 15, 2014, http://i-hls.com/he/2014/12/commercial-vendors-invited-u-s-dod-data-centers.

72 A draft of directives of the Israel banking supervisor on the issue of risk management in the cloud environment, September 10, 2014, http://www.boi.org.il/he/BankingSupervision/DraftsFromTheSupervisorOfBanks/DocLib/10861.pdf.

73 "The US Defense Department uses the Amazon cloud," *iHLS*, August 27, 2014, http://i-hls.com/he/2014/08/amazon-expands-cloud-services-u-s-military.

74 See, for example, the cloud defense systems offered by Microsoft (for Azure): http://azure.microsoft.com/en-us/support/trust-center/security, and of Amazon's cloud: http://aws.amazon.com.

75 See, for example, technology developed by BioCatch. According to the company website, its purpose is mainly cloud protection: http://www.biocatch.com.

76 Hardware attacks are based on treating hardware components – the physical components of the computer, and/or firmware – the software is burned onto these physical elements.

77 This concern, whether justified or not, is expressed in the following example: computer equipment manufactured by Chinese companies Lenovo, Huawei, and ZTE is not authorized for purchase by the CIA, due to the fear of penetration of

attack components during the manufacturing stage. See James Sanders, "Corporate Espionage or Fear Mongering? The Facts about Hardware-Level Backdoors," *IT Security*, August 7, 2013, http://www.techrepublic.com/blog/it-security/corporate-espionage-or-fearmongering-thefacts-about-hardware-level-backdoors.

78 One example was a firmware-based attack demonstrated at the Black Hat security conference in Las Vegas by Jonathan Brossard, a cyber expert. The attack, called Rakshasa, demonstrated "back door" penetration of non-volatile memory (BIOS) and the difficulty in blocking this attack and removing it. See Sebastian Anthony, "Rakshasa: The Hardware Backdoor that China could Embed in Every Computer," *Extreme Tech*, August 1, 2012, http://www.extremetech.com/computing/133773-rakshasa-the-hardware-backdoor-thatchina-could-embed-in-every-computer.

79 Ibid.

80 See Anthony, "Rakshasa."

81 Paganini, "Hardware Attacks, Backdoors and Electronic Component Qualification; Lynn, "Defending a New Domain, The Pentagon Cyber Strategy"; Shahar Smooha, "World under Attack: Cyber Battles Jump up a Level," *Globes*, January 12, 2012, http://www.globes.co.il/news/article.aspx?did=1000714597.

82 Paganini, "Hardware Attacks, Backdoors and Electronic Component Qualification."

83 Gabi Siboni and David Siman-Tov, "Cyber Extortion – North Korea against the United States," *INSS Insight*, no. 646, December 2014, http://heb.inss.org.il/index.aspx?id=4354&articleid=8424; Gabi Siboni and Sami Kronenfeld, "Iranian Cyber Offensive during Operation Protective Edge," *INSS Insight*, no. 598, August 2014, http://heb.inss.org.il/index.aspx?id=4354&articleid=7583.

84 For example, the cyberattacks on the United States that were attributed to Iran, did not provoke any overt response for purposes of deterrence. See Elliot Jager, "Iranian Hackers Penetrated US Navy Marine Corps Internet for Four Months," *Newsmax,* February 18, 2014, http://www.newsmax.com/Newsfront/Iran-hackers-cyberattack-Navy/2014/02/18/id/553238; Julian E. Barnes and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers," *Wall Street Journal*, September 27, 2013, http://online.wsj.com/news/articles/SB10001424052702304526204579101602356751772.

85 Lupovici, "Cyber Warfare and Deterrence."

86 Steve Lewis and Kris Smith, "Lessons Learned from Real World Application of the Bow-Tie 89 Method," Presentation at American Institute of Chemical Engineers, Sixth Global Congress on Process Safety, San Antonio, Texas, March 22-24, 2010.

87 President Obama reacted to the Sony capitulation early on, calling it a mistake, and encouraged the company to screen the film despite the threats and the attack. The president promised a proportional reaction by the United States. As a result, North Korea suffered blows that paralyzed its internet traffic, and the United States authorized sanctions against North Korea. See David E. Sanger, Michael S. Schmidt, and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony,"

New York Times, December 19, 2014, http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-incyberattack-on-sony-pictures.html?_r=0.

88 In late September 2014, the government decided to establish a national cyber authority. On February 15, 2015, the government authorized a detailed "decision-makers proposal" for establishing the authority – see the website of the Prime Minister's Office, announcement of the Government Secretary, February 15, 2015, http://www.pmo.gov.il/mediacenter/secretaryannouncements/pages/govmes150215.aspx#three.

89 Roi Goldstein, "Cyberspace and Defense of Vital Infrastructure," Knesset Research and Information Center, May 12, 2013, www.knesset.gov.il/committees/heb/material/data/mada2013-05-13.doc.

90 Ibid., p. 7.

91 Gil Baram, "Cyber Warfare Technology and Building Force in Israel," *Military and Strategic Affairs* 5, no. 1 (April 2013): 24, http://www.inss.org.il/uploadImages/systemFiles/Armey%20-%205.1.pdf.

92 From the website of the National Security Council – activity of the Counter-Terrorism Bureau: defense of computer-integrated systems, http://147.237.72.17/NSCWeb/Templates/CounterTerrorismActivities.aspx.

93 Government decision no. 3611 of August 7, 2011, http://www.pmo.gov.il/secretary/govdecisions/2011/pages/des3611.aspx.

94 Ibid.

95 See announcement of the Prime Minister's spokesperson, September 21, 2014, http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokerashot210914.aspx.

96 From the website of the Teleprocessing Corps – Cyber Defense Department, http://www.tikshuv.idf.il/1090-he/tikshuv.aspx#.VGD4r8IUHIU.

97 Interview with Eyal Zelinger, chief officer of Teleprocessing Corps, *Haaretz,* March 4, 2013, http://www.haaretz.co.il/news/politics/1.1946156.

98 Announcement of IDF spokesperson: "The Chief of Staff Declares the Establishment of a Cyber Arm," June 15, 2015, http://www.idf.il/1133-22318-he/Dover.aspx.

99 From the Israel Police website: http://www.police.gov.il/contentPage.aspx?pid=308&mid=9.

100 From the website of the Justice Ministry: http://index.justice.gov.il/Units/ lita/news/Pages/NewsSekonimVeDarkiHetmodedot.aspx.

101 According to the decision of the Israeli government, published on September 21, 2014,
http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokerashot210914.aspx.

102 For a description of the arguments on the issue of organizational division of responsibility for cyber security in Israel, see Barak Ravid, "The NSA and Cyber Bureau are Battling over who will Fight Computer Attacks, Netanyahu Refrains from Deciding," *Haaretz*, September 14, 2014, http://www.haaretz.co.il/news/politics/.premium-1.2432606.

103 Gabi Siboni, "An Integrated Approach is Necessary," *Haaretz*, cyber supplement, March 2015.

104 The parallel in the kinetic space is, for example, when crime organizations in southern Israel smuggle weapons from the Sinai Peninsula into Israel, thus creating a combined criminal/security incident.

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

106 Matt Comyns, Tim Cook, Jesse Reich, "Global Leadership – New Threats New Leadership 109 Requirements: Rethinking the Role and the Capabilities of the Chief Information Security Officer," *Russell Reynolds Associate*, October 29, 2014, http://www.russellreynolds.com/content/rethinking-capabilities-of-chief-information-security-officer; Bank of Israel, "The Banking Supervisor, Proper Banking Management, Cyber Defense Management," Directive 361, March 2015, http://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/361.pdf.

107 Lecture of David Brodet in a panel on "The Defense Budget – Separate or Part of the General Pie," INSS Annual Conference, Tel Aviv, February 16, 2015, https://www.youtube.com/watch?v=JqmGOCTxeds.

108 Or Hirshauga, "Hacker Group Initiates Attack on Israel this Wednesday," *Haaretz*, September 9, 2013, http://www.themarker.com/technation/1.2116064.

109 Kaspersky Security Bulletin, Kaspersky Lab Global Research and Analysis Team, 2013, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf.

110 Ibid. Some of the sophisticated attacks are carried out through "hired guns" – groups that offer attack services for hire, some sophisticated and on the basis of specially-built attack tools.

111 The first principle of the US operation in cyberspace relates to cyberspace as a field of battle operations, requiring the department to train and equip itself so that it can obtain the fullest potential advantages in cyberspace. See "Department of Defense Strategy for Operating in Cyberspace," July 2011, pp. 5-6, http://www.defense.gov/news/d20110714cyber.pdf.

112 Rogers stated, "In the year 2025, I believe . . . Army commanders will maneuver offensive and defensive capability much today as they maneuver ground forces," Rogers said, adding that "command and control, key terrain, commander's intent, synchronization with the broader commander's intent, and a broader commander's operational concept of operations will be cornerstones of Army cyber operations by then." See Pellerin, "Cybercom Chief: Cyberspace Operations Key to Future Warfare."

113 David E. Sanger, "Syria War Stirs New U.S. Debate on Cyber-Attacks," *New York Times*, February 24, 2014. The author determines that the Americans' 2011 plan to implement a cyberattack to paralyze the Syrian air force in order to prevent attacks on civilians was not authorized by the president because physical attacks were also needed in order to achieve the objective.

114 John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *New York Times*, August 1, 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?_r=0.
115 Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace."
116 Michael N. Schmitt, "The Law of Cyber Targeting," Tallinn Paper, no. 7 (2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_07_2015.pdf.
117 Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," *Military and Strategic Affairs* 4, no. 3 (December 2013): 77-99, http://media.wix.com/ ugd/ d4 8d94_1f8bd495a0554e44967b99e25e931eae.pdf.
118 Siboni and Siman-Tov, "Cyber Extortion – North Korea vs. the United States"; "The Hackers who Attacked Sony: We'll Carry out Attacks in the United States," *Walla*, December 17, 2014, http://news.walla.co.il/item/2811400; Nicole Perlroth and David Sanger, "North Korea Loses Its Link to the Internet," *New York Times*, December 22, 2014, http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internetcollapses.html?_r=0.
119 Ellada Gamreklidze, "Cyber Security in Developing Countries: A Digital Divide Issue," *Journal of International Communication* 20, no. 2 (2014): 200-217, http://dx.doi.org/10.1080/13216597.2014.954593.
120 Langner, "Stuxnet's Secret Twin."
121 According to Langner's proposed analysis, the goal of the attack was to cause the Iranians to mistrust their ability to operate the centrifuge control system, and not to cause destructive damage to the centrifuges themselves. By planning to cause long-term damage, and not broad immediate damage, the Iranians recognized that the problem was not due to their technological knowledge, but rather a cyberattack. As Langner writes: "If catastrophic damage had been caused by Stuxnet that would have been by accident rather than on purpose. The attackers were in a position where they could have broken the victim's neck, but they chose continuous periodical choking instead. Stuxnet is a low-yield weapon with the overall intention of reducing the lifetime of Iran's centrifuges and making the Iranians' fancy control systems appear beyond their understanding." See Ibid., p. 7.
122 As Langner states "The results of the overpressure attack are unknown. Whatever they were, the attackers decided to try something different in 2009. This new Stuxnet variant was almost entirely different from the old one. For one thing, it was much simpler and much less stealthy than its predecessor. It also attacked a completely different component of the Natanz facility: the centrifuge drive system that controls rotor speeds . . . At some point the attacks should have been recognizable by plant floor staff just by the old eardrum . . . It's another sign that the makers of this second Stuxnet variant had decided to accept the risk that the attack would be detected by operators." Ibid., pp. 5, 7.
123 Ibid., p. 9.
124 Ibid.

INSS Memoranda, July 2014–Present

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].

No. 150, October 2015, Arik Rudnitzky, *Arab Citizens of Israel Early in the Twenty-First Century*.

No. 149, October 2015, Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy* [Hebrew].

No. 148, September 2015, Meir Elran and Gabi Sheffer, eds., *Military Service in Israel: Challenges and Ramifications* [Hebrew].

No. 147, June 2015, Zvi Magen and Tatyana Karasova, eds., *Russian and Israeli Outlooks on Current Developments in the Middle East.*

No. 146, April 2015, Shmuel Even, *The Cost of Defense in Israel: Defense Expenditures and Recommendations for Drafting the Defense Budget* [Hebrew].

No. 145, December 2014, Yoav Zacks and Liran Antebi, eds., *The Use of Unmanned Military Vehicles in 2033: National Policy Recommendations Based on Technology Forecasting Expert Assessments* [Hebrew].

No. 144, November 2014, Oded Eran, Dan Vardi, and Itamar Cohen, *Political Feasibility of Israeli Natural Gas Exports to Turkey*.

No. 143, November 2014, Azriel Bermant, *The Russian and Iranian Missile Threats: Implications for NATO Missile Defense*.

No. 142, September 2014, Emily B. Landau and Anat Kurz, eds., *The Interim Deal on the Iranian Nuclear Program: Toward a Comprehensive Solution?*

No. 141, September 2014, Emily B. Landau and Anat Kurz, eds., *The Interim Deal on the Iranian Nuclear Program: Toward a Comprehensive Solution?* [Hebrew].

No. 140, July 2014, Oded Eran, Dan Vardi, and Itamar Cohen, *Exporting Israeli Natural Gas to Turkey: Is it Politically Possible?* [Hebrew].

No. 139, July 2014, Arik Rudnitzky, *Arab Citizens of Israel at the Start of the Twenty-First Century* [Hebrew].